Industrial Cybersecurity Industry Analysis

October 2023

V011023

WESTLANDS ADVISORY

WESTLANDS ADVISORY

Introduction

The *'Industrial Cybersecurity Industry Analysis 2023'* is Westlands Advisory's 3rd edition and updates forecasts, analysis and segmentation in the previous edition. The research and analysis was conducted from December 2022 and the market forecasts were completed in April 2023. The competitive analysis will be included alongside the *'OT Cybersecurity Navigator'* in July 2023. The *'CISO Guide to the OT Cybersecurity Market'* is an additional report for use by CISO's and engineering teams and can be distributed under license.

The analysis is based on previous work, analysis of secondary information sources (company websites, presentations, government websites, regulation, economic databases, research papers) and interviews with vendors, security services organisations, Managed Security Services Providers, governments, industry thought leaders and CISO's. This includes industrial OEMs, engineering services firms, government contractors, telcos and IT services companies.

Note that some of the industry vertical commentary is similar to 2022. It has been updated and changed where relevant though some passages have remained the same due to limited developments over the last 12 months.

Definitions and Segmentation

Regional Segmentation

North America

Europe

Middle East

Latin America

Central Asia

Asia Pacific

Africa

Technology Segmentation

Visibility & Threat Detection

Endpoint Protection & Detection

Network Access Control

Risk & Vulnerability Management

Network Protection

Advanced Threat Protection

Remote Access Management

Security Operations

Services

Managed Security Services

Professional Security Services

Industrial Verticals

Textiles & Leather
Wood Products
Paper Products & Printing
Rubber & Plastics
Other Non-Metallic
Machinery
Computing & Electronics
Semiconductors
Electrical
Other Transport Equipment
Automotive
Other Discrete Manufacturing
Food, Beverage & Tobacco
Pharmaceuticals
Power Generation
Energy Transmission & Distribution
Water & Wastewater Treatment
Rail
Maritime
Air, Logistics & Warehousing
Oil & Gas
Mining
Refineries
Chemicals & Chemical Products
Basic Metals
Fabricated Metals

Out of Scope

IOT related markets including;

- Building Management Systems
- Hospitals and Medical Devices
- Smart City Applications

Executive Summary

Executive Summary

Overall, OT Cybersecurity maturity remains low across critical infrastructure and manufacturing though there is wide variance both between and within industry sectors. Growing awareness of cybersecurity risk has resulted in increased investment in OT which will result in more mature security programs by 2030. Westlands Advisory estimates that expenditure on OT cybersecurity in 2023 will be $8.4B. At a CAGR of 18% the market will triple in size by 2030, reaching $26.9B.

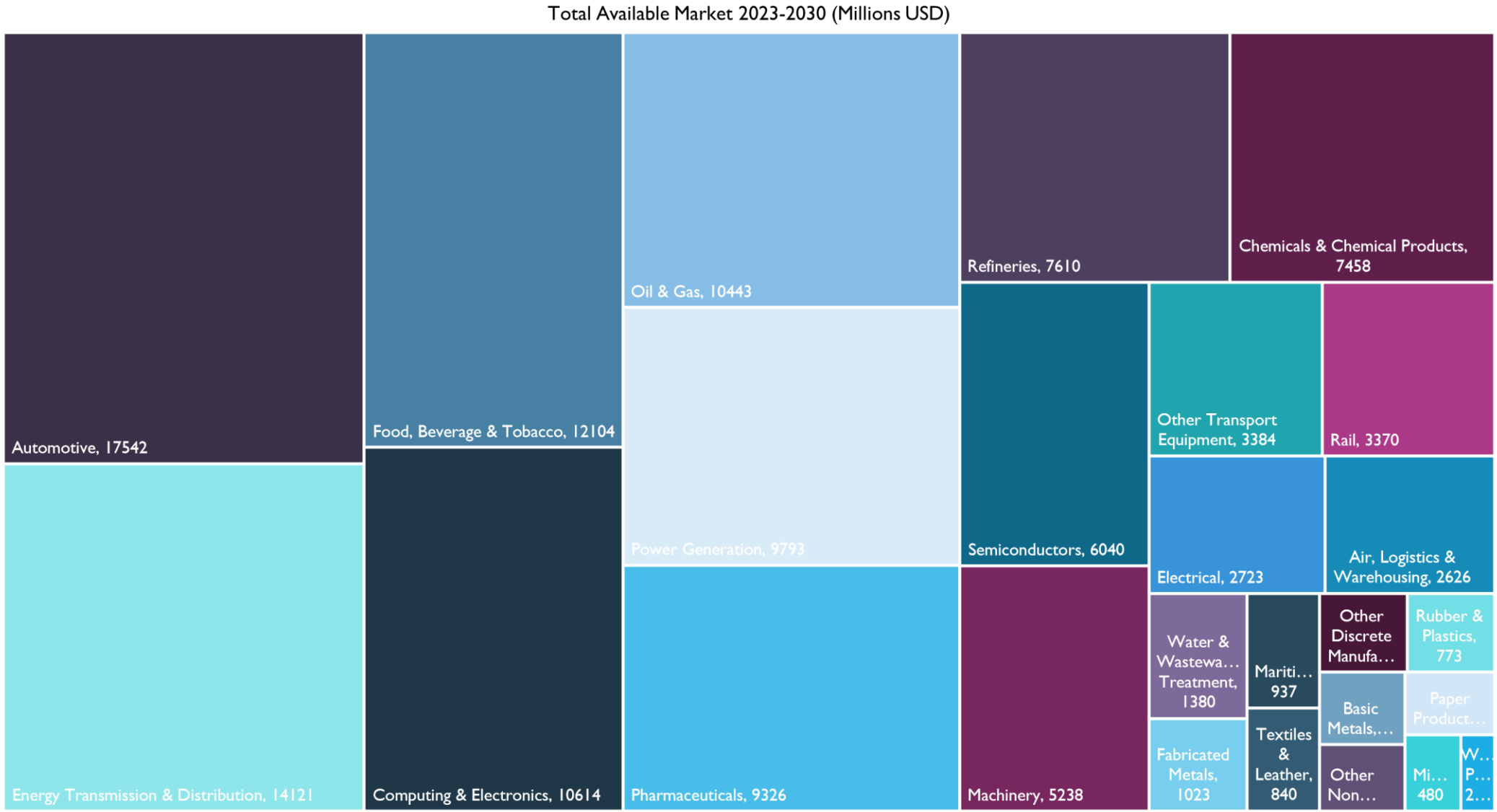
Investment is being driven principally by regulation and the digital transformation (DX) of industrial operations. Energy sectors (power generation, transmission & distribution, Oil & Gas and refining) have been heavily influenced by regulation in recent years whilst the increasing automation and digitalisation of high value manufacturing sectors (Automotive, Pharmaceuticals and Computing & Electronics) has resulted in a growing focus on cybersecurity. These are among the largest market segments and investment will continue to increase to 2030.

OT networks are often Data Rich and Information Poor with huge benefits yet to be derived from greater data exploitation. To accelerate digital transformation asset owners require asset and network visibility but also need to manage the data and alerts efficiently. This has resulted in innovation to not only identify assets, but to also categorise, profile and automate risk and vulnerability management through Machine Learning. Asset discovery and vulnerability management are high growth product segments and address the 'known known' risks to operations. Alongside firewalls and network segmentation, access management, and endpoint protection, these controls provide strong protective measures.

There is a growing requirement in regulation and standards to ensure that the 'unknowns' are covered requiring continuous monitoring through either passive or active scanning and Machine Learning to detect and alert if there are deviations from the baseline. To protect against the unknown scenarios, asset owners should move towards implementing a security model based on resilient operations and a focus on people, technology and processes to ensure organisations are able to withstand and recover from a cyber incident without disruption to operations. Westlands Advisory expects asset owners to increase investment in resilience which will include staff awareness and training, incident response and a greater focus on supply chain partners.

By 2030 we expect OT cybersecurity maturity to have advanced significantly within utilities and large, transnational manufacturing organisations. Many organisations will have converged security operations providing company wide visibility, with dedicated OT teams trained on processes and procedures. Security will be increasingly managed by cloud platforms, either by the asset owners or by a managed service provider, and there will be a growing focus on managing and protecting wireless 5G networks. We also expect improved supply chain cybersecurity maturity and a greater installed base of industrial operations built on secure-by-design principles. Digital and cyber maturity will differ by industry sector though progress to 2030 will continue to depend on technological innovation, regulatory oversight and a stable global economy.

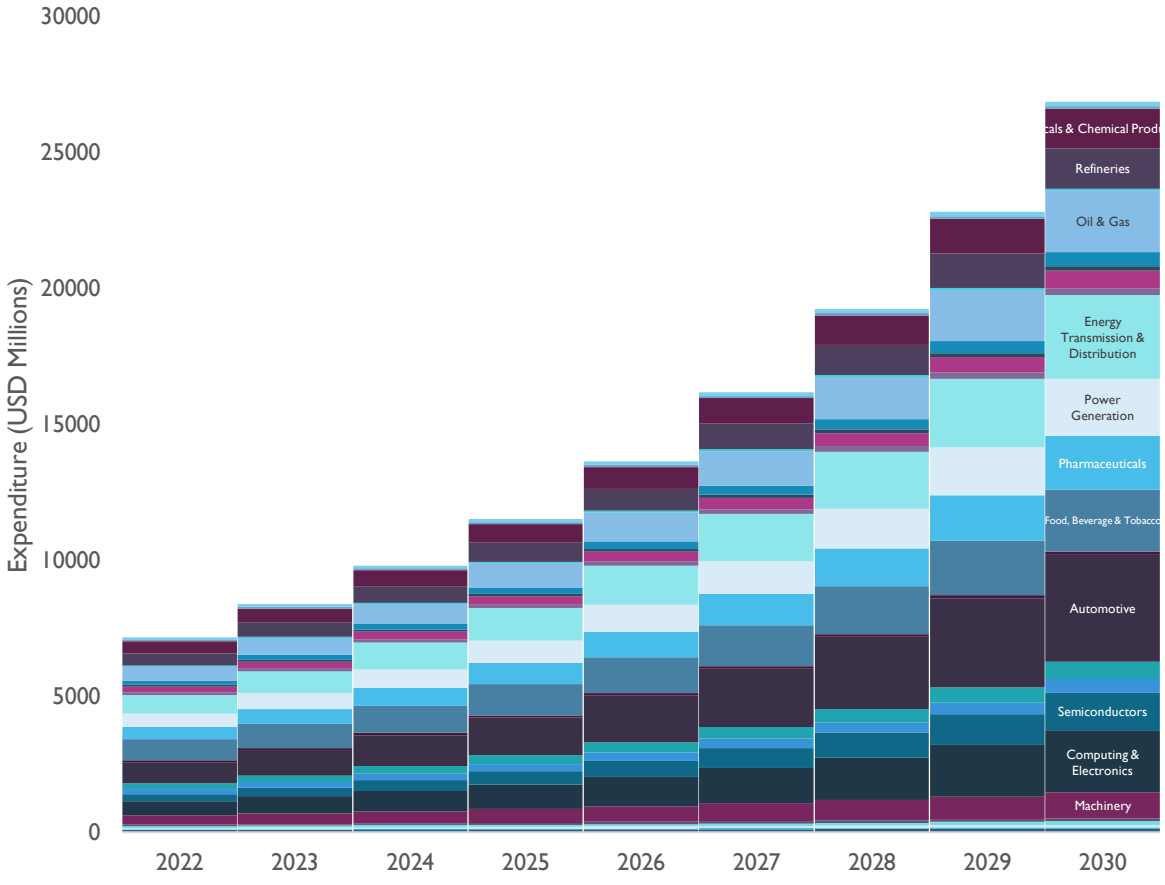
The Total Available Market for OT Security Technology & Services from 2023-2030 is $128B, with significant expenditure in highly automated and regulated market segments



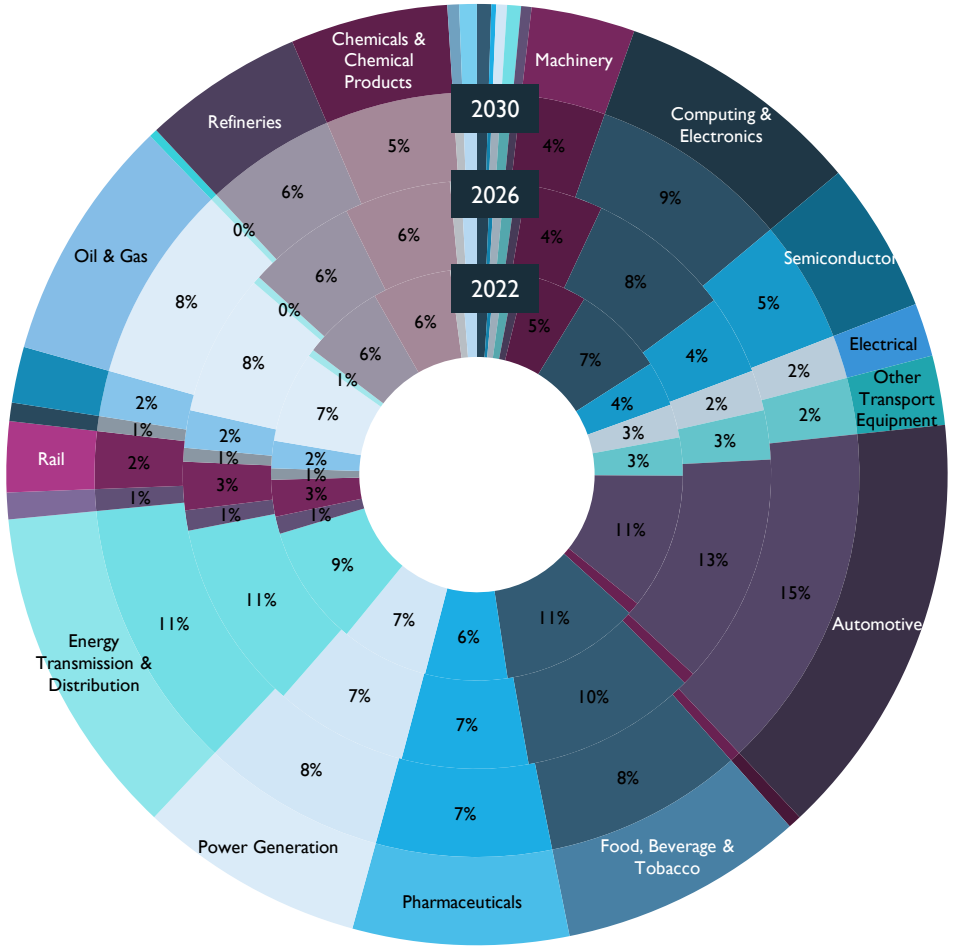
Investment in OT cybersecurity will increase in all market segments but at very different rates. Automotive, Pharma, Oil & Gas and Utilities comprising ~ 50% of the market by 2030

WESTLANDS ADVISORY

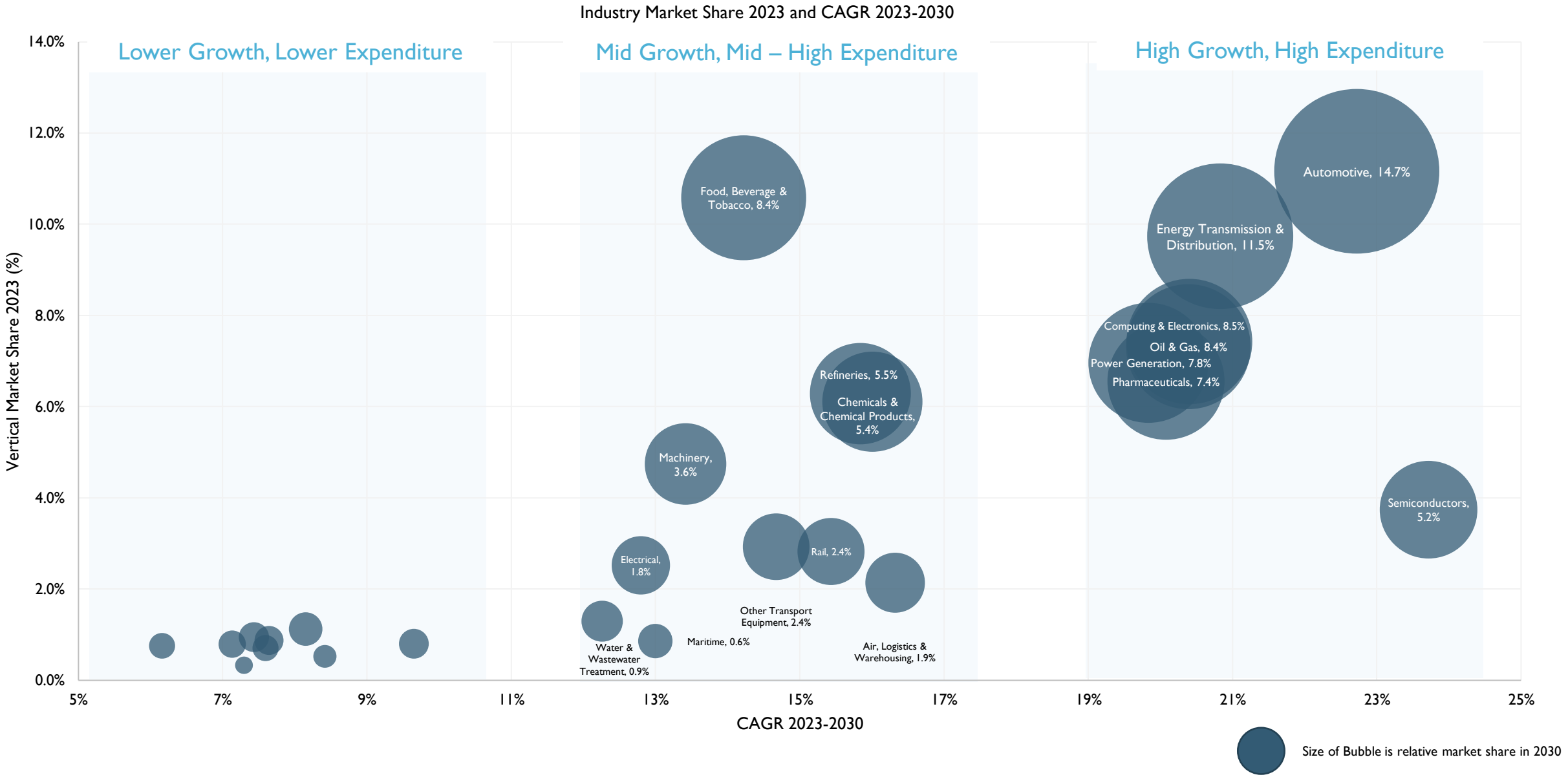
Global OT Cybersecurity Market Expenditure, 2022-2030 (USD Millions)



Global OT Cybersecurity Expenditure 2022,2026,2030



High Growth, High Expenditure markets includes Automotive, Energy, Computing and Electronics, Oil & Gas and Pharmaceuticals

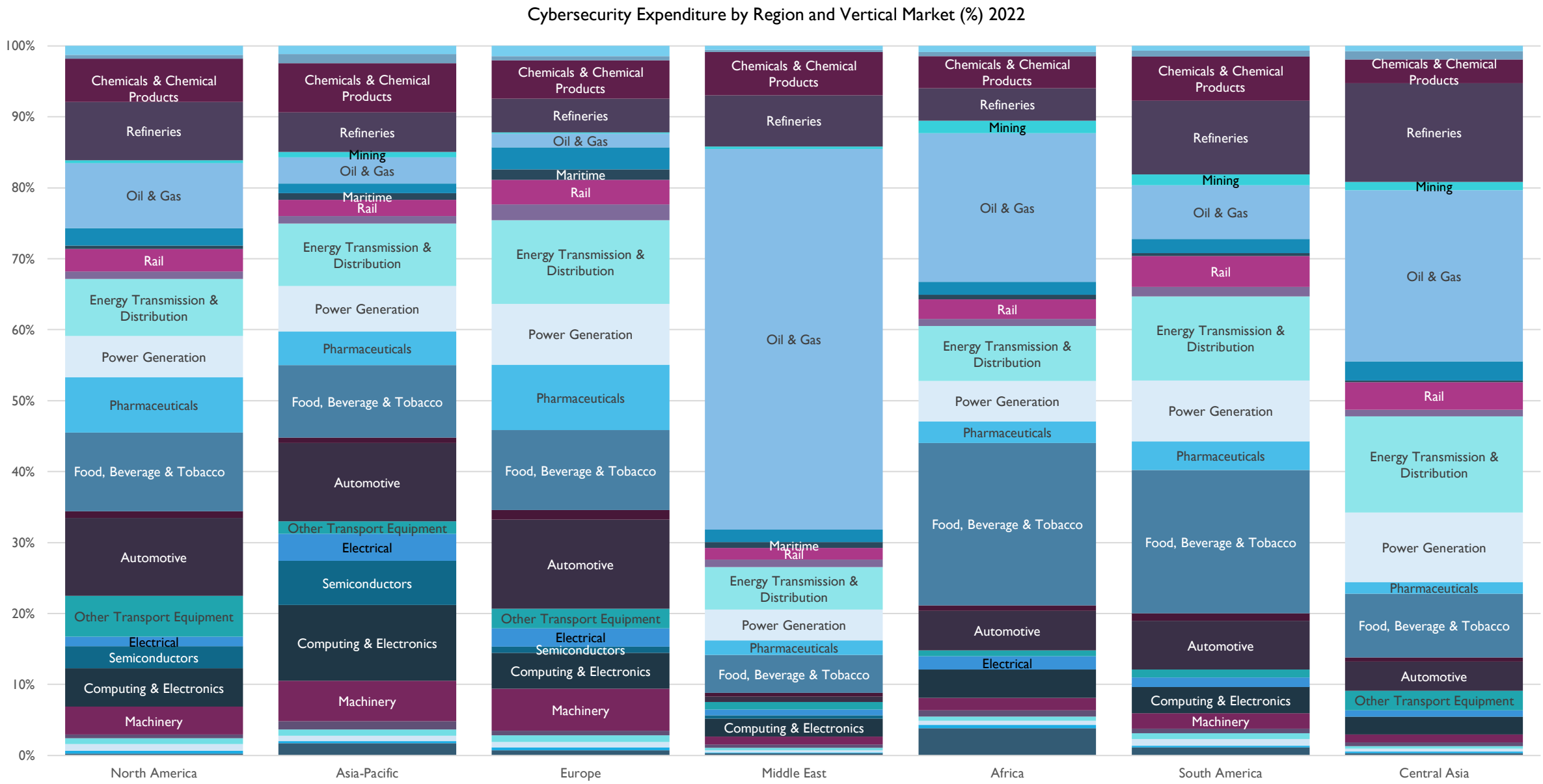


The United States and China spend the most on OT cybersecurity followed by countries with high manufacturing output including Germany and Japan.

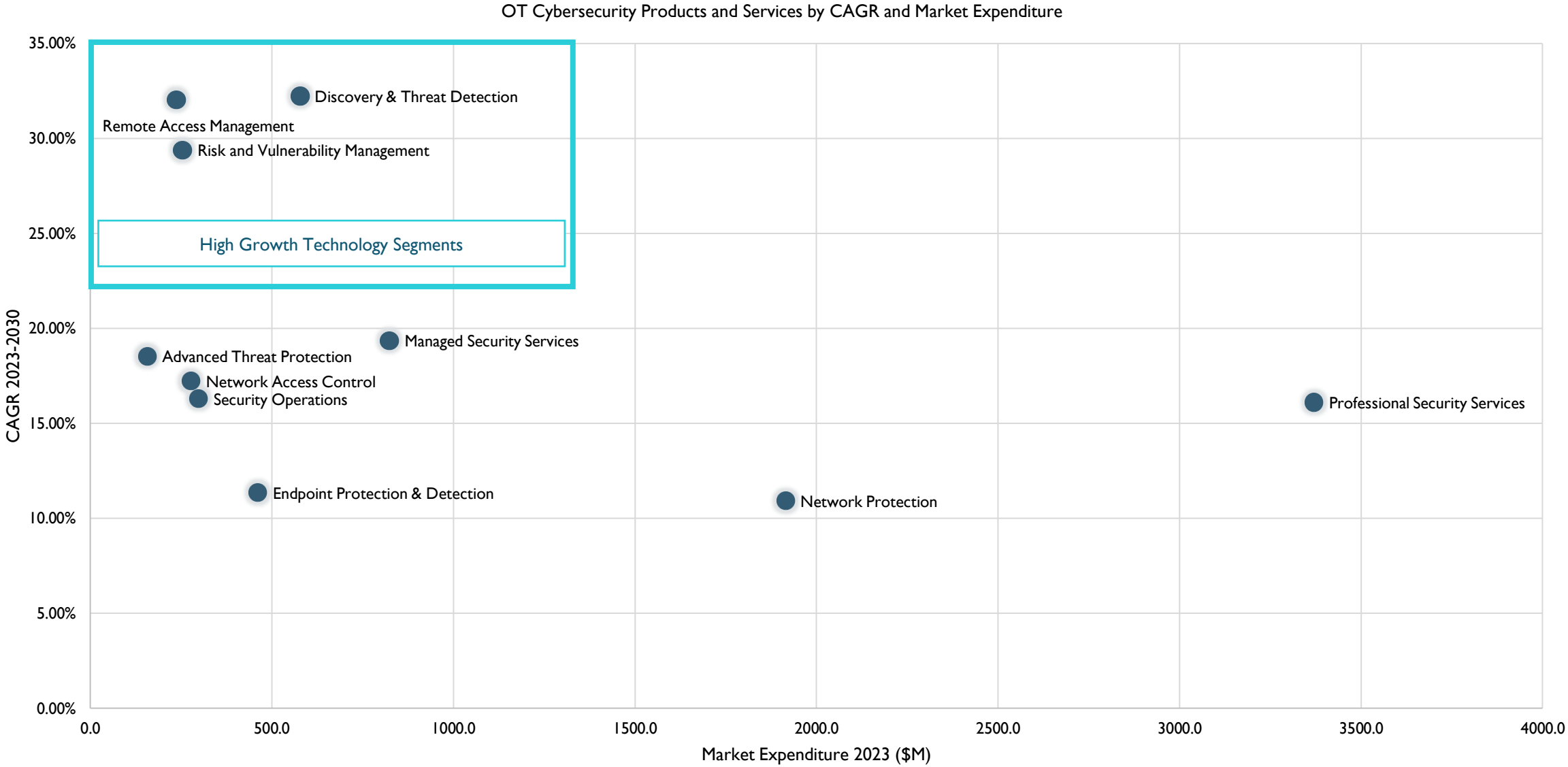
WESTLANDS ADVISORY

Global OT Cybersecurity Market Expenditure by Country 2022 ($M)

Vertical market cybersecurity expenditure varies by region, particularly Oil & Gas and higher end manufacturing segments including automotive and pharmaceuticals



High demand for asset discovery and threat detection tools aligns with low levels of cybersecurity maturity and a requirement for improved network visibility



Cybersecurity Investment Drivers

The underlying conditions that have led to increasing investment in OT cybersecurity will continue to promote higher investment through the forecast period to 2030

WESTLANDS ADVISORY

1. Investment in industrial automation has remained resilient to recent economic uncertainty. The business benefits derived from automation and connectivity are likely to sustain investment in plant modernisation to 2030.

2. Continuing digital transformation to improve productivity, efficiency and innovation through investment in digital twins, machine learning and cloud analytics will increasingly connect the OT environment to IT systems and applications increasing the requirement for secure and resilient operations.

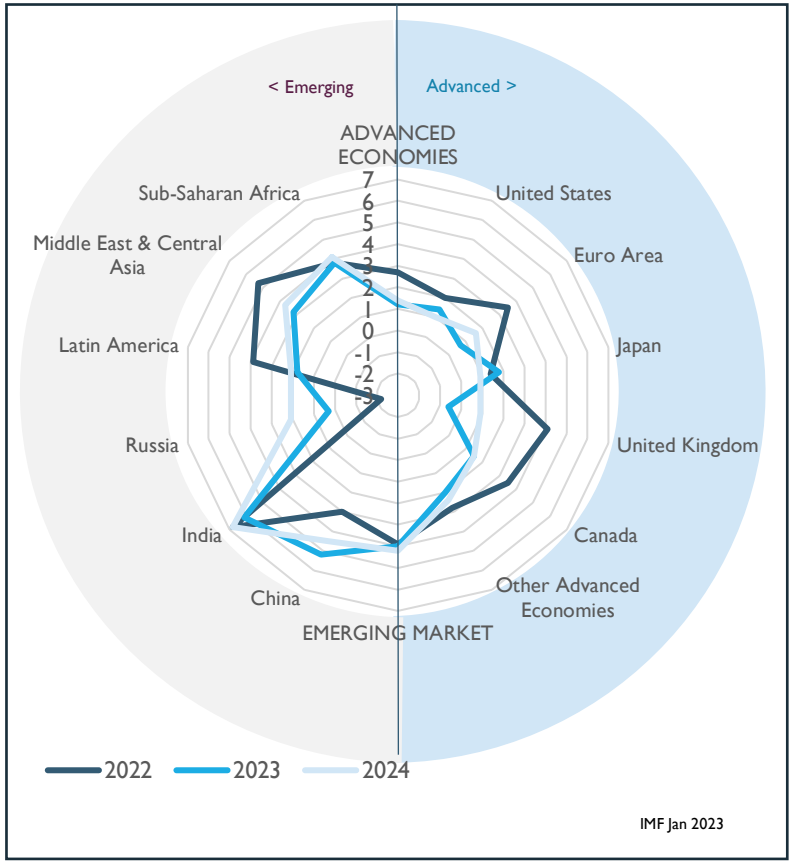
3. Regulatory requirements are expected to strengthen to 2030. This will require asset owners to expand security programs to include a range of security controls and improve processes related to supply chain security. Regulatory coverage will also increase in industry scope – more mid sized manufacturing organisations will come under the purview of national regulators.

4. The cyber threat is unlikely to reduce to 2030 and, with increasing IT and OT convergence, the risk of a cyber incident compromising the availability of manufacturing operations will remain elevated until cybersecurity programs mature.

The Economic environment for manufacturing has been bleak for several years though there are signs of recovery in high tech sectors. Conversely utilities have benefited from inflation.

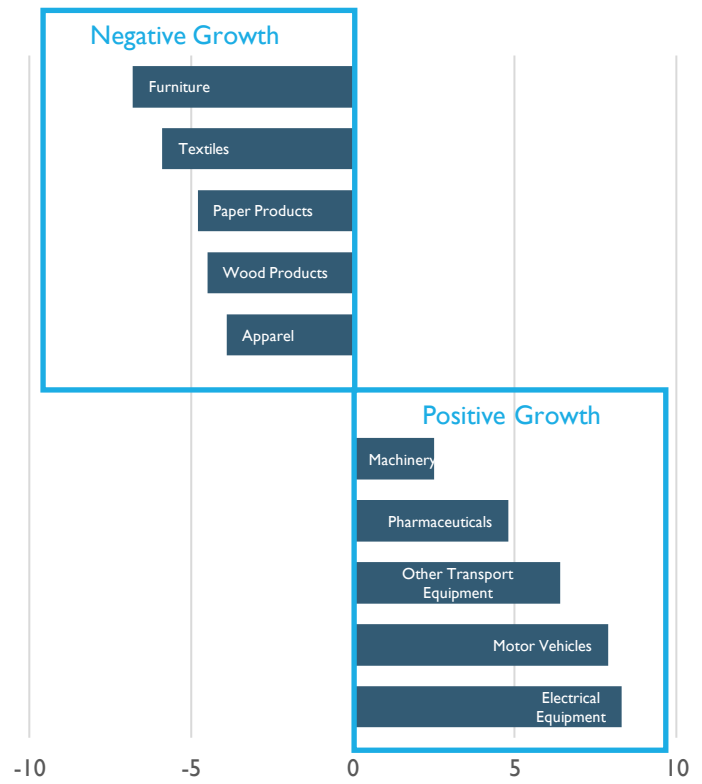
WESTLANDS ADVISORY

GDP Growth to pick up after 2023 for most regions
(annual % growth)



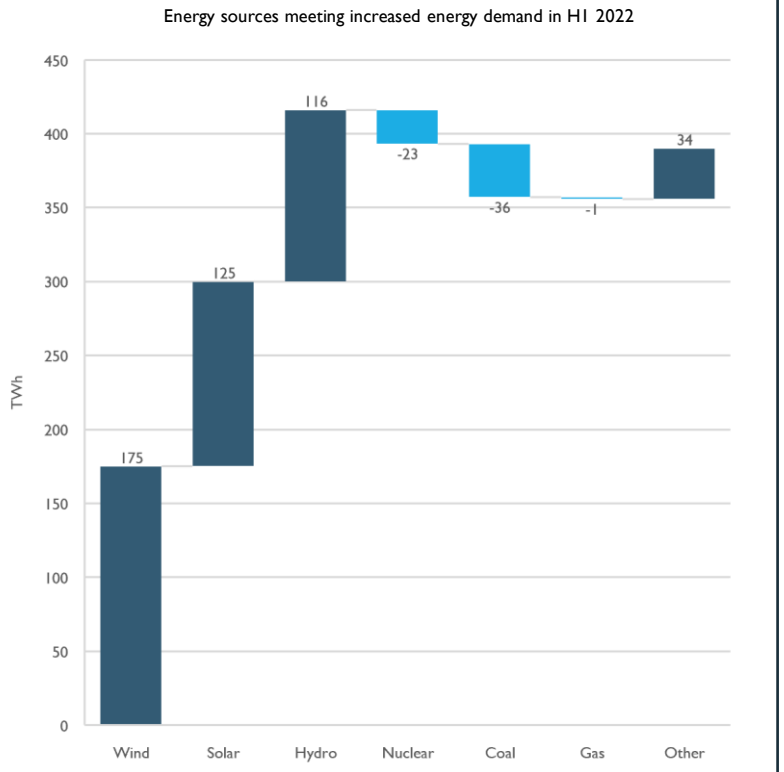
IMF Jan 2023

Year over Year manufacturing growth in Q4 2022 varied significantly by industry sector with high tech sectors expanding and low tech sectors contracting



UNIDO Q4 2022

Global energy demand increased by 389TW in H1 2022 with increased demand mostly met by renewable energy sources



Ember

Inflation will ease and a return to stable economic growth for most countries is expected, albeit at suppressed levels with advanced economies growing at only 1.4% in 2024. Developing market growth for the same year is 4.2%. China at 4.5% is well below it's pre covid trend whilst India is forecast to grow strongly

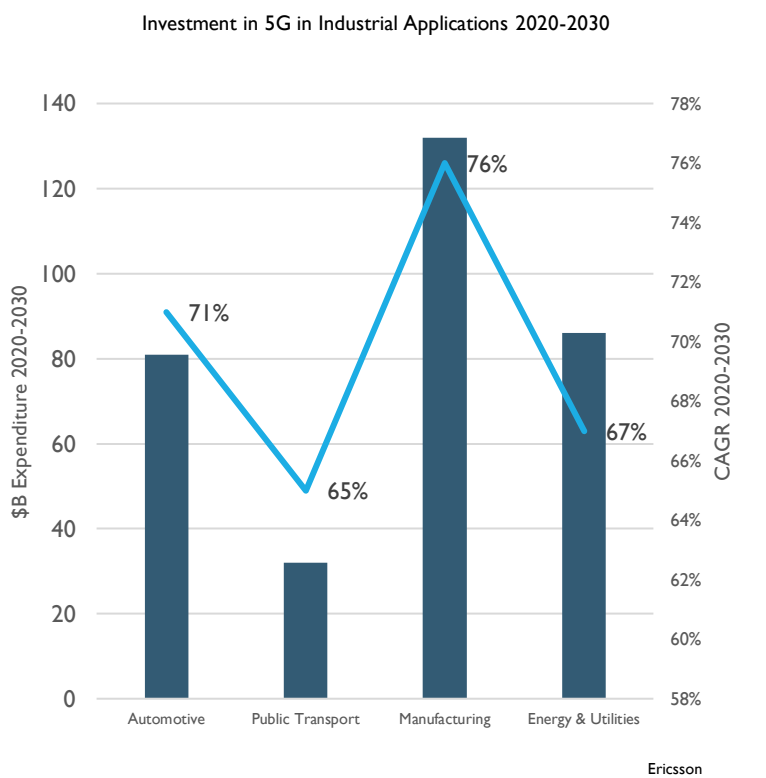
Manufacturing production in Q4 2022 only increased 1.5% year-over-year, the slowest rate since the post pandemic bounce back. Demand for products from high tech sectors is expected to grow to 2030.

High oil and electricity prices in 2022 resulted in record energy company profits. Renewable production is growing globally, resulting in investment in distributed generation and connection to the grid. High company profitability may result in higher CAPEX on energy system modernisation.

Digital transformation of manufacturing and process industries is progressing though at varying rates across regions and industries

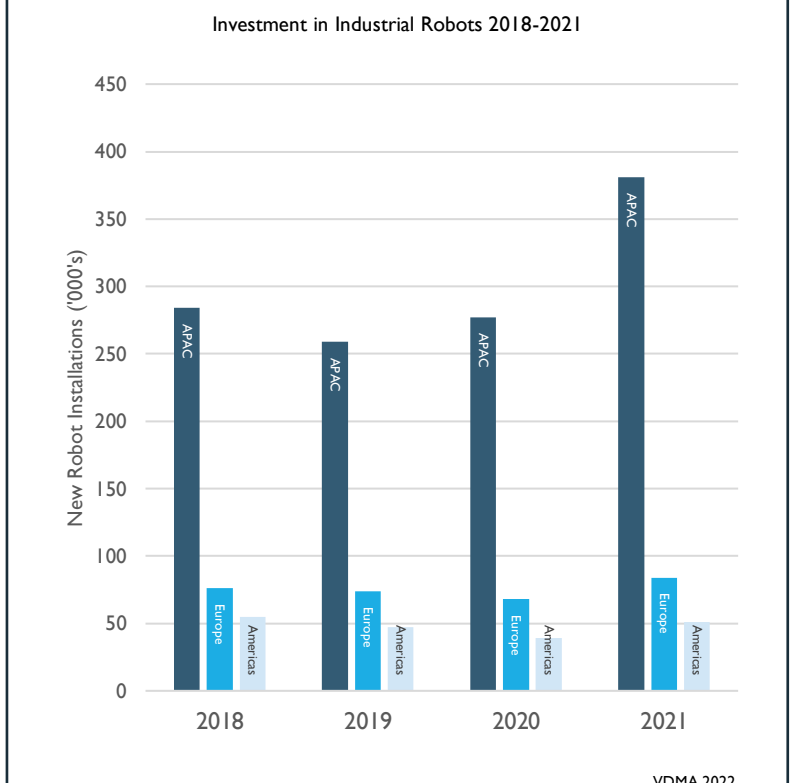
WESTLANDS ADVISORY

5G networks, digital twins and AI will transform manufacturing and process industries



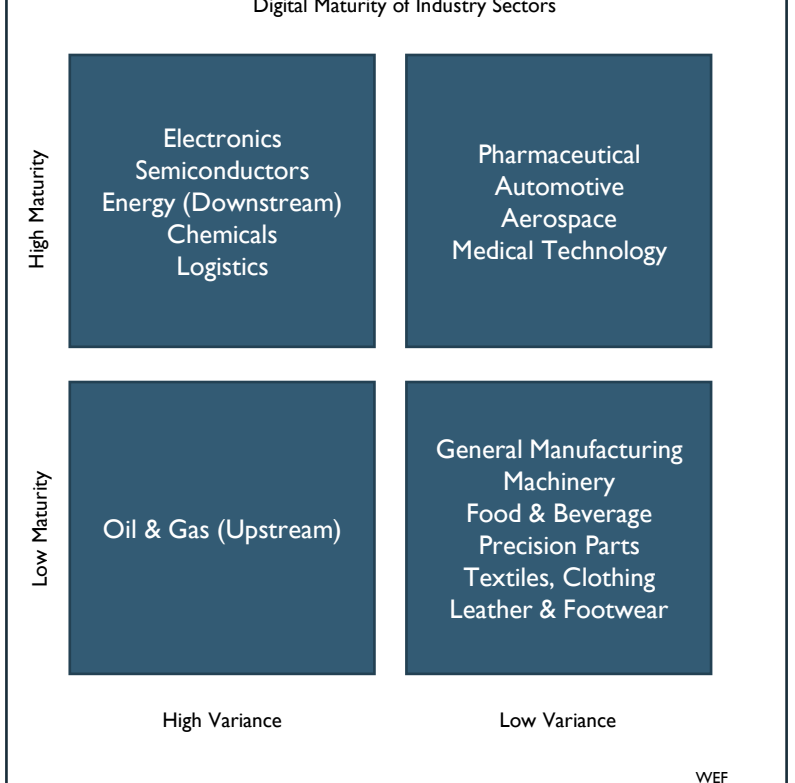
Manufacturing is expected to invest heavily in 5G networks to 2030, with cumulative expenditure from 2020-2030 to total $130B, and a CAGR of 76%, enabling significant improvements to real-time automation, monitoring and tracking.

Growing automation as new robot installations hit a record high in 2021 with future growth expected to settle at approximately 8-10% per year



The installed base of autonomous robotics is increasing with significant investment in APAC. The electronics (26% of new installations in 2021) and automotive industry (23%) are the largest investors in industrial robots. Machinery, Plastic Products and Food & Beverage are the remaining significant sectors.

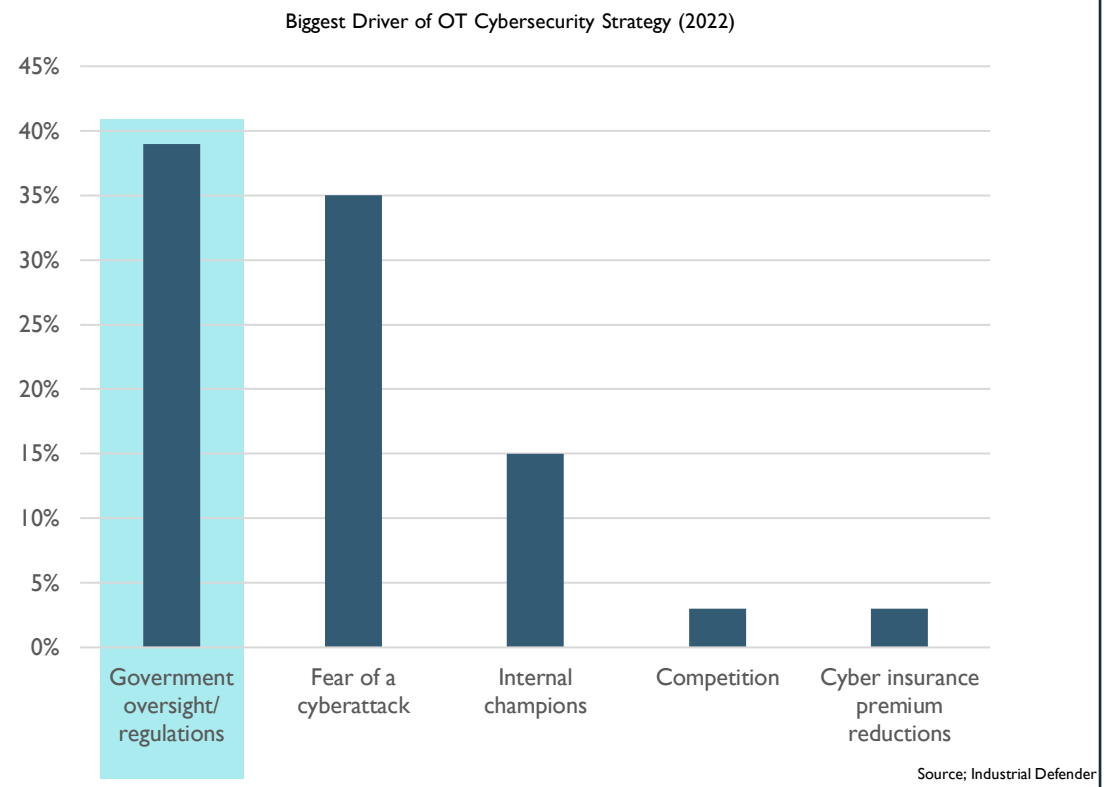
Despite fast digitalisation in some sectors, there remains wide variance within industries



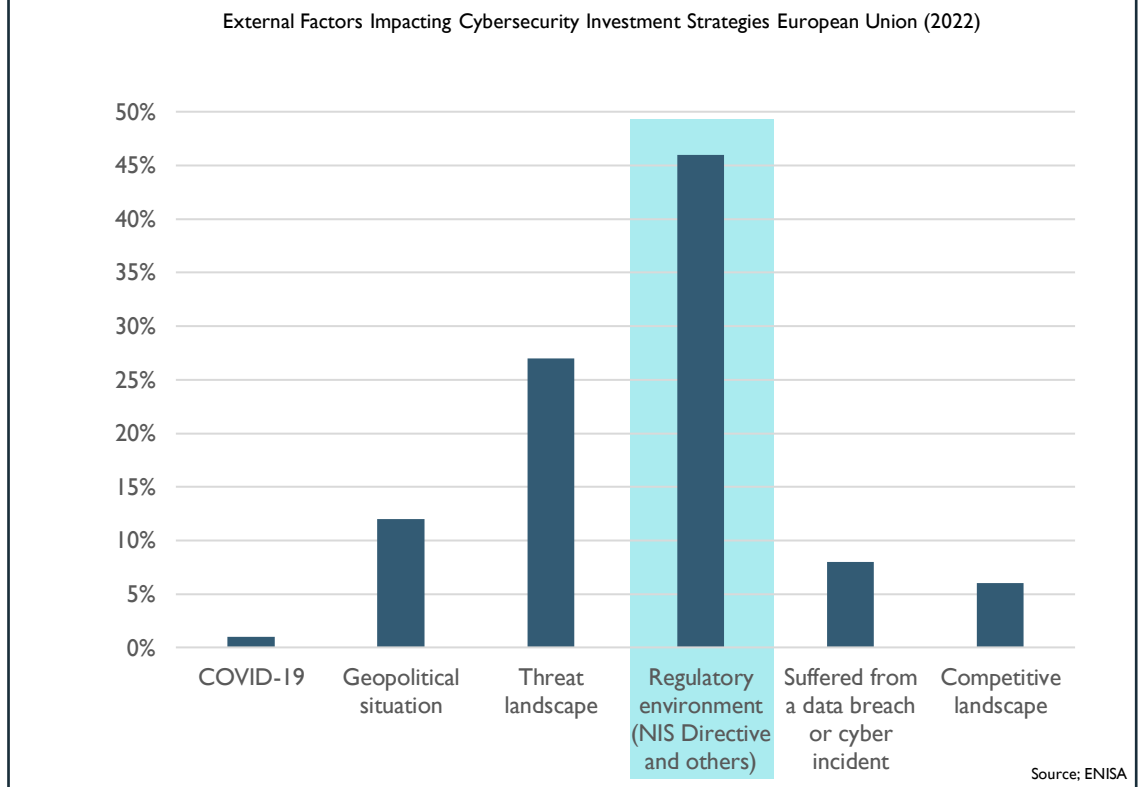
WEF's analysis of a 'basket' of companies concludes that Pharma, Automotive, Aerospace and Medical Technology are among the most digitally mature with low variance between companies. Electronics, Semiconductors, Energy, Chemicals and Logistics are also relatively mature but with high variance.

Regulation is consistently cited as the primary reason for investing in cybersecurity products and services across regions and industries

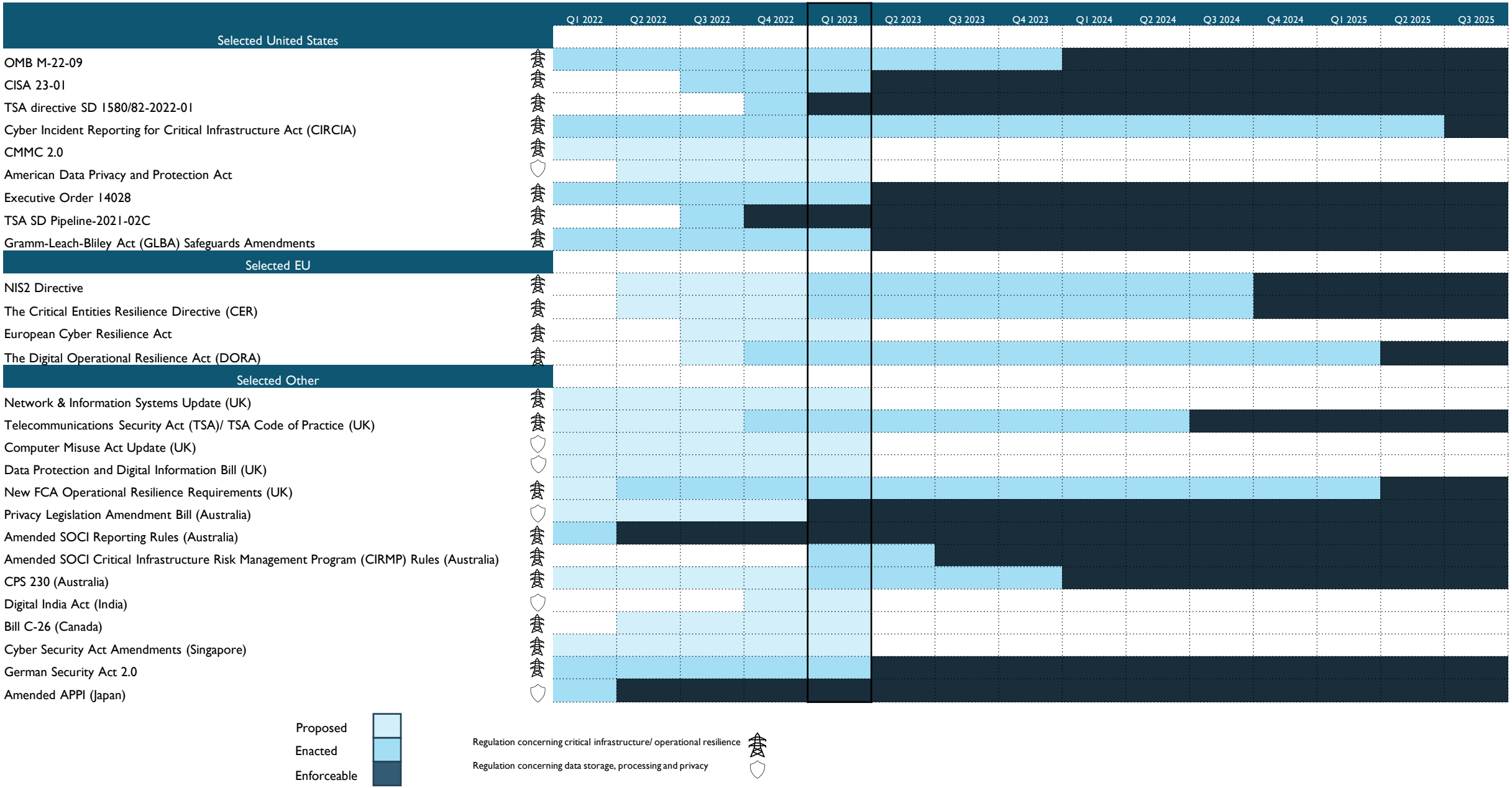
Government oversight and regulations remain the biggest driver for investment in cybersecurity



Regulation is consistently cited as the primary motivation for investment around the world, though the perceived high threat and growing understanding of the cyber risk are also principle drivers of security programs.



Whilst Regulation has been a contributing factor to increasing investment in cybersecurity, low enforcement has led to low adoption. New regulation aims to address previous weaknesses



Regulation is extending beyond the classic definitions of critical infrastructure to include other industries of national importance or essential to the wider supply chain

WESTLANDS ADVISORY

NIS (EU)

Energy
Water supply
Banking
Transport
Healthcare
Digital services

NIS 2 (EU)

Energy
Water supply
Banking
Transport
Healthcare
Electronic communication networks
Waste management
Space
Digital services
Certain manufacturing
Postal service
Food
Social Networks
Public Administration

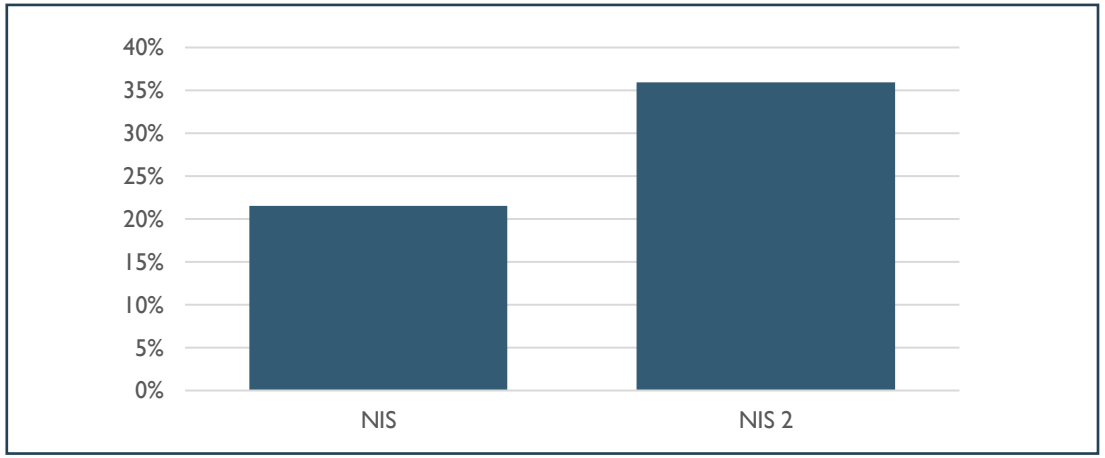
Initial SOCI (Australia)

Energy
Water supply
Transport

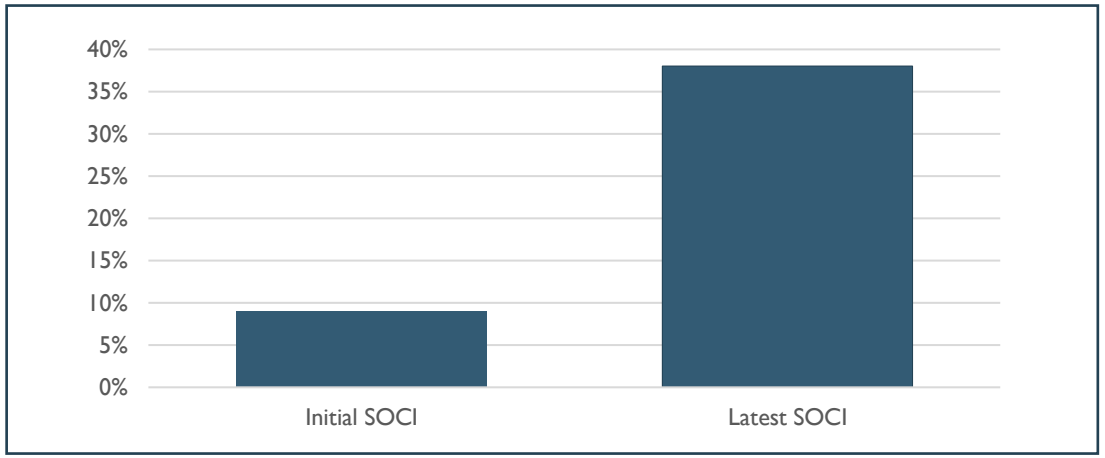
Latest SOCI (Australia)

Energy
Water supply
Banking
Transport
Healthcare
Electronic communication networks
Waste management
Space
Data storage and processing
Certain manufacturing
Postal service
Food
Social Networks
Public Administration

Economic Coverage of NIS across the 12 largest EU states



Economic Coverage of SOCI



Sources; Security of Critical Infrastructure Act 2018, the Security Legislation Amendment (Critical Infrastructure) Act 2021, NIS2 Directive, WA Analysis of Economic Input Output Data

Perceptions of cybersecurity related Risk to OT processes are maturing as asset owners' understanding of threats, vulnerabilities and the impact on business operations improve

WESTLANDS ADVISORY

Threats

- Internal Error
- Malware / Ransomware
- Advanced Persistent Threat (APT)

Probability of threat targeting infrastructure

Threat research continues to highlight a significant number of known threats with little evidence to suggest that either the risk from ransomware will decline, or that current geopolitics will lead to a de-escalation from state sponsored groups

Vulnerabilities

- Software vulnerabilities
- Misconfigurations
- Physical vulnerabilities
- Supply chain

Probability of vulnerability being exploited

There are a high number of known software vulnerabilities that asset owners need to prioritise and mitigate, whilst supply chain vulnerabilities and human error continue to contribute to risk.

Impact

- Production downtime
- Financial loss
- Safety Incident
- Supply chain disruption
- Legal

Impact of event on business operations

Consequences from an OT related incident are increasingly well known though cybersecurity maturity remains low despite growing expenditure.

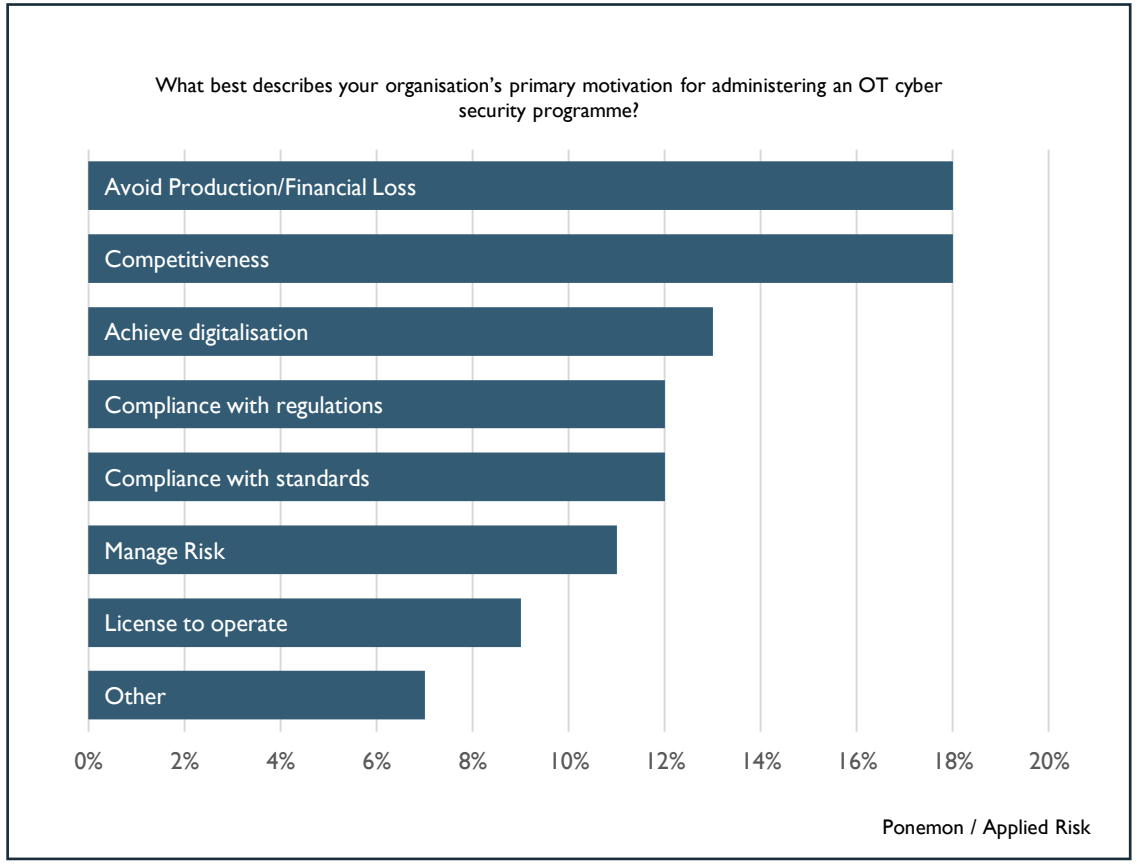
Risk

There is a growing understanding of the business risk which may result from a cyber incident, and this is leading to increased investment.

Risk to OT needs to be expressed in terms of the reliability and availability of operating systems and safety to workers and customers. Compromise to availability and safety = high risk

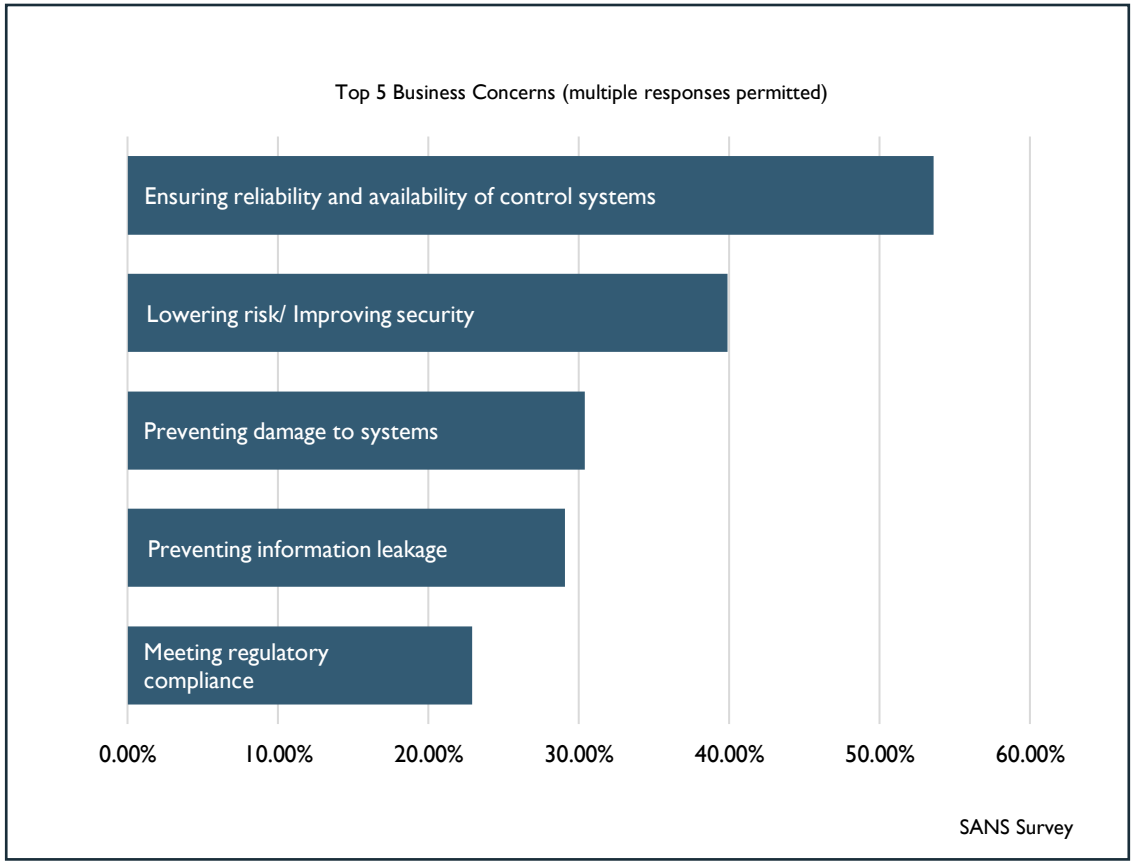
WESTLANDS ADVISORY

Industrial operators are principally concerned with Reliability, Availability and Maintainability of operations



OT cybersecurity investment drivers are usually a blend of factors related to regulation, availability (risk) and digitalisation. Engineering teams will be mostly concerned with ensuring 99.999% availability of systems with investment in DX and implementation of regulation having to fit with engineering priorities rather than vice versa.

Meeting regulations is a lower concern though priorities change according to who answers the question

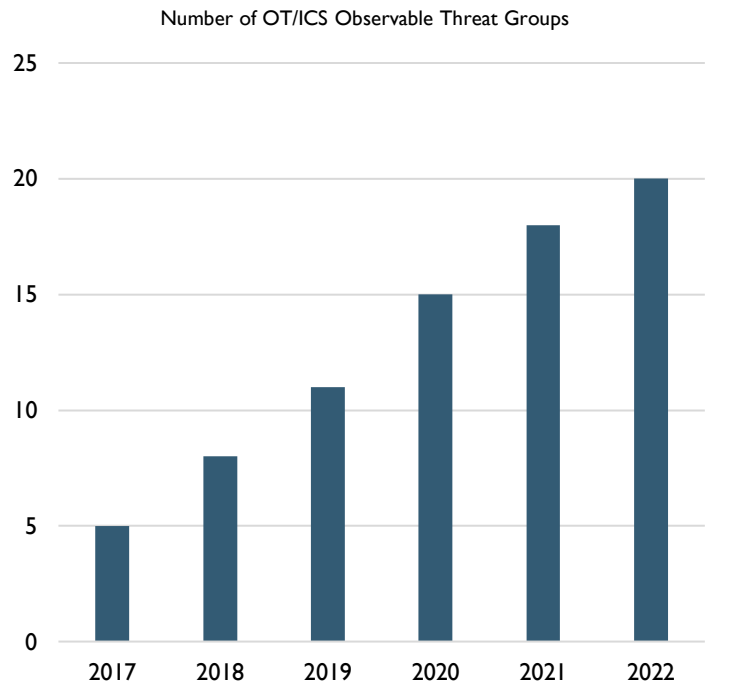


Whilst reliability and availability is of critical importance to engineering teams, the increasing convergence between IT and OT means that priorities differ according to the stakeholders involved in implementing programs. Risk officers and CISO's will be more concerned with compliance and information leakage than engineering teams.

Risk continues to be influenced by high threat levels, new vulnerabilities and the growing number of ransomware incidents

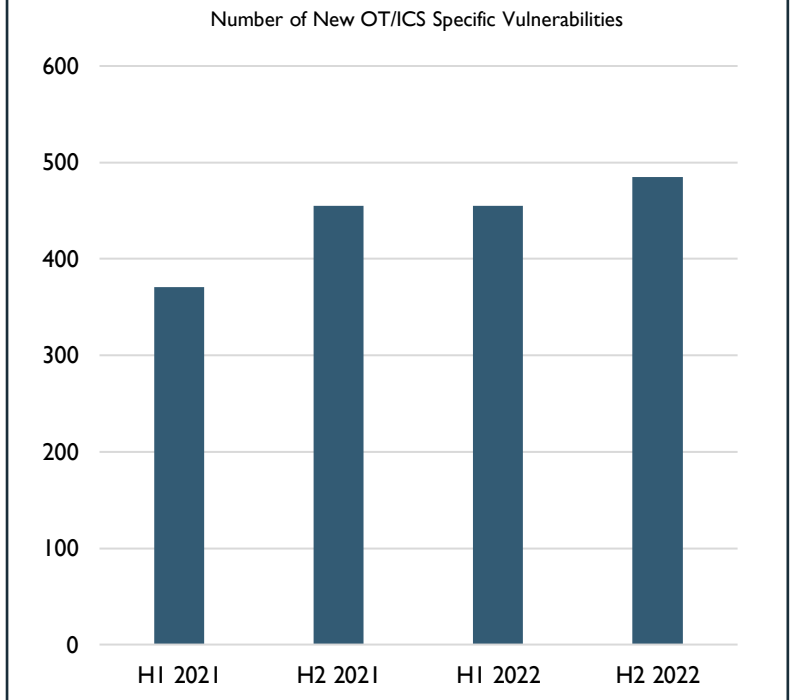
WESTLANDS ADVISORY

The number of observable ICS threat groups has increased



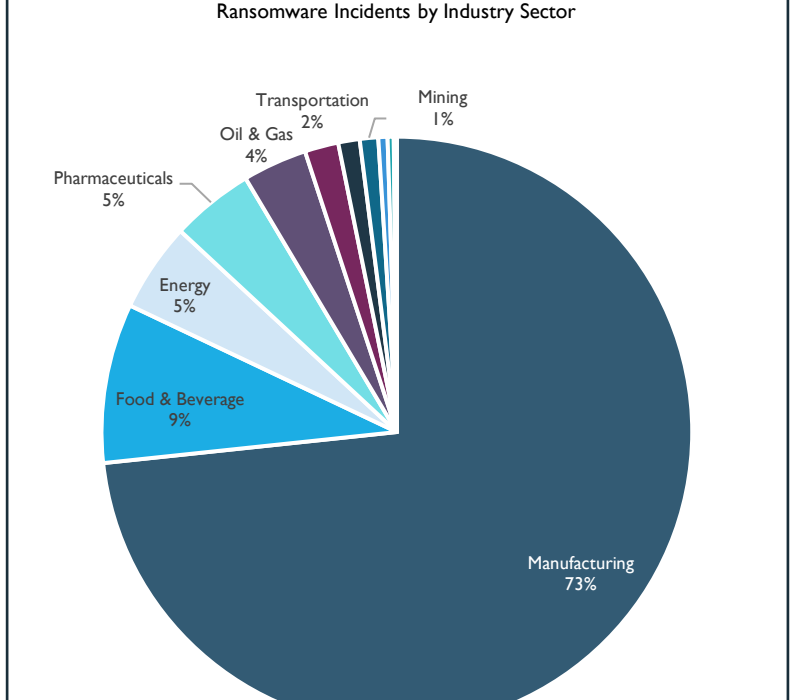
The number of threat groups connected to OT is slowly increasing. This profile is unlikely to change due to the current direction of geopolitics.

Newly discovered vulnerabilities remains high



ICS specific vulnerabilities discovered each year has grown partly due to the additional resources dedicated to discovering them. Evaluating vulnerabilities – old and new – and mitigating them is important to understanding current and future risk.

Ransomware is consistently cited as the greatest threat to manufacturing firms with a high annual increase in incidents reported

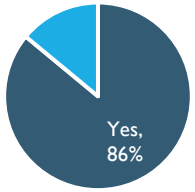


Ransomware is a threat across all OT sectors. The number of reported incidents by segment is closely aligned to the respective industry size.

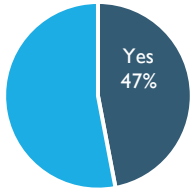
Cyber Risk strategy is increasingly concerned with ensuring supply chain resilience which is becoming a more substantial requirement in regulation.

WESTLANDS ADVISORY

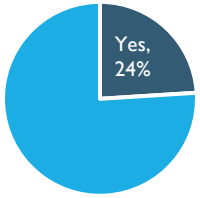
3rd party risk management lacks dedicated resource …



Percentage of EU companies with a 3rd Party Risk Management Policy



Percentage with a dedicated 3rd Party Risk Management Budget

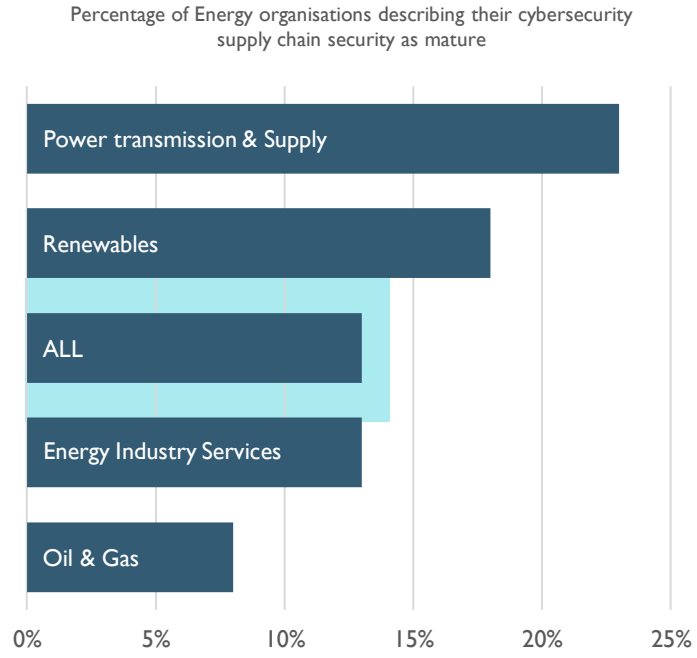


Percentage with dedicated 3rd Party Risk Management Staff

ENISA

Supply chain cybersecurity is an important requirement within NIS2. ENISA evaluated attitudes to 3rd party risk management as part of the implementation and found that there is little dedicated resource responsible for managing supply chain risk and that cybersecurity was not a major consideration.

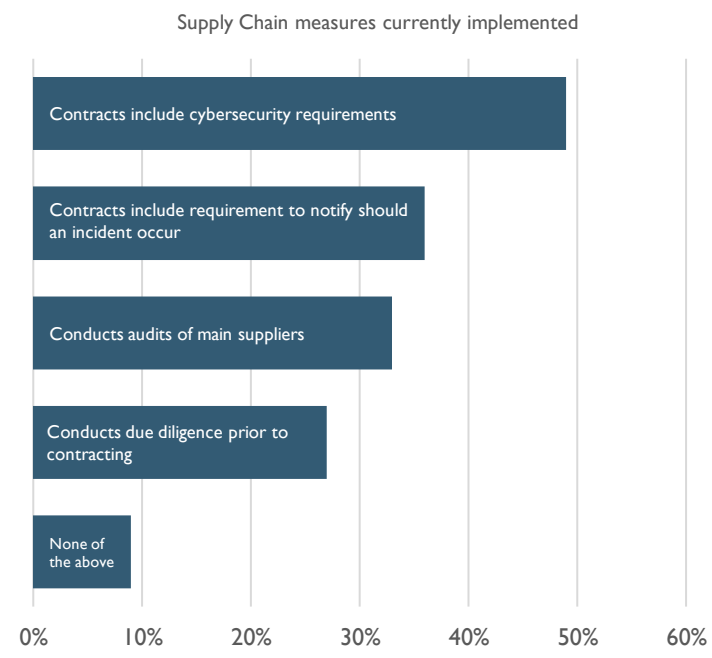
… and is at low levels of maturity …



DHV

The low level of cybersecurity maturity is likely to improve over the forecast period as regulators place responsibility on asset owners to ensure supply chain partners are compliant with cybersecurity requirements outlined in regulation.

… with organisations implementing a relatively low number of controls.



Ponemon / Applied risk

Industries reliant on global supply chains and using high levels of IT and communication technology in their products, such as the automotive industry, are more mature than other industries. A focus on SBOM and more rigorous testing of 3rd party products on delivery is expected.

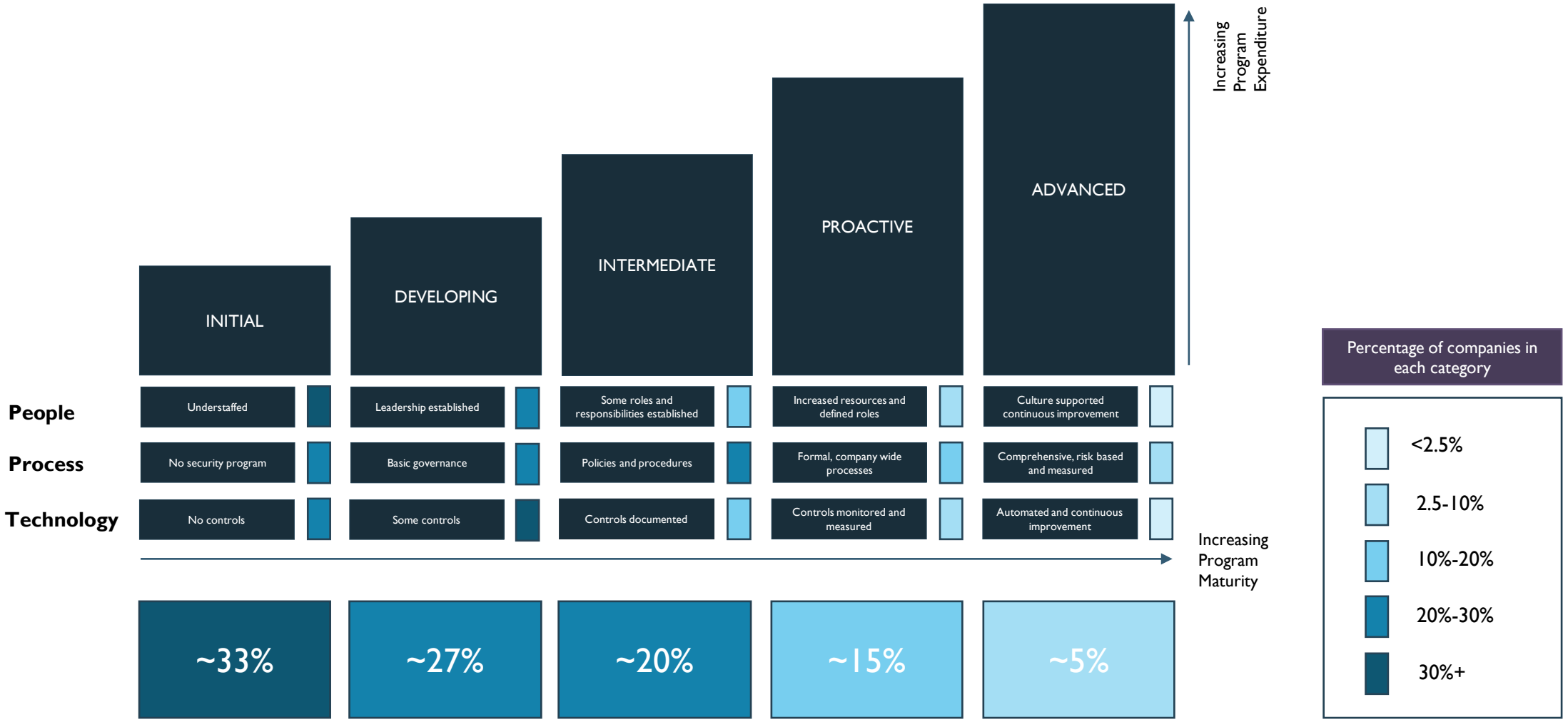
Industrial Cybersecurity Maturity & Buying Personas

WESTLANDS ADVISORY

Summary

1	OT cybersecurity maturity remains low, though there is significant variance in security programs both between and within industry sectors. Nevertheless, there is a growing installed based of OT security detection programs.
2	Awareness of OT cybersecurity risks continues to increase at a Board level and amongst management and operational teams. However, a lack of staff and skilled cybersecurity personnel is a challenge to advancing cybersecurity programs. Improving awareness through communicating risk and increasing the skill level remains a significant industry requirement.
3	Most asset owners need to make improvements to processes, implement robust cybersecurity supply chain management, and address inadequate incident response planning. Without security automation, supply chain management and incident planning, asset owners are falling short of achieving operational resilience.
4	Ownership of the OT cybersecurity challenge differs by industry. However, the role of the IT CISO in decision making is growing with OT engineering leadership responsible for the problem and implementation of the program.

OT Cybersecurity maturity related to People, Processes and Technology remains low though there are advances in regulated, critical process industries

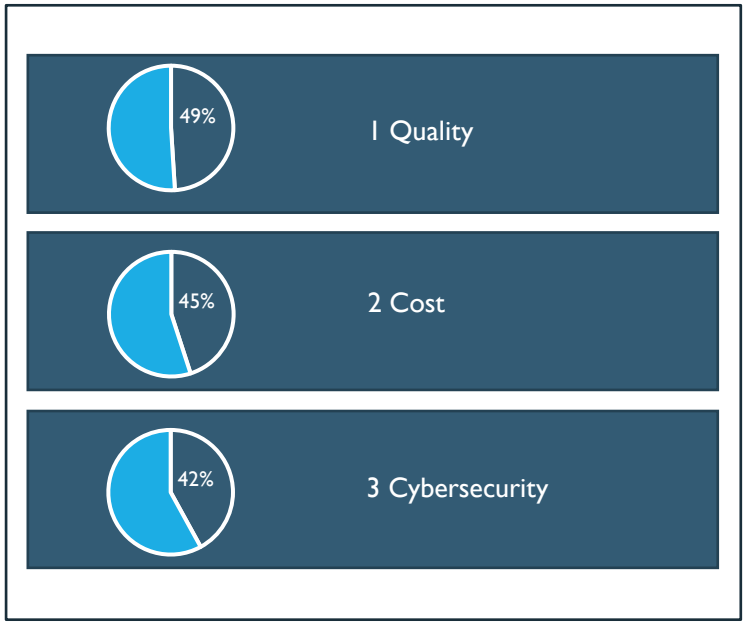


Methodology based on sourcing, classifying, and modelling a variety of industry surveys.

Cybersecurity awareness continues to increase along with budgets, though challenges remain with implementing and advancing programs quickly including lack of skilled personnel

WESTLANDS ADVISORY

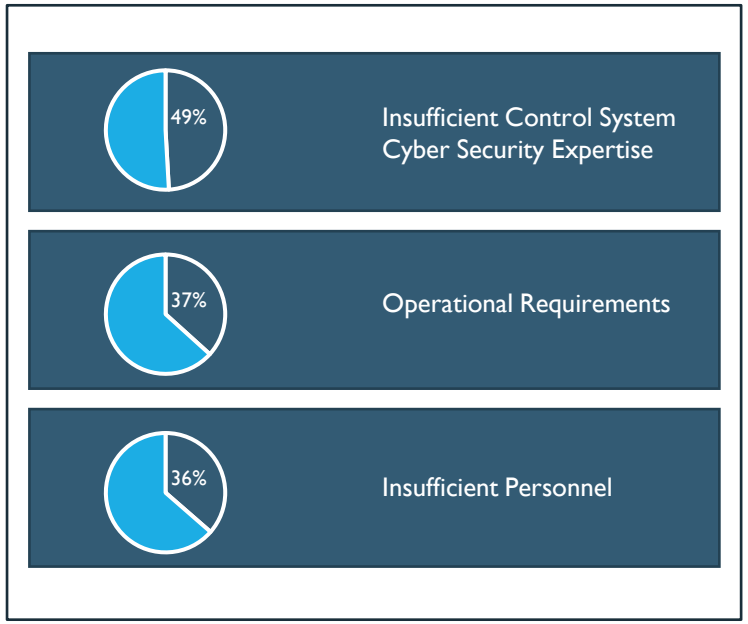
Cybersecurity remains a top 3 board priority in manufacturing



Cybersecurity ranks higher with larger organisations and in regulated and critical manufacturing sectors

PwC COO Survey

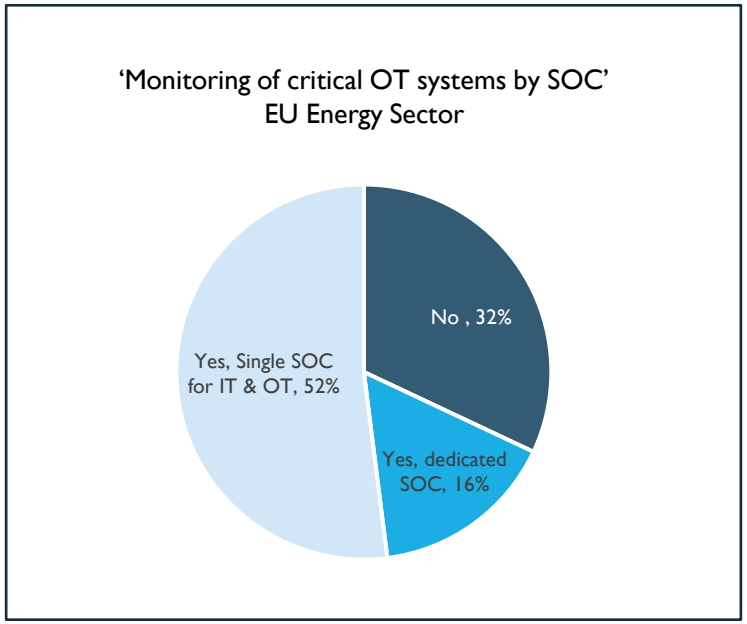
Significant challenges to advancing security programs. Top 3 cited challenges



Insufficient Threat Intelligence ranked 4th

(CS)2AI KPMG Survey

Maturity remains low even in the EU with regulated industries like energy



Operators without a SOC may well still be using detection tools whilst those with SOC's do not necessarily have detection and incident response capabilities (30% of those with a single SOC)

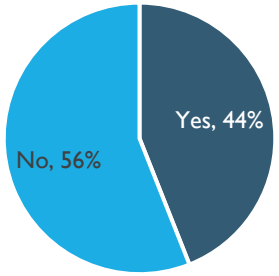
ENISA

People maturity in a 'typical' OT cybersecurity operation remains relatively low, lacking leadership commitment, personnel and skilled staff

WESTLANDS ADVISORY

Cybersecurity staffing levels are below what is perceived as necessary…

Do you have enough staff to manage risk?

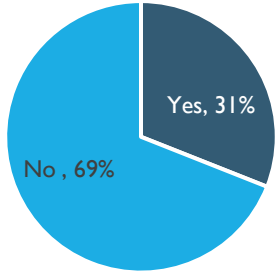


A shortage of skills has resulted in high demand for OT cybersecurity expertise. This is benefiting managed security services firms who are able to provide access to expertise.

Ponemon

… awareness of processes appears to fall short of what is needed …

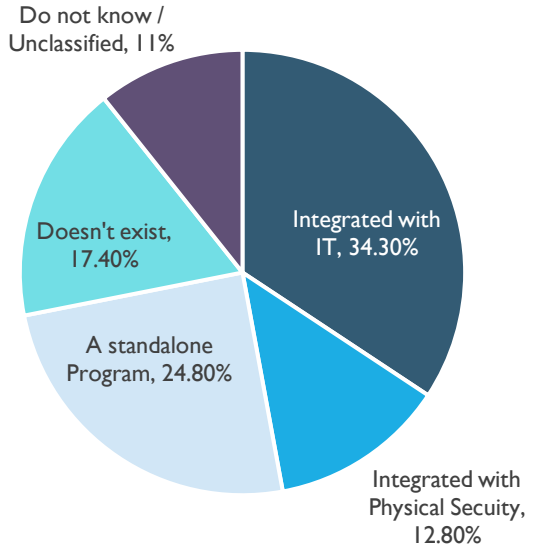
Would you know exactly what to do if concerned about a cyber attack?



Processes become ineffective if poorly implemented and communicated and is common among less mature cyber operations.

DHV

… whilst there is a lack of OT cybersecurity specific training and development.



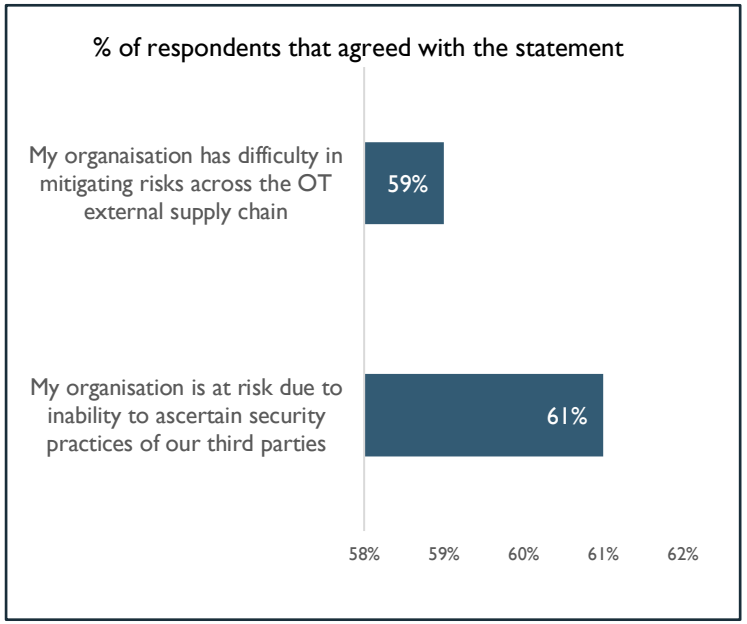
Ongoing OT cybersecurity training is an essential component of security programs but are rarely implemented as a standalone program.

WA Analysis based on (CS)2AI KPMG Survey

Process maturity is improving though organisations remain behind the curve with regards to supply chain risk and incident response

WESTLANDS ADVISORY

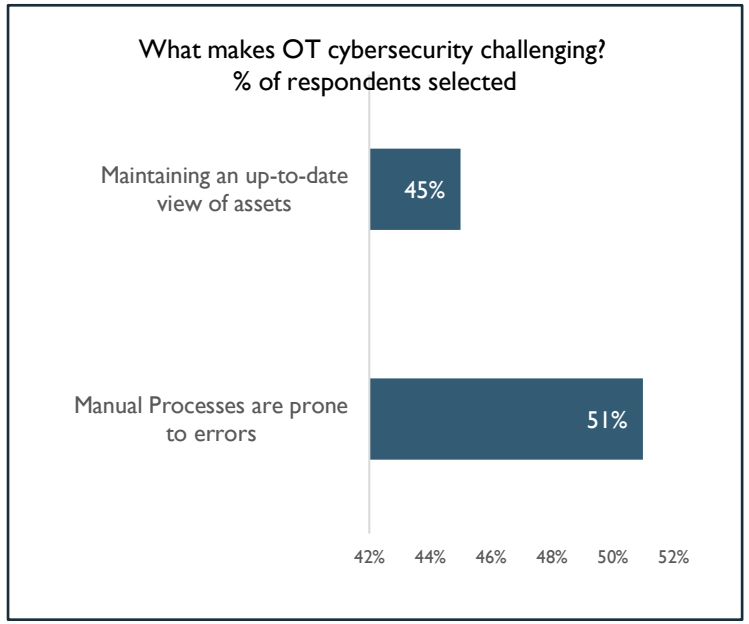
Asset Owners struggle to implement and manage processes to manage third party risk



Regulation, including NIS2 is increasing the focus on supply chain maturity and putting the onus on asset owners to ensure they are using 'secure by design' products from cyber mature partners. This is a significant undertaking for many firms with no dedicated roles or budget assigned.

Ponemon & Applied Risk

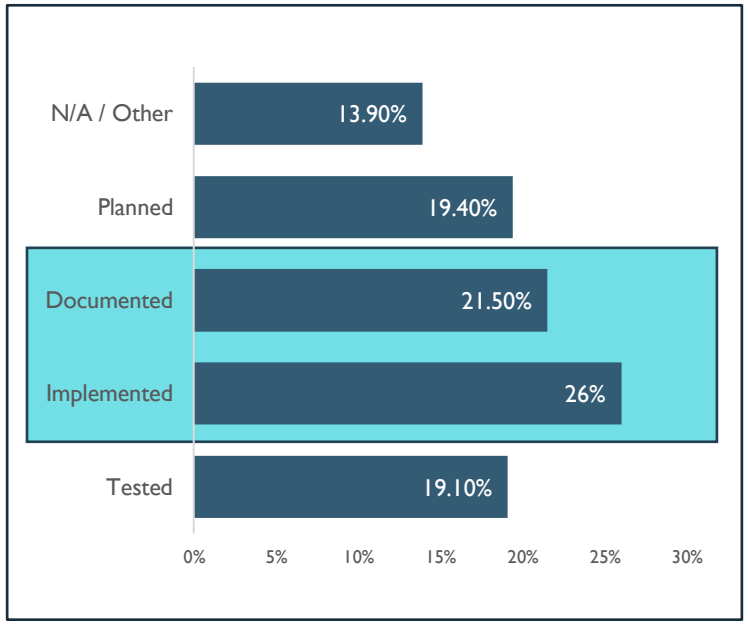
Some processes are still manual and prone to error whilst asset management practices are less than mature.



Policies and procedures, where present, are still dependent on manual process. Without staff training these are prone to error. Equally, identifying and managing assets requires automated policies and procedures.

Ponemon & Applied Risk

There is a lack of Incident Response maturity



Under 50% of respondents have implemented or documented cybersecurity Incident Response plans.

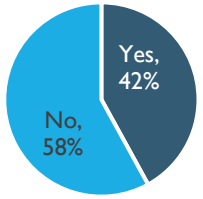
WA Analysis based on (CS)2AI KPMG Survey

Technology maturity is improving though automation, orchestration and machine learning concepts are largely underutilised.

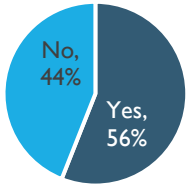
WESTLANDS ADVISORY

The current installed base of technology is low when compared to IT, and not always used effectively

Use of OT Threat Intelligence



Use of Detection & Containment Technologies

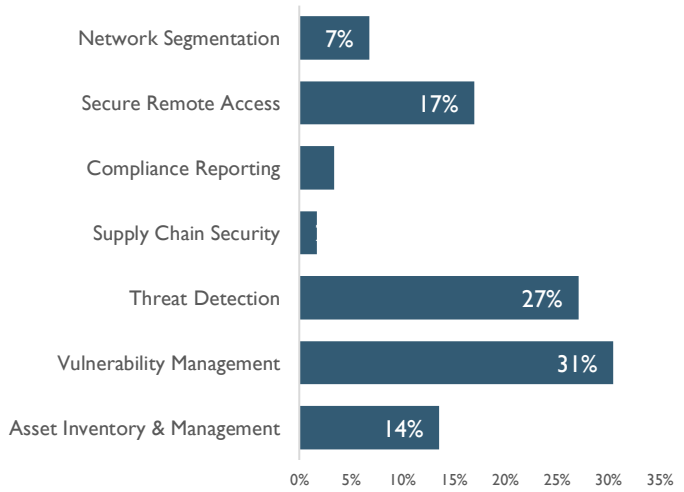


A larger installed base of detection technology is expected over the next 5 years including use of vendor, third party and industry specific threat intelligence.

DHV

Plans to invest in asset inventory, threat detection, VM and RAM confirm the low level of adoption

Which security solution will you invest most in?

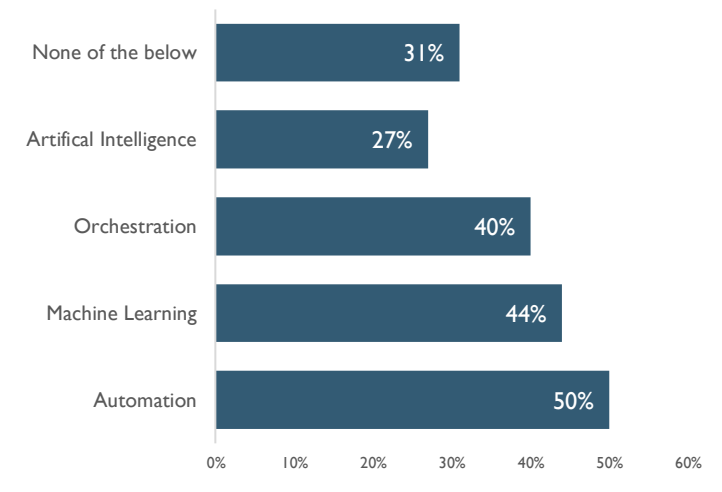


Asset Management and Threat detection investment is stronger in less mature organisations. More advanced programs are already leveraging the tools and lean towards network segmentation as a priority.

(CS)2AI KPMG Survey

Security automation, machine learning and orchestration improvements

What technology do you use?



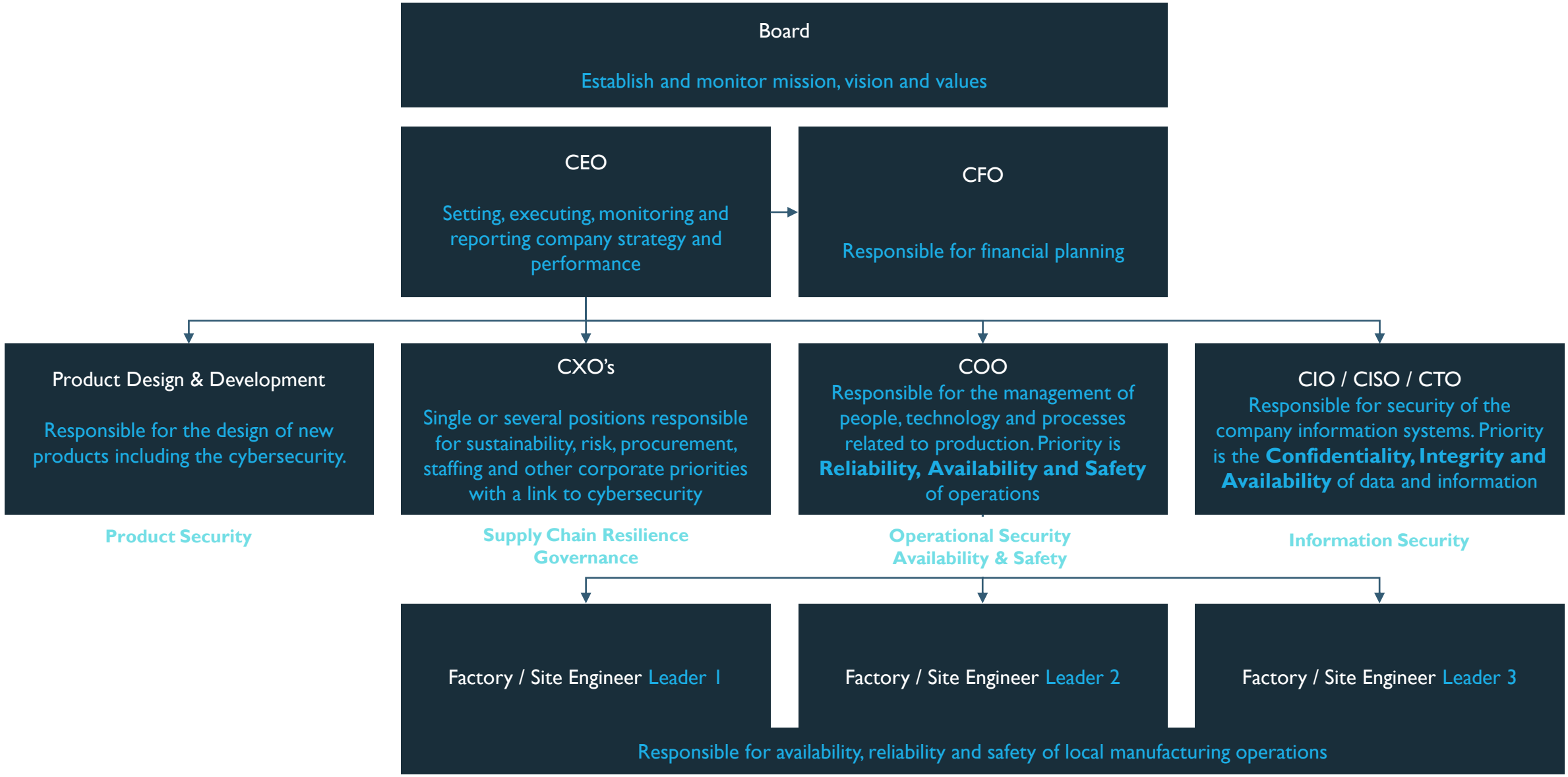
The use of advanced technologies remains relatively low with the majority of organisations still not using machine learning and orchestration.

Ponemon & Applied Risk

Organisational complexity and different priorities can act as a barrier to fast implementation of OT cybersecurity programs with organisations struggling to assign ownership of OT cybersecurity

WESTLANDS ADVISORY

Simplified Example of 'Typical' Large Industrial Company



OT Cybersecurity requires knowledge of assets, industrial networks, and cybersecurity principles which often reside in different teams. Collaboration is critical to program success

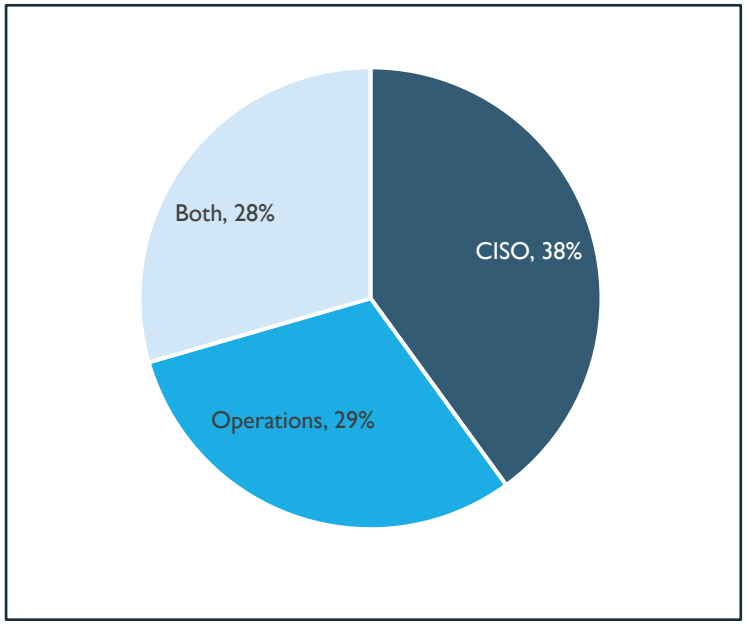
WESTLANDS ADVISORY

Function	IT	OT	Product Development
Responsibility	Responsible for ensuring that IT networks provide the QoS expected by staff, partners and customers including the confidentiality, integrity and availability of data.	Responsible for production targets, ensuring that systems are reliable, available and safe.	Responsible for new products and delivering against security design principles including protecting data in transit and unauthorised access and modification.
Operational Priorities	Confidentiality Integrity Availability	Reliability Availability Maintainability Safety	Confidentiality Integrity Availability
Leadership	CIO / CTO CISO IT Security Management	COO VP Engineering Plant Manager	COO VP Engineering Plant Manager

Leadership, financing and management of OT cybersecurity varies greatly by asset owner; identification of a cross organisational team with clear responsibilities is key

WESTLANDS ADVISORY

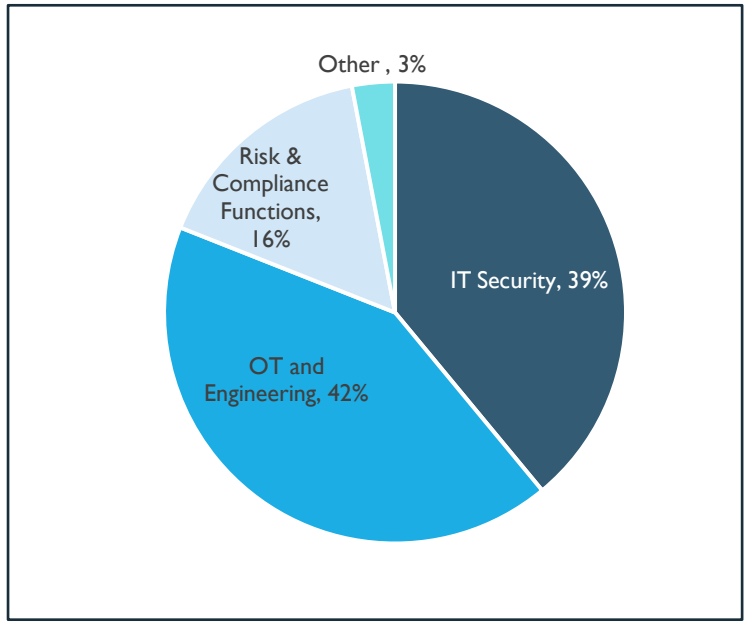
Analysis suggests that CISOs often have responsibility for the OT cybersecurity budget…



The CISO team usually holds the budget and this appears to be a growing trend as IT and OT operations converge. CISO involvement is particularly strong in multi-site, international engagements.

Industrial Defender Survey

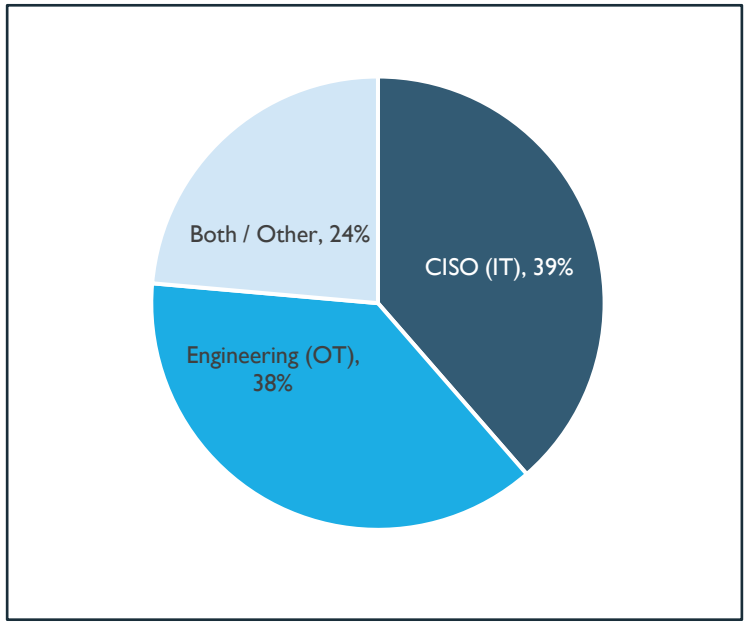
… whilst engineering owns the problem including implementation and management of OT security operations



The engineering team will remain a key stakeholder and is often responsible for the implementation and management of OT cybersecurity.

Ponemon Survey

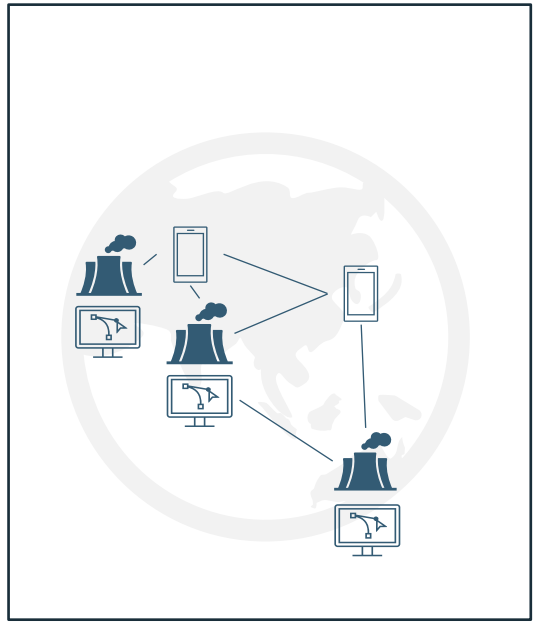
However, boundaries are blurred and ownership of OT cybersecurity is often mixed



Responsibility for OT cybersecurity is mixed and occasionally the responsibility of an IT & OT decision making unit. Other influencers may include the CTO or Product Engineering with an increasing focus on Secure by Design.

Westlands Advisory Analysis

OT Cybersecurity is becoming a strategic investment; decision making is moving to the CXO but delivery includes a network of stakeholders

Type 1: Protect the Operational Technology	Type 2: Protect the IT and OT across the local operation	Type 3: Protect OT at plants internationally	Type 4: Protect my business operations
			
Site Engineer Manager	Site IT Director	Global Engineering Leader; COO / CISO	COO / CISO; Board
Lower Cost Lower Complexity Decentralised Decision Making			Higher Cost Higher Complexity Centralised Decision Making
Proof Of Concept (POC)			Global Program

Source: Westlands Advisory

Decision making and responsibilities differs widely depending on the company size, industry sector, maturity of the security program and number of sites asset owners are managing

WESTLANDS ADVISORY

Single Site, Critical Infrastructure

Objective: Improve OT Cybersecurity Maturity

Securing Critical infrastructure challenge is often complicated by the need for 99.999% availability which means security needs to be implemented and managed by teams with deep knowledge of OT systems. In this example the single site, OT security focus of the projects means it's likely that the COO or Engineering team will be the main stakeholders.

Board	I
CEO CFO	I
CIO CTO CISO	C
COO	A
Site Engineer	R

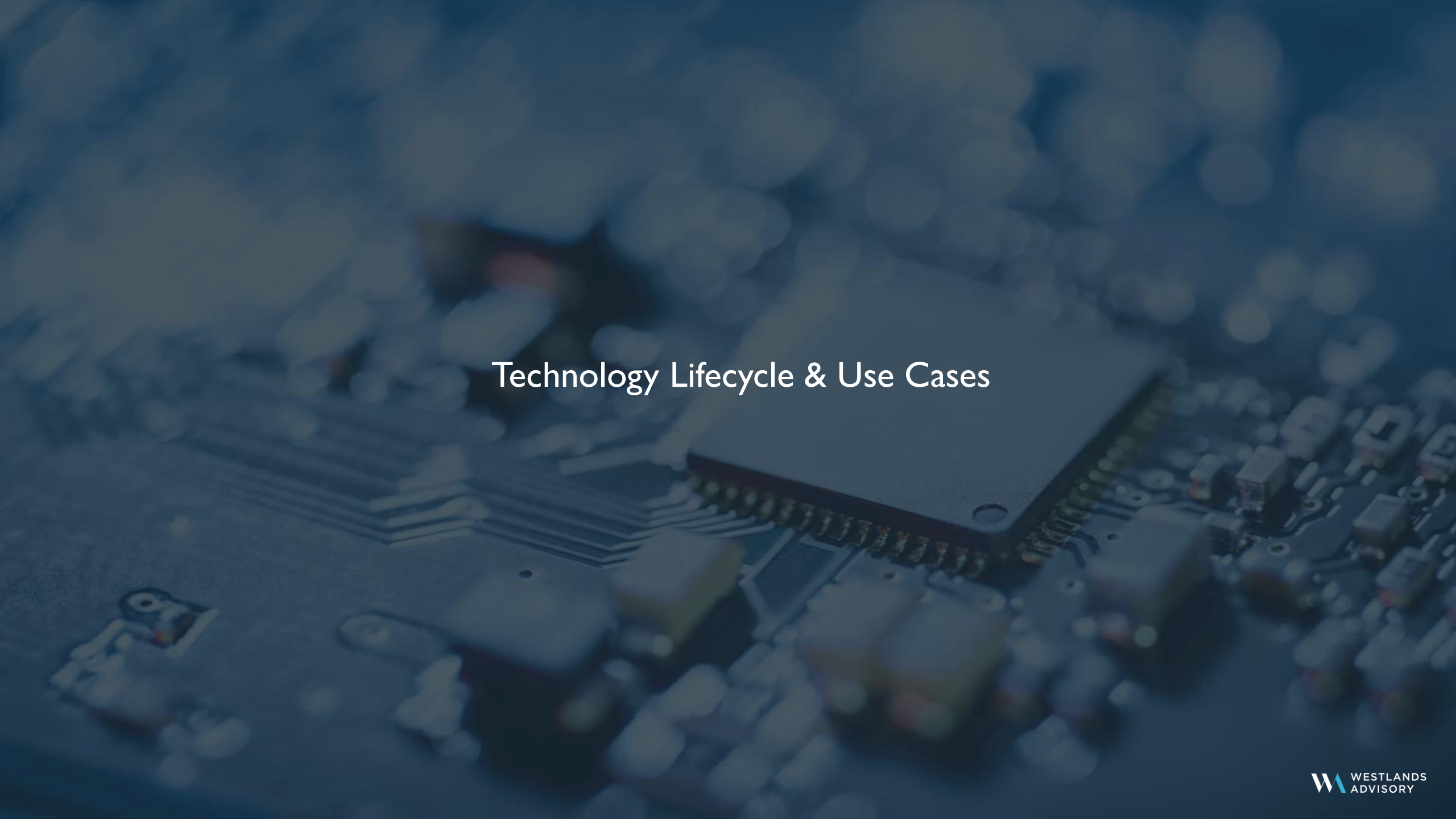
Multiple Sites, Manufacturing

Objective: Accelerate IT/OT Convergence and establish unified security operation

Research highlights that as projects move from single site to organisation wide implementation of a converged IT/OT security operation, Accountability moves to the CISO team whilst engineering is consulted and a key partner on the security transformation.

Board	I
CEO CFO	C
CIO CTO CISO	A
COO	C
IT Engineer	R
Site Engineer	C

R	Responsible
A	Accountable
C	Consulted
I	Informed


Technology Lifecycle & Use Cases

Summary

1	Asset Visibility remains a key goal for asset owners and the starting point for security programs. Innovation includes integration with CMDB's to improve asset management, and the use of machine learning to automatically classify assets, detect configuration changes or deviations from the baseline. ML innovation also includes quantifying risk and prioritising actions.
2	There is growing use of cloud services for OT cybersecurity. This includes the use of agent and agentless solutions that enable visibility and detection in centralised cloud platforms using threat intelligence and security analytics. Cloud based analytics control platforms often integrate from cloud and on-prem appliances, centralising and enriching data collection. Most vendors now offer on-prem and cloud solutions to provide customers with choice.
3	IT/OT convergence continues to mature, and asset owners seek improved efficiency, visibility and centralisation of security policy and processes. This is driving technology innovation. Yokogawa OpreX IT/OT SOC is an example of an OEM developed solution developed to unite IT and OT operations, delivered as an elastic cloud with automated and orchestrated incident response tooling.
4	The concept of operational resilience continues to influence technology and service innovation. The ability to identify and recover quickly from a cybersecurity incident has shifted the focus slightly from protection to proactive threat hunting and incident response planning. This includes a range of innovations including OT cybersecurity attack simulations, OT playbooks, staff training and a greater focus on supply chain resilience.
5	OT cybersecurity platforms are expanding coverage to more use-cases, including more tools and integrations. This is being driven by the customer requirement for consolidation, simplification and integration of security tools, and reduction in the number of vendors. IT/OT convergence will likely result in growing partnerships between IT and OT vendors.

Aligning Products and Definitions with the Project Segmentation

	Network Protection	Network Access	Visibility & Threat Detection	Risk & Vulnerability Management	Endpoint Protection & Detection	Advanced Threat Protection	Remote Access Management	Security Operations
In scope	Industrial Firewalls	NAC	Visibility	Vulnerability Management	Industrial Endpoint Protection	Sandbox	Remote Access Management	SIEM
	NGFW		Threat Detection	Configuration Management	EDR	CDR		SOAR
	Unidirectional Gateway / Data Diode		Network Detection & Response	Compliance Management				
			Deception	Risk Management				
				Continuous Controls Monitoring				
	Professional Security Services							
	Managed Security Services							
Out of scope	Switches			Configuration Management Database (CMDB)				
	Routers			Software Bill of Materials (SBOM)				
	Wireless Access Points							

Note regarding Threat Intelligence

- Vendor threat intelligence, often provided as a subscription for Threat Detection, is included in the product definitions and is in the project scope.
- *Third party intelligence provided as a service by managed security service providers is included in Managed Security Services.

OT Network Protection

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
Industrial Firewalls	Industrial Firewalls, also referred to as OT network appliances, are ruggedised firewalls typically deployed at Purdue model layers 1 and 2, delivering network segmentation to prevent lateral movement between cell zones. Industrial Firewalls differ from enterprise firewalls due to 1) ruggedised features enabling reliable performance in harsher operating environments and 2) monitoring and deep packet inspection of industrial protocols including Modbus and PROFIBUS. Additional functionality may include IPsec to enable secure, encrypted communication between devices and the creation of VPNs for remote access.	• Belden (Eagle 20/30/40 and Tofino Xenon) • Check Point (1570R Security Gateway • Cisco (ISA3000) • Fortinet (Fortigate Rugged) • Palo Alto Networks (PA-220R)	Typically deployed at layers 1 & 2 in the Purdue model, both between the process control and local control room level, and between manufacturing cells. OT Security Solution	Sustained Growth	• Security operations and management • Network protection and threat detection including Deep Packet Inspection (DPI) • Network segmentation • Virtual Private Networks • Investigation and forensics	The total revenue generated by vendors through the sale of hardware, subscriptions and virtualised solutions direct to the end-use customer or more commonly through channel partners including OEMs and system integrators.
Next Generation Firewalls (NGFW)	Next Generation Firewalls are mainly deployed in the DMZ between Purdue layer 3 and 4 to enforce policy, monitor and filter IT/OT traffic. Typically these are not ruggedised. NGFW's filter packets, either forwarding or dropping packets based on source IP address or destination, TCP/UDP source or ICMP message type. Stateless firewalls filter packets at OSI layer 3 or 4 whereas Stateful firewalls compare packets to a session table and stop traffic based on the set rules. NGFW's incorporate IDS/IPS. The IDS will detect vulnerabilities and exploits against targeted endpoints or servers and by definition is a passive security tool, listening without taking action other than alerting the SOC analyst to any anomalies. The IPS is placed in-line with the network traffic and will take action, either terminating the TCP session, reconfiguring the firewall, and removing any malicious content. NGFW also inspects encrypted traffic (SSL), performs DPI, and provides Application Control. Rules are set based on signatures, anomalies or policy. Additional redundancy is required in industrial applications to ensure back-up if a firewall is compromised. It is not uncommon for the customer to use two different vendors in this set-up.	• Check Point (Quantum series) • Cisco (1000, 2100, 3100, 4100 series) • Fortinet (Fortigate series) • Palo Alto Networks (PA-3200, PA-3400, PA-5200, PA-5400, PA-7000 series)	Typically deployed in the DMZ between layers 3 & 4, protecting network connectivity between IT and OT. They can also be deployed at layer 2. IT/OT Security Solution	Sustained Growth	• Threat Detection and blocking • Policy enforcement • Network segmentation and monitoring • VPN aggregator • Application control • Deep Packet Inspection (DPI)	The total revenue generated by vendors through the sale of the firewall appliance to channel partners and integrators. This includes related subscriptions including maintenance and services.
Unidirectional Gateway	A unidirectional gateway, or data diode, is a hardware appliance deployed between two networks to allow information to move in one direction. Data diodes have become increasingly used within industrial applications to allow data to move from OT to IT networks but not the other way, protecting the operational environment.	• Cyber Owl "OPDS-100D" • NCC / Fox IT "DataDiode" • OPSWAT "Netwall USG" • Waterfall "WF-500"	Typically deployed between IT and OT although it is also deployed at lower levels in some instances. OT & IT/OT Security Solution	Sustained Growth	• Network security • Data security • Network segmentation • Compliance management	The total revenue generated by vendors direct to the end-use customer or more typically revenue received from OEM integrated services or other channel partners.

Industrial Networking

	Product Definition	Example Vendors	Market Revenue Definition
Industrial Switches	Industrial Ethernet Switches connect together industrial devices and servers into a Local Area Network using TCP/IP protocol, enabling real-time communication between devices. Switches can be managed or unmanaged, and either Layer 2 or Layer 3, with a variety of port configurations to meet a wide range of industrial requirements. Industrial Switches are typically ruggedised to meet harsher operating conditions which may require additional waterproofing, protection from extreme temperatures or excessive vibration. Due to the high availability requirements of manufacturing processes, Industrial Switches also have redundant power inputs for back-up power.	• Belden • Cisco • Fortinet • Siemens	Not included within the scope of this analysis. Definition has been included for completeness.
Industrial Wireless Access Points (WAP)	A Wireless Access Point enables wireless enabled devices to connect to a wired network. Various configurations enable industrial operators to connect to wired LAN's, extend the current range of the network to provide additional coverage, and bridges to connect multiple networks. Industrial versions are typically ruggedised, with durable coverings and the capability to withstand higher temperature ranges.	• Cisco • Fortinet • Moxa • Siemens	Not included within the scope of this analysis. Definition has been included for completeness.
Industrial Routers	Industrial Routers connect computer networks through routing IP packets, controlling data traffic through either wired, WI-FI or cellular connectivity.	• Advantech • Cisco • Siemens	Not included within the scope of this analysis. Definition has been included for completeness.
Industrial Gateways	Industrial Gateways, or IoT Gateways, join dissimilar networks together that rely on different protocols. The network is often external to the organisation, providing connectivity between ICS and the cloud. Gateways and routers can be combined into a single solution.	• ABB • Cisco • GE • HMS Networks "Anybus" & "Ewon" for remote monitoring • Ixon "IXrouter" • Siemens	Not included within the scope of this analysis. Definition has been included for completeness.

Network Access Control

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
Network Access Control (NAC)	NAC adds policies to the network for controlling access by devices and users, ensuring network visibility (what's on the network), access control (who can access it) and compliance (company risk and regulatory compliance). Orchestration ensures that non-compliant devices are denied access, quarantined or given restricted access. Features include policy enforcement for multiple operating scenarios, user profiling, guest networking access, compliance management and incident response. Asset classification and management, effective detection and timely, automated response, are key competitive considerations.	• Cisco "IoT Threat Defence" • Forescout "eyeControl" • Fortinet "FortiNAC" • HPE (Aruba Networks)	NAC is typically deployed in the DMZ or at layer 3 depending on the site architecture OT & IT/OT Security Solution	Sustained Growth	• Network visibility and control • Access Management • Asset grouping, segmentation and management • Compliance and reporting • Threat detection and remediation • Privilege management	The total revenues generated by the vendors selling direct to end-use customers or to channel partners. This includes the hardware appliance, virtual appliance or SaaS and associated support services.

Visibility & Threat Detection

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
Visibility	Network discovery is essential to ensuring good cybersecurity practices and is often the starting point in a cybersecurity program as it allows organisations to map physical and digital assets, establishing further device information including IP address, device type, function, firmware etc. This in turn helps operators to identify vulnerabilities, establish operational risk, and prioritise necessary actions. There are several methodologies used to map the network including passive network scanning of switches, active network scanning, agent based discovery and several others.	• Armis "Asset Management" • Cisco "Cyber Vision" • Claroty "xDome" • Dragos "Asset Visibility & Inventory" • Forescout "The Forescout Platform" • Hexagon "PAS OT Integrity" • Honeywell "Forge Cybersecurity Suite" • Industrial Defender "Asset Management" • Microsoft Defender for IoT • Nozomi "Asset Intelligence" • OPSWAT "Neuralyzer" • Radiflow "Visibility & Anomaly Detection" • Tenable "tenable.ot" • Verve Platform	Typically deployed at Level 3 and lower to map network devices from Level 1-3 OT Security Solution	High Growth	• Asset identification • OT Systems visualisation and management • Operational health monitoring and alerts (errors, malfunctioning devices) • Change detection	The total revenue generated by vendors direct to the end-use customer or to channel partners and excluding additional professional services.

Visibility & Threat Detection

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
OT Threat Detection	Threat Detection usually combines a range of methodologies to identify deviations from the expected device or network behaviour and can be effective at identifying unknown threats such as zero days. Anomaly Detection relies on different methodologies including signature-based and behavioural analysis. Threat Detection is commonly sold as an additional service to asset discovery and vulnerability management. Cloud and On-Prem deployment options are now common place. Most vendors have integrations with SIEM, Firewalls vendors and strategic relationships with OEM vendors and managed service providers.	• Armis "Threat Detection & Response" • Cisco "Cyber Vision" • Claroty "CTD – Continuous Threat Detection" • Dragos "Threat Detection" • Forescout "eyeInspect" • Microsoft Defender for IoT • Nozomi "Guardian" • OPSWAT "Neuralyzer" • Radiflow "Visibility & Anomaly Detection" • SCADAfence Platform • Tenable "tenable.ot"	Typically deployed in the DMZ or at Level 3 and below depending on the architecture. OT Security Solution	High Growth	• OT security risk analysis • Early threat detection (reduced MTTD) • Response (reduced MTTR)	The total revenue generated by vendors direct to the end-use customer or to channel partners and excluding additional professional services.
Network Traffic Analysis, Detection & Response (NDR)	NDR has evolved from network traffic analysis and monitoring to a proactive security operations tool using machine intelligence to detect anomalies and automate response based on playbooks. This may include dropping traffic, quarantining and collecting forensic evidence. NDR differs from Endpoint Detection & Response (EDR) by its wider coverage, inspecting network traffic from OSI layers 2-7 but unlike EDR it does not deploy endpoint agents and therefore can be less effective in remote working applications. The segment has a wide range of vendors with different strengths in traffic analysis, delivering low false positive anomaly detection, and providing strong incident response.	• Cisco "Stealthwatch" • DarkTrace "OT" • Honeywell "AMIR" • IronNet Platform • Trellix "NDR" • Vectra Platform	IT/OT Solution providing threat detection across enterprise and effective at Level 3.	High Growth	• Insider threat detection • Employee monitoring • User behaviour monitoring • Threat detection • Threat hunting • Investigation • Compliance • Network traffic analysis and management	The total revenue generated by vendors through annual sales of NDR technology direct to end-use customers, through integration and channel partners.
Deception Technology	Deception Technology in OT networks is an emerging use-case and not widely deployed. Deception works through deploying lures to deceive attackers who have penetrated the network, alerting the security operations team to unusual activity on the network. Lures include false OT devices and jump servers.	• Fortinet "FortiDeceptor" • Illusive Networks "Attack Detection Systems" • Attivo "ThreatDefend Platform"	Typically deployed in the DMZ or at layer 3 depending on the site architecture. OT Security Solution	Early	• Hide and protect high value assets • Detection (lower MTTD) • Active Response (low MTTR) • Forensics	The total revenue generated by vendors direct to the end-use customer or through channel partners. Excludes professional service revenue.

Risk & Vulnerability Management

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
Vulnerability Management	Vulnerability Management platforms, also referred to as Risk Based Vulnerability Management (RBVM), scan enterprise networks and applications for known vulnerabilities (Common Vulnerabilities & Exposures) and to create a CVSS score (Common Vulnerability Scoring System) to help prioritise risk, remediation and reporting. Platforms have evolved from simply identifying and patching to providing more context through integrating threat intelligence so that actions are prioritised according to the severity of the risk.	• Armis "Asset Vulnerability Management" • Cisco "Cyber Vision" • Claroty "xDome" • Dragos "Vulnerability Management" • Forescout ""The Forescout Platform" • Honeywell "Forge Cybersecurity Suite" • Hexagon "PAS OT Integrity" • Industrial Defender "Vulnerability Management" • Langer "OT-Base" • Nozomi "Vantage" • OTORIO • Verve "The Verve Security Center" • SCADAfence Platform • Tenable "Tenable.ot"	Typically deployed in the DMZ or at layer 3 depending on the site architecture IT/OT & OT Security Solution	High Growth	• Asset management including scheduling • Security configuration • Vulnerability management • Risk analysis	The total revenue generated by vendors direct to the end-use customer or through channel partners, excluding additional professional services that many include risk assessments, advisory and integration.
Secure Configuration Management	Secure Configuration Management (SCM) is used to adjust and monitor hardware and software settings, aligning security controls with governance and operational objectives which may include adherence to standards. NIST SP 800-128 Guide for Security Focused Configuration Management of Information Systems outlines the requirement to ensure integrity of information systems.	• Hexagon "PAS OT Integrity" • Industrial Defender "CCM" • Tenable "Nessus" • Titania "Nipper" • Tripwire "Enterprise for OT"	Typically deployed in the DMZ or at layer 3 depending on the site architecture IT/OT & OT Security Solution	High Growth	• Configuration management • Minimise vulnerabilities and risk • Forensics	The total revenue generated by vendors through the sale of services to third parties, managed service providers, channel partners or direct to the end-use customer.
Compliance Management	OT Compliance Management is ensuring that company systems and networks are adhering to relevant standards or regulation. Technology will monitor systems to ensure that configuration meets that standards (e.g. NERC CIP, NIST SP 800-82, IEC 62443) and will recommend actions for any deviation.	• Awen Collective "Profile" • Industrial Defender "Compliance Reporting" • Forescout "Compliance Center" • SCADAfence "Governance Portal" • Tripwire "Compliance Solutions"	Typically deployed in the DMZ or at layer 3 depending on the site architecture IT/OT & OT Security Solution	High Growth	• Risk Management • Regulatory Compliance • Supply Chain Compliance • Cyber Insurance	The total revenue generated by vendors through the sale of services to third parties, managed service providers, channel partners or direct to the end-use customer.

Risk & Vulnerability Management

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
Cyber Risk Assessment	The solution generates a risk rating for controls and processes and may also include benchmarks against industry norms and best practices. Cyber Risk Quantification is a foundational product in an Integrated Risk Management program and frequently integrated into GRC platforms. Scoring is generated through the automated collection and analysis of network data, open source data and threat intelligence, to allow organisations to quantify operational risk, including assessing their own security controls and evaluating the cyber risk of third party suppliers and partners. Suppliers compete through the quality of the model and data sources, the reporting, the frequency of delivery and notifications. The product is early in its growth cycle and is expected to become more widely used to inform insurance policy and supplier selection.	• Awen Collective "Optics" • Claroty "xDome" • CyberOwl "Medulla" • OTORIO • Radiflow "CIARA" • SecurityGate.io	Typically deployed in the DMZ or at layer 3 depending on the site architecture IT/OT & OT Security Solution	Early	• Cyber Risk Quantification • Risk Prioritisation • Compliance • Insurance and Brokerage • M&A	The total revenue generated by vendors through the sale of Security Ratings to third parties, managed service providers, channel partners or direct to the end-use customer.
Security Continuous Controls Monitoring	Security CCM provides a security asset register, automating security controls management to ensure that controls are aligned with risk management strategy. Security CCM is part of a broader CCM solution set and integrated into risk management platforms.	• Panaseer "Panaseer Platform"	Typically deployed in the DMZ or at layer 3 depending on the site architecture and integrated with the SOC	Early	• Risk management • Compliance	CCM has not be included in the OT market forecasts due to its early position on the industry lifecycle curve.

Endpoint Protection and Detection

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
Industrial Endpoint Protection	OT systems comprise a significant number of endpoints at Purdue layer 2 and 3, including workstations and servers. Estimates suggest that 20% of ICS endpoints exist at these levels, with the remaining 80% at layers 0 and 1. Protection at layer 2 & 3 is reliant on antimalware to detect and block zero day attacks and ransomware. Endpoint Protection is provided as a service through OEM partnerships (e.g. Emerson & Broadcom/ Symantec, Rockwell & McAfee (Trellix)) or through other channels partners. This category also includes portable malware scanning tools for OT, permitting scanning and removal of malware without installing software on the industrial device.	• Nozomi "Arc" • TxOne "Stellar Protect" • Symantec • Trelliix	Antivirus Servers are typically deployed in the DMZ OT & IT/OT Security Solution	Slowing Growth	• Endpoint discovery • Endpoint patch management • Endpoint protection • Endpoint monitoring and threat detection • Application Whitelisting	The total revenue generated by vendors direct to the end-use customer or more typically revenue received from OEM integrated services or other channel partners.
USB Protection	USB's are required to transfer files and updates to devices and operating systems. USB protection solutions scan and monitor the use of USBs to detect and remove malware.	• OPSWAT • Honeywell • KUB • Symantec		Slowing Growth	• Malware detection • Compliance management	The total revenue generated by vendors direct to the end-use customer or from a channel partner.
Endpoint Detection & Response	EDR is a fast growing product category that has developed from a different approach to security. Traditional endpoint protection is based on methods including virus signatures, and whitelisting or blacklisting IP addresses or applications. EDR solutions deliver active threat detection, including user behaviour analytics, machine learning based detection, network analysis tools, and response orchestration. Key vendor selection criteria, beyond functionalities such as usability, impact on network performance, and cost, includes the MTTD (Mean Time to Detection) and MTTR (Mean Time to Response). MTTD and MTTR are reliant on the strength of the machine learning, automation, threat intelligence and playbooks.	• Check Point • Cisco • Crowdstrike • Fortinet • Palo Alto Networks • SentinelOne • Tanium • Trend Micro	Typically deployed in the DMZ, at Purdue model layer 3 or in the enterprise depending on the architecture OT & IT/OT Security Solution	High Growth	• Threat Hunting including modified files, obfuscated scripts and network attacks • Insider threat reduction • Ransomware protection • BYoD Detection and Monitoring • Data Loss Prevention • Removable media detection	The total revenue generated by vendors through the sale of endpoint detection & response use cases to third parties or direct to the end-user.
Extended Detection and Response (XDR)	XDR is an extension of the Endpoint Detection and Response market segment. EDR is a cloud based platform that monitors endpoints, using analytics and Indicators of Behaviour to detect unusual activity, and providing the response functionality to resolve the event. XDR uses the same principles across the distributed modern IT network, including network and cloud infrastructure.	• Cisco • Crowdstrike • Fortinet • Microsoft • Palo Alto Networks • Trellix	Typically deployed in the DMZ, at layer 3 or in the enterprise depending on the site architecture IT/OT Security Solution	Early	• Insider threat detection • Employee monitoring • User behaviour monitoring • Threat detection • Threat hunting • Investigation • Compliance • Network traffic analysis and management • Endpoint analysis	The total revenue generated by vendors through annual sales of XDR technology direct to end-use customers, through integration and channel partners.

Other Advanced Threat Prevention & Protection

	Product Definition	Example Vendors	Use Cases	Market Revenue Definition
Sandboxes	Sandboxing to detain, investigate and detonate suspected malware in a safe environment.	• Check Point Software • Fortinet • Trend Micro	• Protection from sophisticated malware including encrypted files to prevent ransomware • Security policy enforcement • Compliance enforcement including blocking access to content • User behaviour analysis	The total revenue generated by vendors through the sale of ATP hardware or subscription services to channel partners and integrators.
Content Disarm & Reconstruction	CDR (Content Disarm and Reconstruction) to extract all safe data from a file before forwarding.	• Glasswall Solutions • OPSWAT • ReSec • Votiro	• File transfer	The total revenue generated by vendors through the sale of ATP hardware or subscription services to channel partners and integrators.

Security Operations

	Product Definition	Example Vendors	Technology Lifecycle	Use Cases	Market Revenue Definition
Security Information & Event Management	SIEM platforms log security information and provide a process for reporting and managing security events. SIEM vendors integrate a wide range of industry products into their platforms, providing customers with choice. In OT this includes integration of anomaly detection and other telemetry into SIEM platforms that are often managed by IT operations. The SOC relies on the SIEM for security management and is often the main GUI used by the security analyst. SIEM is a foundational SOC technology. However, the Cyber Security Operations market is evolving quickly and SIEM is increasingly being augmented with more advanced tools that aggregate additional data sources, use machine intelligence to detect unusual patterns, and automates incident response. Examples include 3rd party Threat Intelligence, UEBA, Network Traffic Analysis, Endpoint Detection & Response and Security Automation. SIEM is delivered as a hardware appliance, virtualised, or as a cloud delivered service which is a fast growing segment with a number of cloud native SIEM vendors such as Sumo Logic. As the lines between IT/OT become increasingly blurred it is likely that merged IT/OT SOC's will become the norm with dedicated specialist analysts to manage OT security processes.	CyberRes / Opentext (ArcSight) Fortinet (FortiSIEM) IBM (QRadar) LogRhythm Splunk	Typically deployed in the DMZ if an OT dedicated SOC or at levels 4 & 5 IT/OT & OT Security Solution	• Security management • Compliance • Risk management • Detection • Orchestration • Response Management • Forensics	Revenues generated by vendors for OT specific SIEM either directly from end-users or from channel partners and system integrators.
Security Automation & Incident Response (also known as SOAR)	Security Automation & Incident Response platforms are the automated version of the SIEM platform, collecting additional data from threat intelligence feeds, and automating the investigation and response process through playbooks. The technology is widely known by its acronym, SOAR (Security Orchestration & Automated Response) and the recognised benefit is the increased level of automation, especially related to regularly recurring events. This reduces analyst workload, enabling them to work on more high value tasks. The effectiveness of a SOAR implementation depends on several factors including integration with a wide range of security tools and the relevance of the playbooks.	AT&T Cyber Security IBM (QRadar SOAR) Palo Alto Networks (CORTEX) Splunk	Typically deployed in the DMZ if an OT dedicated SOC or at levels 4 & 5 IT/OT & OT Security Solution	• Improve MTTR through automation • Improved detection through threat intelligence • Reduction in false positives • Efficient event management and reduced analyst workload • Case management	The total revenue generated by vendors of SOAR applications primarily from channel partners, including resellers, integrators and managed service providers.

Secure Remote Access

	Product Definition	Example Vendors	Architecture	Market Maturity	Use Cases	Market Revenue Definition
Secure Remote Access Management (RAM)	Secure Remote Access Management solutions facilitate off site access for engineers and third parties to industrial assets through creating remote access sessions. Establishing trust is essential and therefore solutions need to be able to manage and enforce compliance, typically only allowing corporate issued and managed devices to access the network. This can be managed through Privileged Access Workstations (PAW) which enforce policies based on time, roles and activity, and enforce Multi Factor Authentication. Features include Management tools to onboard users, manage privileges, monitor activity and review, Threat Detection to identify unusual activity, just-in time PAM for third party access, and management of digital certificates. Zero Trust Network Access (ZTNA) is an additional approach to RAM that assumes that users and devices are untrusted before gaining access to the network. Benefits include: • Obscuring applications from visibility on the public internet • Enforcing policy giving enough time and access to resources as opposed to unlimited access • Providing access based on the status of the user, device and application rather than solely on IP address or physical location • Cloud-based service Remote Desktop is not included in this scope. VPN is included with Network Firewalls.	BeyondTrust "Privileged Remote Access" Cisco "Duo" Claroty SRA "Secure Remote Access" CyberArk "Privileged Access Manager" Honeywell "Secure Remote Access" OPSWAT "Secure Access Module" OTORIO Platform Xage "Zero Trust Remote Access" Xona "Critical System Gateway" Zscaler "ZPA"	Deployed in the DMZ at layer 3.5	High Growth	• Least privilege access • Zero trust enforcement • Multi Factor Authentication • Usage monitoring • Threat detection	Revenues generated by vendors for the sale of on-prem or cloud services direct to the end-user, to manage service providers or through the channel.

CMDB and SBOM

	Product Definition	Example Vendors	Market Maturity	Use Cases	Market Revenue Definition
Configuration Management Databases (CMDB)	CMDBs are an essential technology within an enterprise's IT Service Management (ITSM) strategy, holding records on assets and the relationship between them. CMDB differ from Asset Management. Whilst Asset Management is concerned with the processes to manage the lifecycle of assets (e.g. maintenance, procurement records), CMDBs are about the data used to manage the asset (i.e. what components constitute the asset and the relationship with other assets). Integration of anomaly detection tools with CMDB will accelerate the convergence of OT and IT security operations. This includes asset management records (e.g. assets, IP & MAC addresses, firmware and risk scoring), vulnerability data and alert management (records, ticketing etc).	• ServiceNow	NA	• Asset Management • Risk Management • Change Management • Incident Response • IT Operations Management and Improvements	CMDBs are part of the ITSM framework. OT integration with CMDBs will improve OT security management due to collaboration, knowledge sharing and improved processes. However, it is not an OT security technology expenditure and therefore revenues generated through integrations or sales of CMDBs from vendors such as ServiceNow are excluded.
Software Bill Of Materials (SBOM)	A SBOM is a list of all of the open source and commercial software used for a specific industrial software product or application and will list version numbers and licenses. There is an increasing focus on SBOMs to ensure supply chain resilience and to limit risk. The SBOM is related to the CMDB insofar as it can be used as a source of information.	• aDolus	NA	• Asset Management • Risk Management • Change Management • Incident Response • IT Operations Management and Improvements	Not included within the scope of this analysis. Definition has been included for completeness.

Threat Intelligence

	Product Definition	Example Vendors	Market Maturity	Use Cases	Market Revenue Definition
Threat Intelligence	Threat intelligence includes platforms that collate 3rd party intelligence, providing real-time insight and context through automated processes. The quality of the service is dependent on the range and type of data collected, context provided and ability to quantify the nature of the threat and associated risk. Operationalising threat intelligence requires collection, processing and integrating the data with security tools. The data is generated from a variety of sources including company sources (network traffic and logs), technical sources (vulnerability databases) and other sources such as the dark web and social media. However, collecting, organising and contextualising the data is challenging due to the size, complexity and dynamic nature of threat intelligence, making it "noisy". This is exacerbated by the enterprise requirement for a range of intelligence from cyber criminality, fraud, dark web and nation state intelligence, which often results in enterprises relying on multiple vendors. OT Threat Intelligence is specific to industrial control systems. This includes intelligence on adversaries that are explicitly targeting ICS; Tactics, Techniques and Procedures (TTP), and the direct and indirect impact on control systems.	Dragos IBM Security Mandiant Nozomi Otorio Tenable	High Growth	• Third Party Intelligence and Vendor Management • Supply Chain Security • Security Operations Intelligence and Threat Hunting • Threat Detction • Vulnerability Management • Threat Investigations & Response • Risk Management • Security Strategy Development	Threat intelligence has not been segmented in this analysis. Threat Intelligence is often provided as part of a wider service offering and therefore vendor revenue has been captured in the relevant segments.

Managed Security Services

	Concept Definition	Example Service Providers	Security Use Cases	Market Revenue Definition
Managed Security Monitoring Service	Managed Security Service Providers (MSSPs) provide remote monitoring and management of security through a single or network of Security Operating Centres (SOCs) usually providing a 24x7x365 service. The model can include managing the customer's on-prem security solutions or in external datacentres. Managed security technologies include firewalls, endpoints, vulnerability management, web and email gateways, intrusion detection and prevention systems, security information and event management (SIEM). Tasks include administration, patch management, configuration management, compliance and monitoring. Management of OT requires MSSPs to deploy specific tools that are able to detect threats whilst not impacting operational performance, and to have the technical skills to understand OT systems and protocols.	All firms are at varying stages of moving from providing mainly monitoring services to delivering threat detection and response. Professional Services • Accenture • Capgemini • Deloitte • EY MNO's • NTT • Orange Cyberdefense • T-Systems • Verizon IT Services • Accenture • ATOS • Fujitsu • WIPRO Security Services • OPTIV • Kudelski • SecureWorks • Trustwave (Singtel) Engineering Security Services • Airbus • Thales Industrials • Honeywell • Rockwell Automation • Siemens	• Risk Management • Compliance • Configuration Management • Patch Management • Security Controls Monitoring • Log Management • Incident Management	The total subscription revenue generated in the year by MSSPs through providing a managed security services solution to monitor industrial operating systems from the DMZ down. Professional Services, related to consulting and advising on risk, and systems integration services, are excluded unless specifically included in the MSS contract.
Managed Security Detection & Response Services (includes MTD and MTR)	MSSPs are providing an growing range of security services to help customers manage the full security lifecycle from identify, protect, detect, respond to recover. This includes the traditional monitoring services together with more specialised services including risk scoring, continuous controls monitoring, threat hunting and threat detection and response services. This is typically delivered through the MSSP's own Managed Detection & Response (MDR) platform or MTR (Managed Threat Response) which is also used to enable results based, proactive threat hunting.		• Advanced Monitoring • Threat Hunting • Threat Intelligence • Threat Detection • Incident Response Playbooks	The total subscription revenue generated in the year by MSSPs through providing a Managed Security Detection & Response service. Professional Services, related to consulting and advising on risk, and systems integration services, are excluded unless specifically included in the MSS contract.

Professional Security Services

	Product Definition	Example Vendors	Market Revenue Definition
Professional Security Services	The professional Security Services segment is the largest area of investment and includes a range of services. These are broadly categorised as the following. • *Governance & Risk Management* which includes the client risk assessment, standards adherence and creation of cybersecurity policies in relation to the business objectives. • *Assessment & Assurance* includes activities to test the resilience of the operation and includes penetration testing, red-teaming exercises and threat assessments. • *Advisory* services is typically the technical consulting work, helping CISOs to address a challenge by designing a solution to a problem. Use cases includes SOC operations, threat intelligence, incident response planning, remote access management, deploying new manufacturing processes securely, and staff training and awareness programs. • *Secure-by-Design* is the process of building cybersecurity into the engineering process to ensure that the product is safe and secure throughout its lifecycle. Use cases may include designing of sensors or machines for use within a manufacturing process. • *Systems Integration* is the deployment of security controls either onsite or as part of remote managed service. Support services are also included in this segment.	Professional Services • 1898 • Accenture • Applied Risk • Airbus • Arup • Atkins • ATOS • Bain • Booz Allen Hamilton • Capgemini • Deloitte • Dragos • EY • HCL • Honeywell • IBM • Jacobs • KPMG • Mandiant • McKinsey • Orange Cyberdefense • PA Consulting • PwC • Rockwell Collins • Roland Berger • Siemens • TCS • Telekom Security • Thales • WIPRO	Revenues generated by professional security services firm either as a single engagement or through a retainer contract.

Technology innovation is driven by changing customer requirements related to business models, responsiveness, accuracy, scalability, automation and interoperability.

WESTLANDS ADVISORY

Essentials

Specifications	Pricing Model	Compliance
The solutions solves the security use-case	Pricing is aligned with market expectations	The solution is compliant with industry norms

Strategic Alignment between vendor and customer	Strength of the vendor's Business operation	Financial return on investment	Vendor's Technical Solution	Productivity gains from the vendor's solution	Operational gains from the vendor's solution	Buyers and users Personal preferences
The vendor and customer share a common understanding of operational imperatives	The vendor demonstrates deep experience of addressing the security use-cases in the relevant industry	The vendor reduces the cost of ownership through financial, operational, or process improvements	The vendor provides a superior range of products and services improving protection and detection	The vendor provides a solution that improves optimises security processes and user experience	The vendor products and services meet the operational requirements of the customer	The vendor provides a service that is aligned to the needs and requirements of the individual
Vision	Infrastructure	Business Model	Reliability	Collaboration	Integration	Design
Mission	Credibility	Efficiency	Scalability	Usability	Interoperability	Brand
Innovation	Ecosystem	Consolidation	Accuracy	Automation	Safety	Skills
Cultural	Responsiveness	Risk Reduction	Variety	Transparency	Simplification	Career
	Stability		Configuration		Availability	
	Governance				Support	

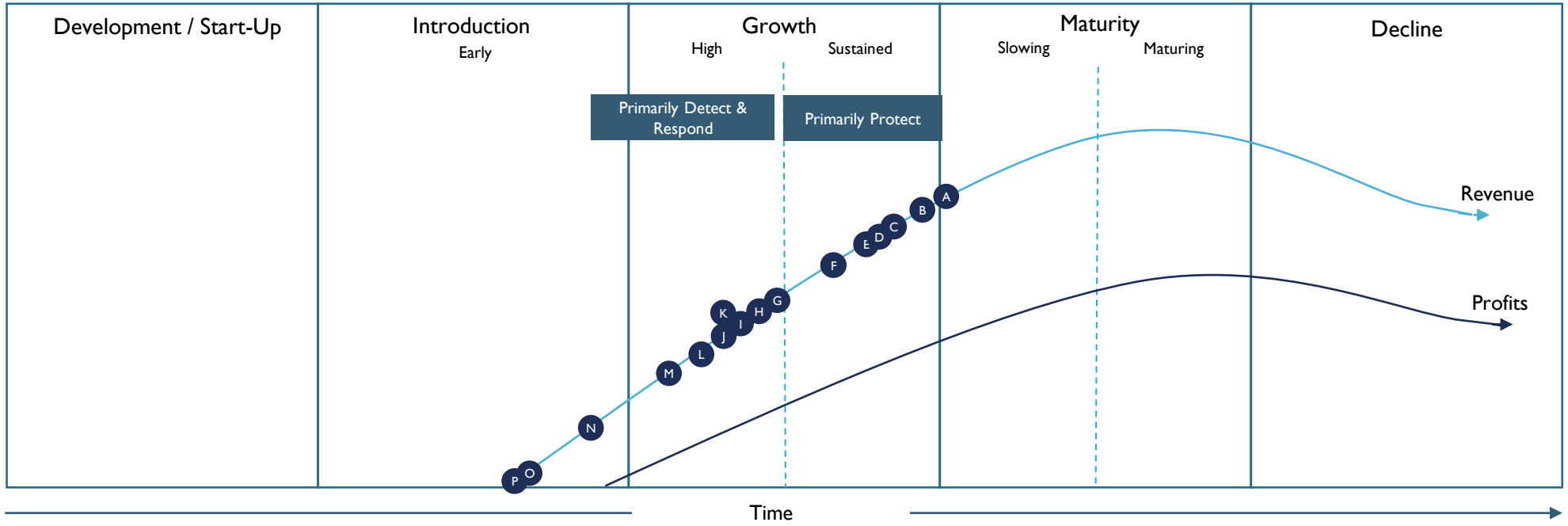
Customer Priorities

References: Modelled from Bain's B2B Elements of Value

Operational Technology Security Lifecycle

WESTLANDS ADVISORY

A. EPP
B. Industrial Firewall
C. Next Generation Firewall
D. Unidirectional
E. NAC
F. Advanced Threat Protection
G. Vulnerability Management
H. Secure Access Remote Management
I. Asset Visibility
J. Threat Detection
K. NDR
L. EDR
M. Cyber Risk Management*
N. Continuous Controls Monitoring
O. Deception
P. SBOM Management

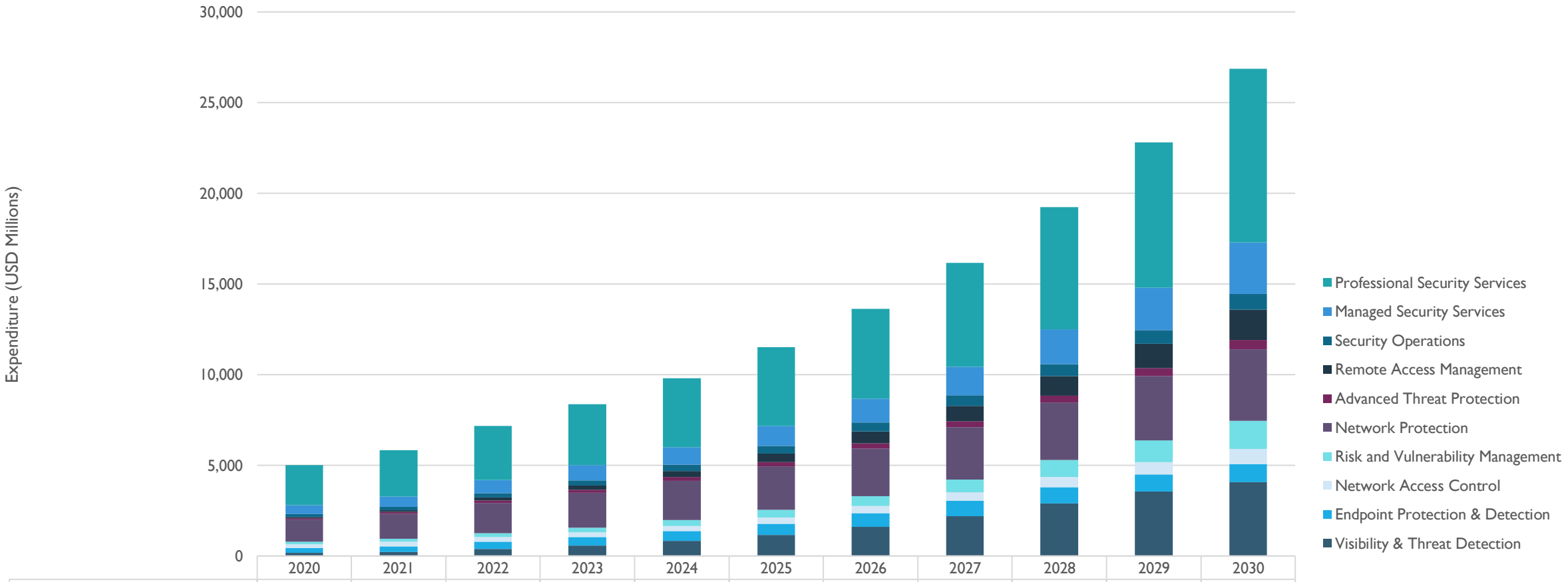


Lifecycle Characteristics	Development / Start-Up	Introduction (Early)	Growth (High)	Growth (Sustained)	Maturity (Slowing)	Maturity (Maturing)	Decline
Growth Rate	None	>20%	>15%	>10%	>5%	>0%	<0%
Customer Saturation (Accessible Market)	None	<10%	Accelerating 10-20%	High 20-50%	Slowing 50-70% / Maturing 70-80%		80%
Balance of Revenue	None	New Product Sales	New Product Sales & Renewals		Customer Renewals, Upsell & Services		Services
Industry Consolidation	None	Start-ups	New Competitors & Increasing M&A		Consolidating, High Market Share		Exits & New Markets
Balance of Budget	Product Development	Sales & Marketing	Sales & Marketing		Product Development		Product Development
Productivity/ Profitability	0	Lowest	Medium		Highest		High

Marketing Priorities	Awareness	Differentiation	Brand Leadership / Evolve
Product	Initial Product	Innovation & Variations	Expanding Product Portfolio
Price	Entry	Evolution	Leadership
Place	Target Market Segment	Channel Expansion	Multi Segment & Channel
Promotion	Educate	Differentiation	Innovation

Source: Westlands Advisory

Cybersecurity expenditure will increase across all technology and service categories to 2030

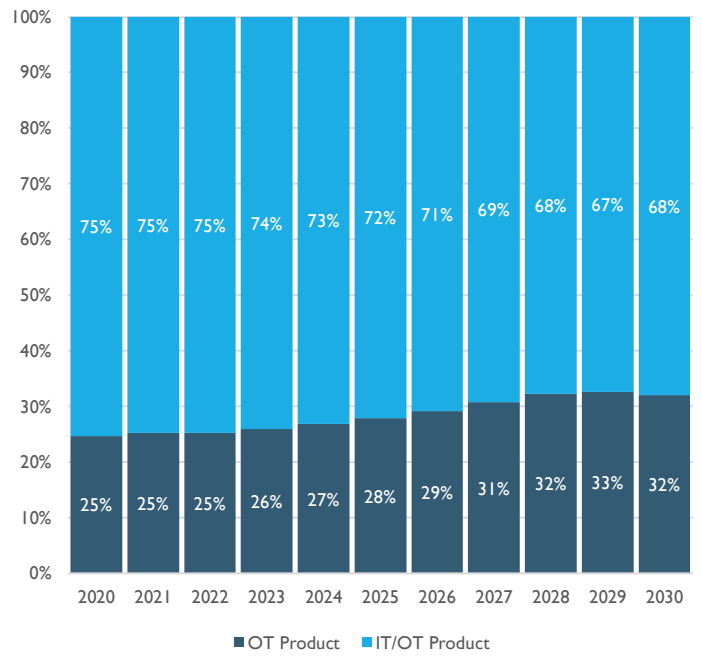


	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Professional Security Services	2216.8	2548.2	2983.5	3370.5	3809.3	4321.2	4951.1	5726.7	6720.9	7998.5	9584.3
Managed Security Services	487.8	575.3	712.6	824.5	954.0	1107.6	1319.5	1587.0	1936.6	2358.7	2846.2
Security Operations	152.9	171.2	246.1	298.8	357.0	421.0	493.7	574.9	657.3	749.2	859.8
Remote Access Management	70.8	103.4	163.5	237.8	340.3	480.8	649.8	849.8	1078.5	1345.9	1664.6
Advanced Threat Protection	71.5	85.7	124.2	156.8	197.6	238.5	286.3	336.1	387.4	445.2	515.2
Network Protection	1234.6	1398.8	1686.8	1915.3	2154.1	2395.0	2638.1	2888.8	3170.2	3530.1	3957.7
Risk and Vulnerability Management	138.8	170.1	202.8	254.2	325.8	417.4	539.1	705.9	927.9	1214.4	1542.5
Network Access Control	209.1	239.4	257.1	277.2	303.5	339.9	393.5	463.2	553.0	677.4	842.6
Endpoint Protection & Detection	266.6	306.5	396.0	462.0	539.0	630.8	745.6	833.2	896.6	943.4	980.9
Visibility & Threat Detection	167.7	234.4	393.3	577.9	827.2	1156.5	1612.7	2210.0	2909.1	3550.0	4081.7

Expenditure on OT technology to rise as a percentage of expenditure due to high demand for visibility and detection. Demand for Managed Security Services will also increase substantially.

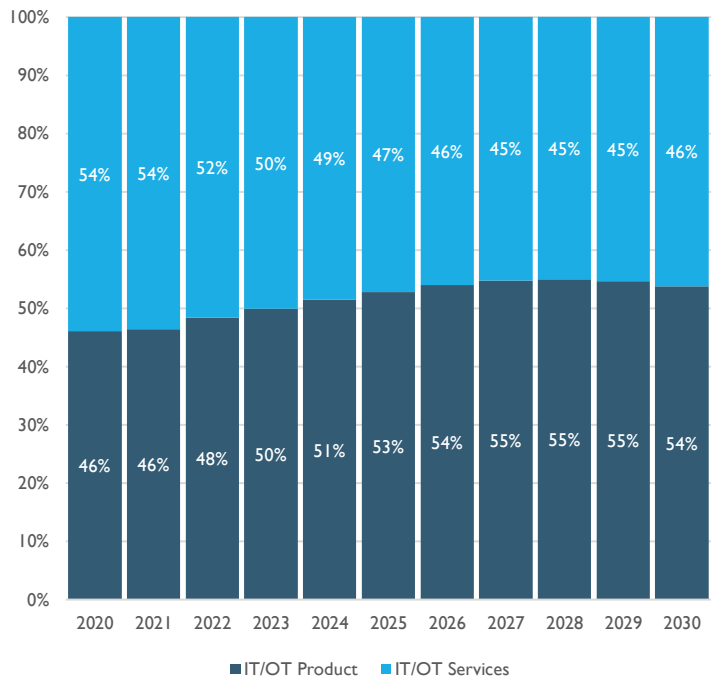
WESTLANDS ADVISORY

High growth in OT security product expenditure



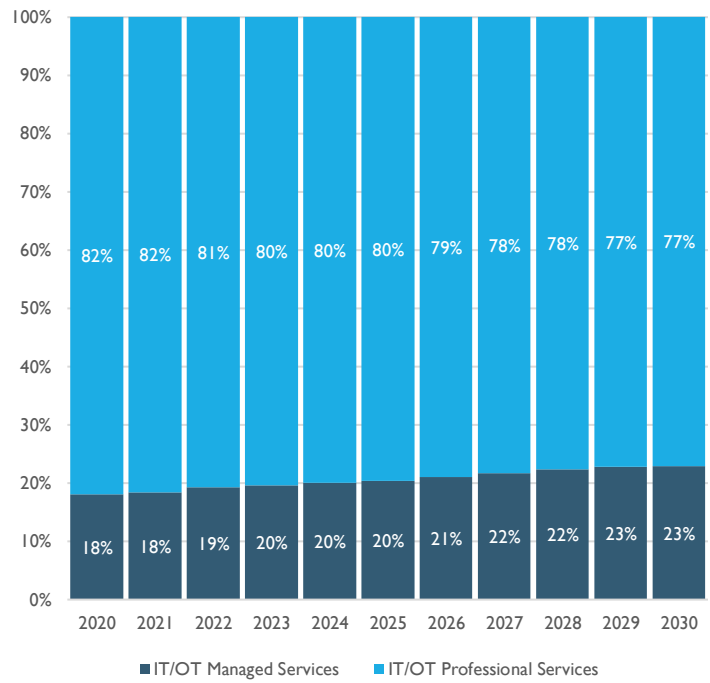
Investment in visibility and detection technology means that the market for OT is growing faster that IT/OT though this will stabilise towards the end of the forecast period as the market matures.

Percentage of OT cybersecurity expenditure on products versus services will increase slightly before flattening by 2026 onwards



Product growth has outgrown consulting services growth in recent years. This is expected to reverse towards the end of the forecast period as program complexity increases and services are outsourced.

OT Managed Security Services is expected to increase as a percentage of expenditure on all services



Managed Security Services are expected to grow as a percentage of service sales over the forecast period.

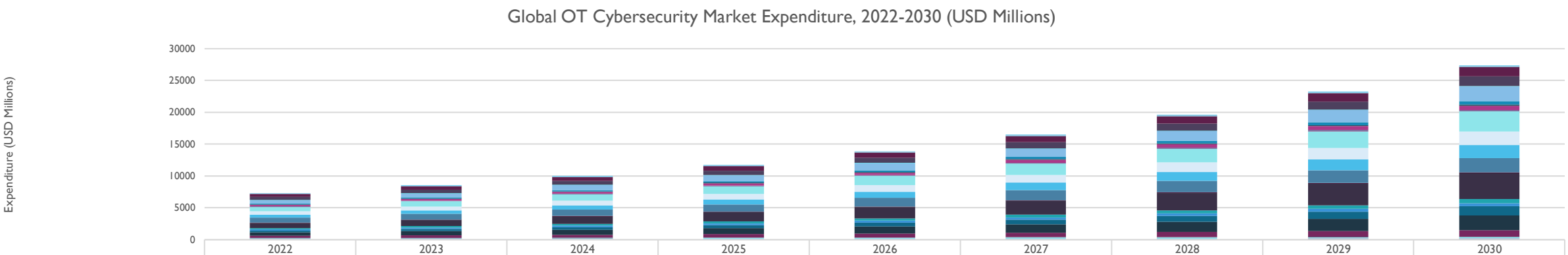
Market Expenditure & Outlook

WESTLANDS ADVISORY

Summary

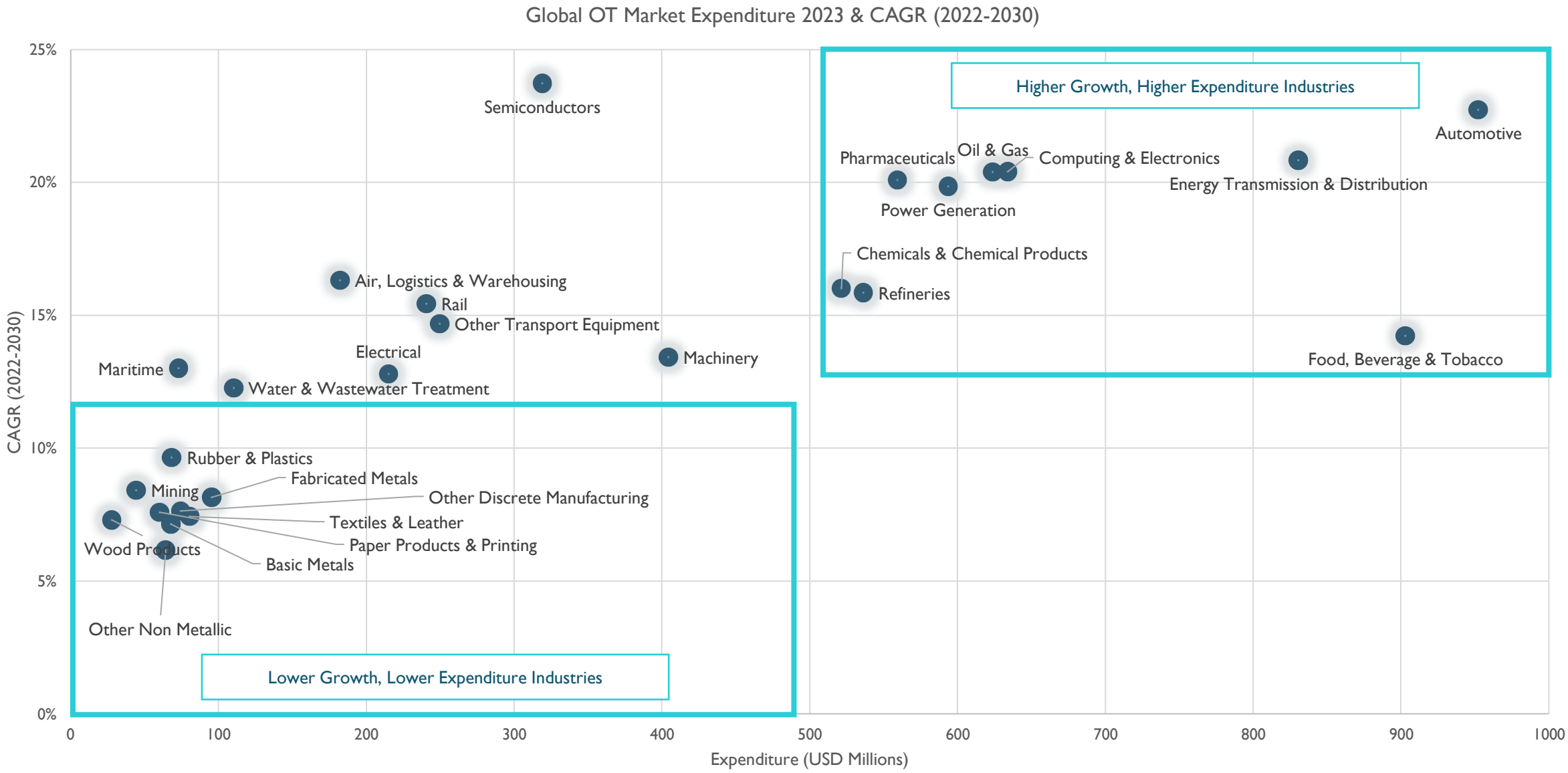
1	Investment in OT cybersecurity is expected across all industry sectors, with the 26 segments all growing >5% p.a. to 2030.
2	The highest investment is in complex process industries (Energy, Oil & Gas and Chemicals) and high value, automated manufacturing processes (Automotive, Pharmaceuticals and Computing & Electronics). These sectors will continue to grow up until 2030.
3	High growth segments include semiconductor manufacturing and transport related sectors include rail, air and distribution.
4	Investment in low automation/ low digital industries will grow at a slower pace although increasing regulatory requirements will lead to security transformation.
5	Most expenditure will be in North America, Asia Pacific and Europe due to the high concentration of process industries and high-value manufacturing in the regions. Investment in the Middle East is mainly related to Oil & Gas.

Global OT Cybersecurity Market 2022-2030

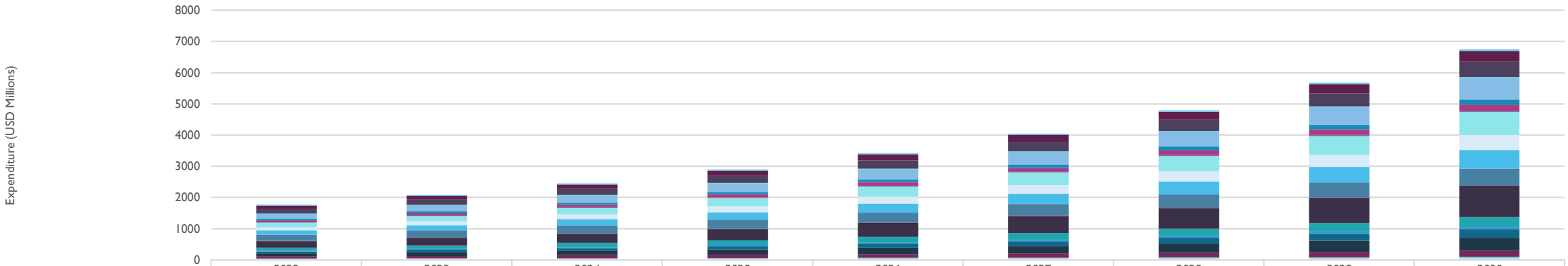


	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	89	96	103	112	121	131	142	153	166
Basic Metals	63	68	72	78	83	89	95	102	110
Chemicals & Chemical Products	452	521	602	696	812	949	1109	1288	1482
Refineries	466	536	618	712	829	967	1128	1310	1511
Mining	41	44	48	52	57	61	67	72	79
Oil & Gas	522	624	748	897	1081	1306	1578	1907	2302
Air, Logistics & Warehousing	157	182	212	246	286	333	388	452	527
Maritime	65	73	82	92	105	120	137	155	173
Rail	210	241	276	316	368	428	500	579	663
Water & Wastewater Treatment	99	110	123	137	155	177	201	227	250
Energy Transmission & Distribution	690	831	1001	1208	1459	1764	2135	2587	3137
Power Generation	500	594	706	840	1015	1229	1491	1792	2126
Pharmaceuticals	470	560	666	794	964	1171	1424	1714	2032
Food, Beverage & Tobacco	795	903	1026	1166	1342	1545	1780	2037	2304
Other Discrete Manufacturing	69	74	80	86	93	100	107	116	125
Automotive	781	952	1163	1420	1760	2183	2710	3336	4016
Other Transport Equipment	218	250	286	327	375	431	494	568	653
Electrical	191	215	242	273	308	348	392	443	501
Semiconductors	258	319	395	488	604	747	925	1145	1417
Computing & Electronics	527	634	763	918	1105	1331	1603	1932	2329
Machinery	357	404	458	520	589	669	759	861	977
Other Non Metallic	61	64	68	73	77	82	87	92	98
Rubber & Plastics	63	68	75	82	90	99	108	119	131
Paper Products & Printing	56	60	65	70	75	81	87	93	101
Wood Products	26	28	30	32	34	37	40	43	46
Textiles & Leather	75	81	87	93	100	107	115	124	133

There is a clear difference in investment size and growth. Complex, regulated and high automation sectors are the biggest market opportunities but also highly competitive

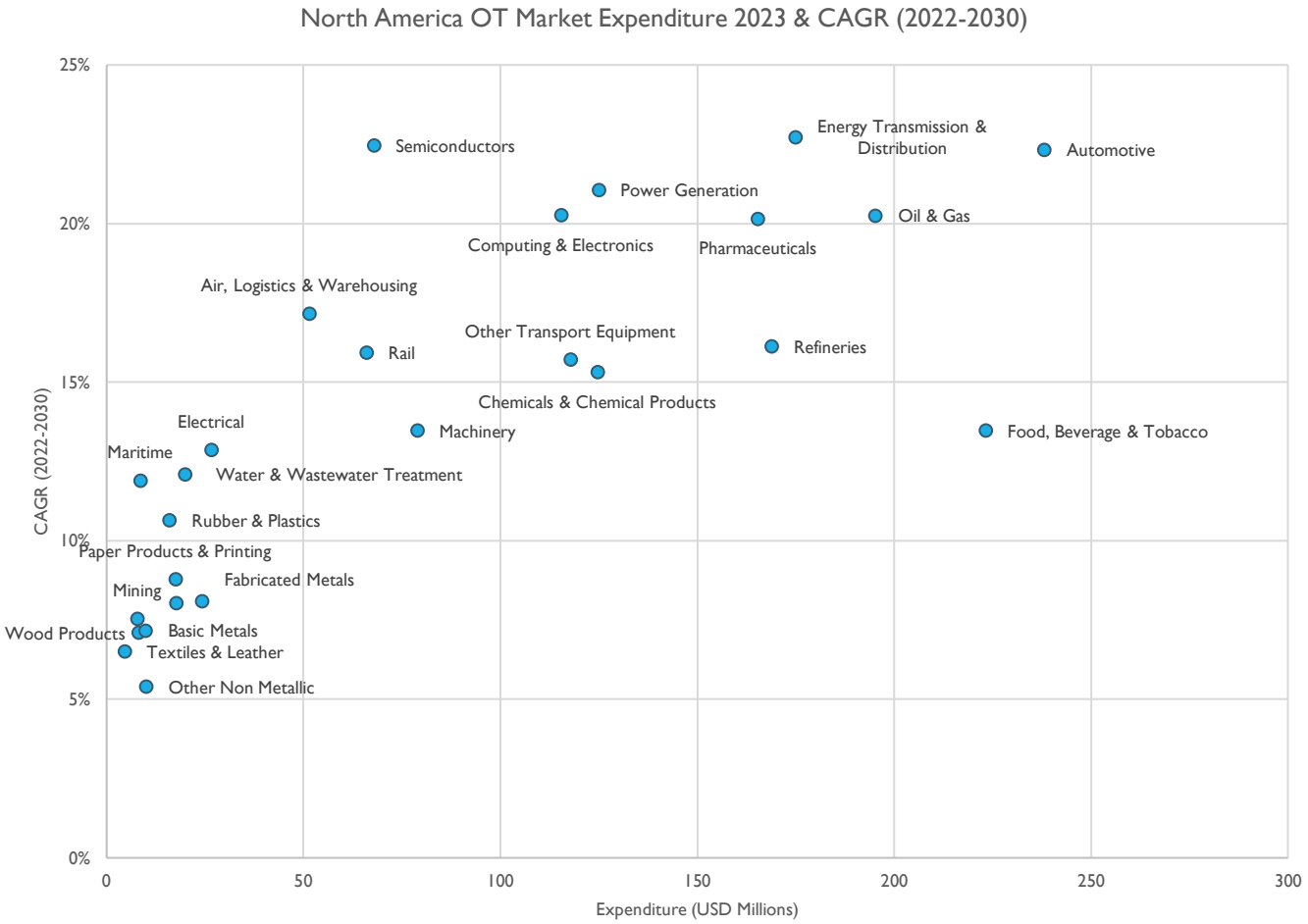


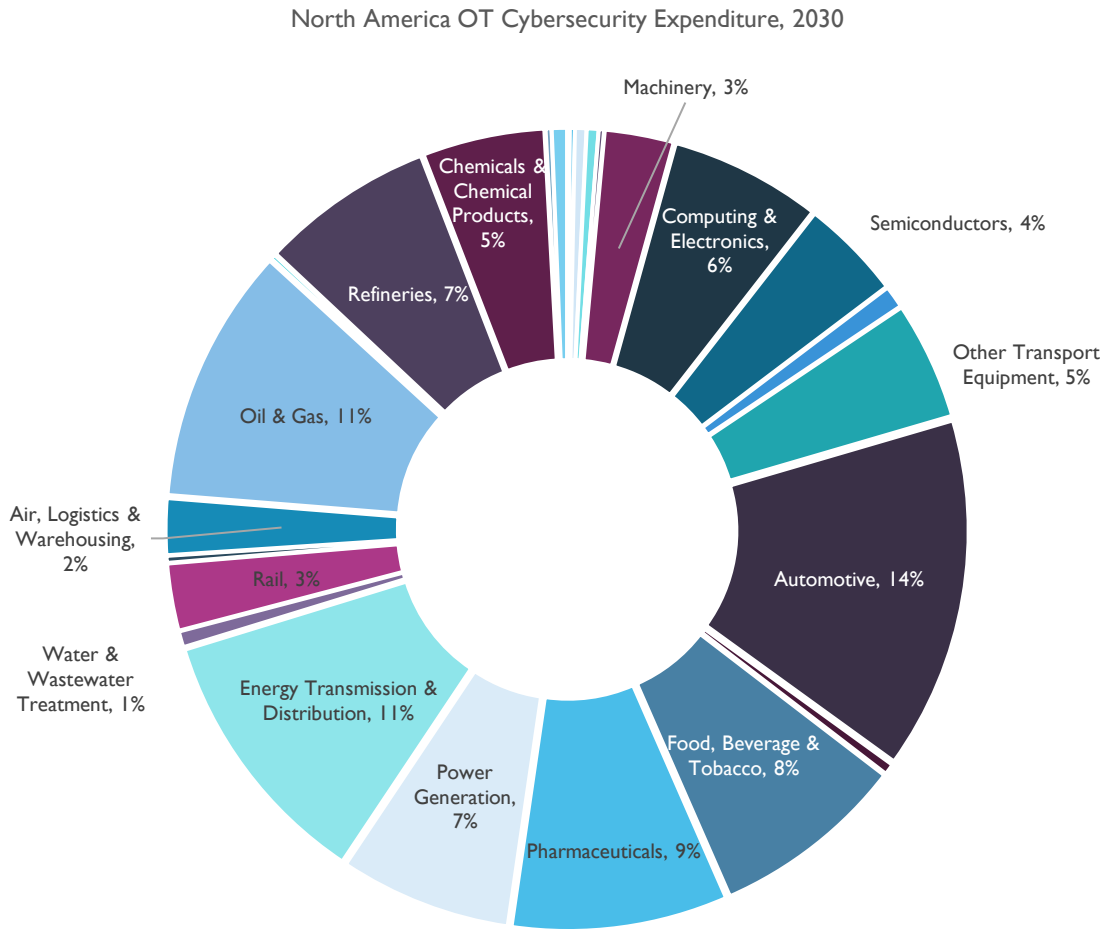
North America TAM for 2023-2030 is $32.1B with a CAGR of 18%



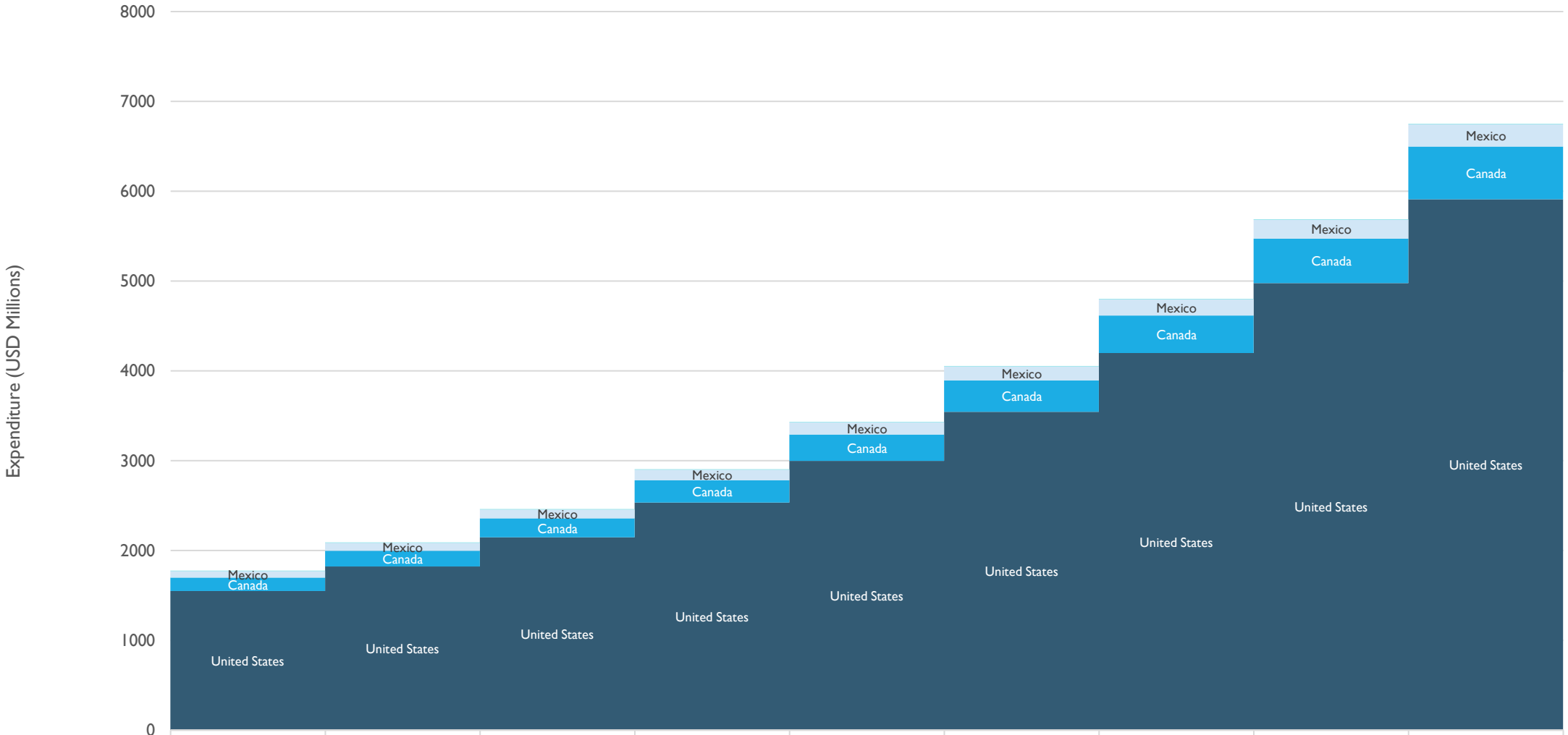
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	22	24	26	28	31	33	36	39	42
Basic Metals	9	10	11	11	12	13	14	15	16
Chemicals & Chemical Products	108	125	144	166	191	220	254	293	338
Refineries	145	169	196	228	264	307	357	414	481
Mining	7	8	8	9	10	10	11	12	13
Oil & Gas	162	195	235	282	339	408	491	591	710
Air, Logistics & Warehousing	44	52	60	71	83	97	114	133	156
Maritime	8	9	10	11	12	14	15	17	19
Rail	57	66	76	89	103	119	138	160	186
Water & Wastewater Treatment	18	20	22	25	28	31	35	40	44
Energy Transmission & Distribution	143	175	215	263	323	397	487	598	734
Power Generation	103	125	151	183	222	268	325	394	477
Pharmaceuticals	138	165	199	239	287	345	414	498	598
Food, Beverage & Tobacco	197	223	253	287	326	370	420	476	541
Other Discrete Manufacturing	16	18	19	21	22	24	26	28	30
Automotive	195	238	291	356	436	533	653	799	977
Other Transport Equipment	102	118	136	158	183	211	245	283	328
Electrical	24	27	30	34	38	43	49	55	62
Semiconductors	55	68	83	102	125	153	187	229	281
Computing & Electronics	96	115	139	167	201	242	290	349	420
Machinery	70	79	90	102	115	131	149	169	191
Other Non Metallic	10	10	11	11	12	12	13	14	14
Rubber & Plastics	14	16	18	20	22	24	26	29	32
Paper Products & Printing	16	18	19	21	23	25	27	29	32
Wood Products	8	8	9	9	10	11	12	12	13
Textiles & Leather	4	5	5	5	6	6	6	7	7

North America High Growth Industries with High Expenditure includes Automotive, Pharma, Utilities and Oil & Gas. Strong growth is expected in Semiconductors and Computing



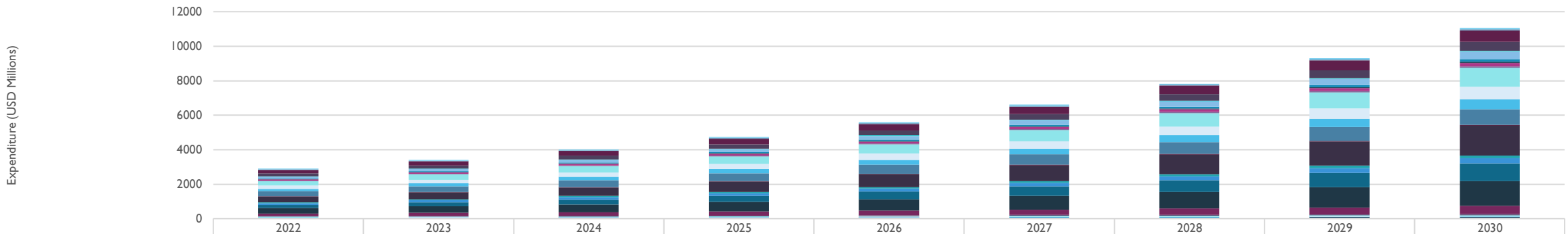


North America The United States is the largest market with diversified industries and strong growth expected. Canada's Oil & Gas sector and Mexico's manufacturing are sizable segments



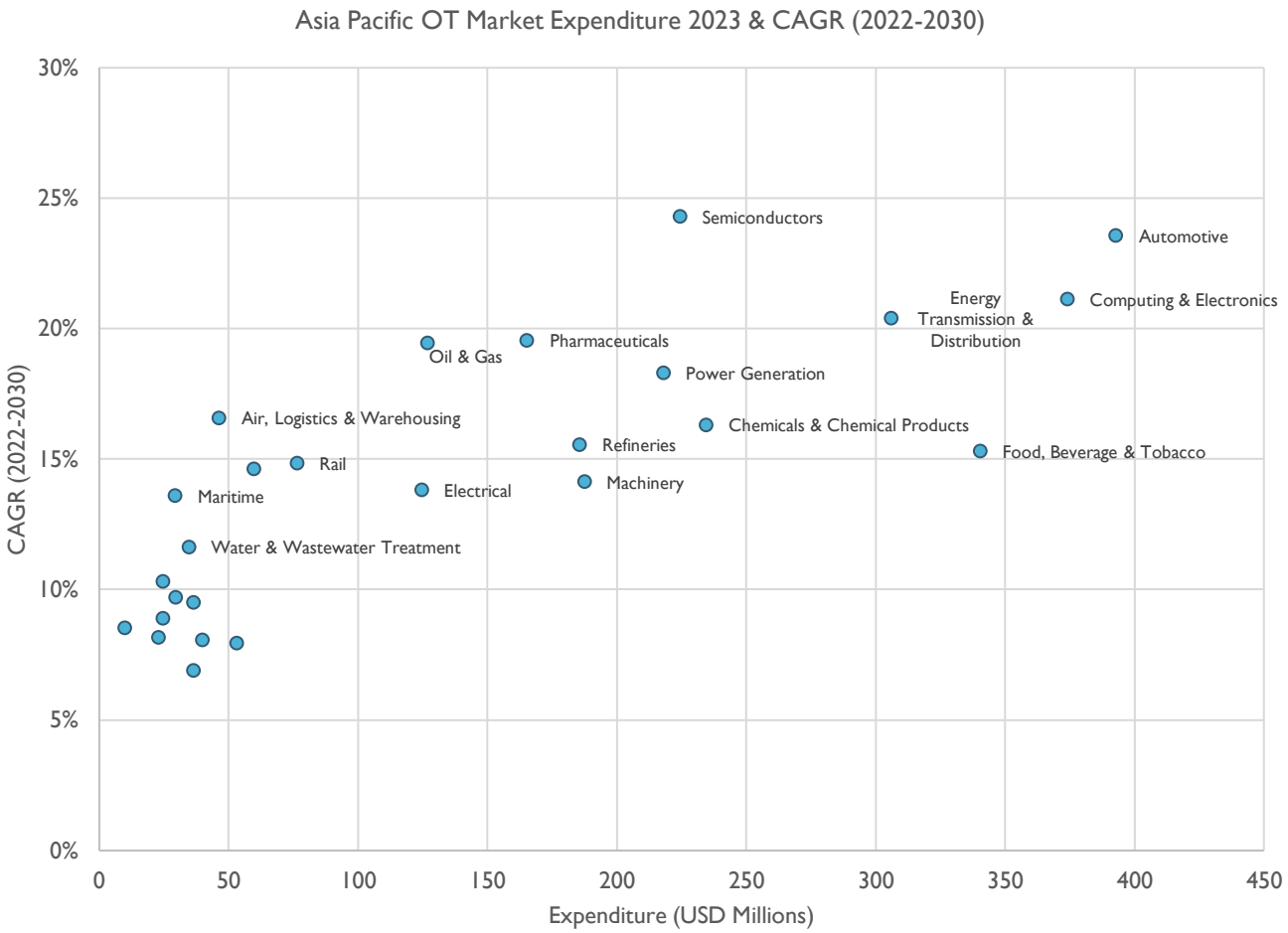
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Virgin Islands (U.S.)	0	0	0	0	0	0	0	0	0
Mexico	74	86	99	115	134	155	180	210	245
Canada	150	178	210	249	295	350	416	495	590
United States	1546	1821	2147	2534	2995	3544	4197	4977	5909

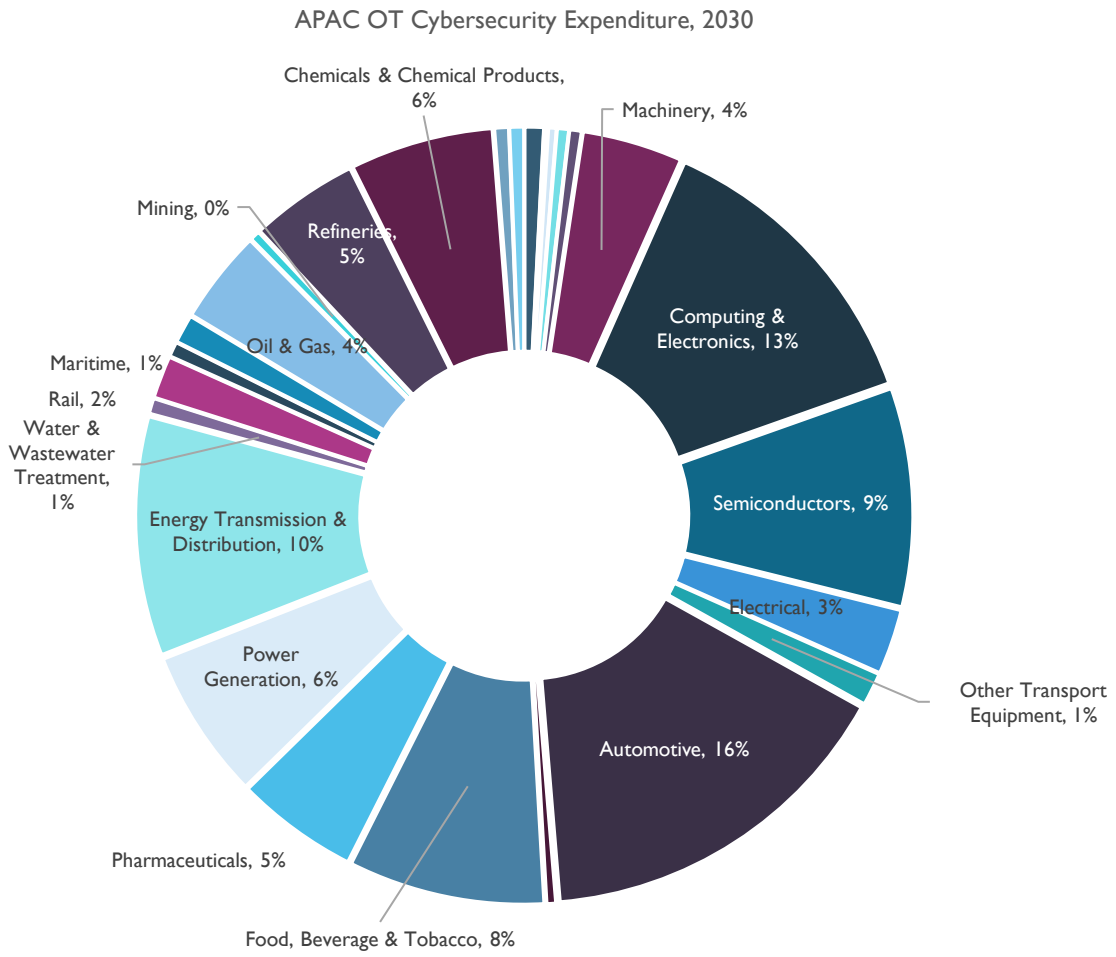
APAC TAM for 2023-2030 is $52.5B with a CAGR of 18%



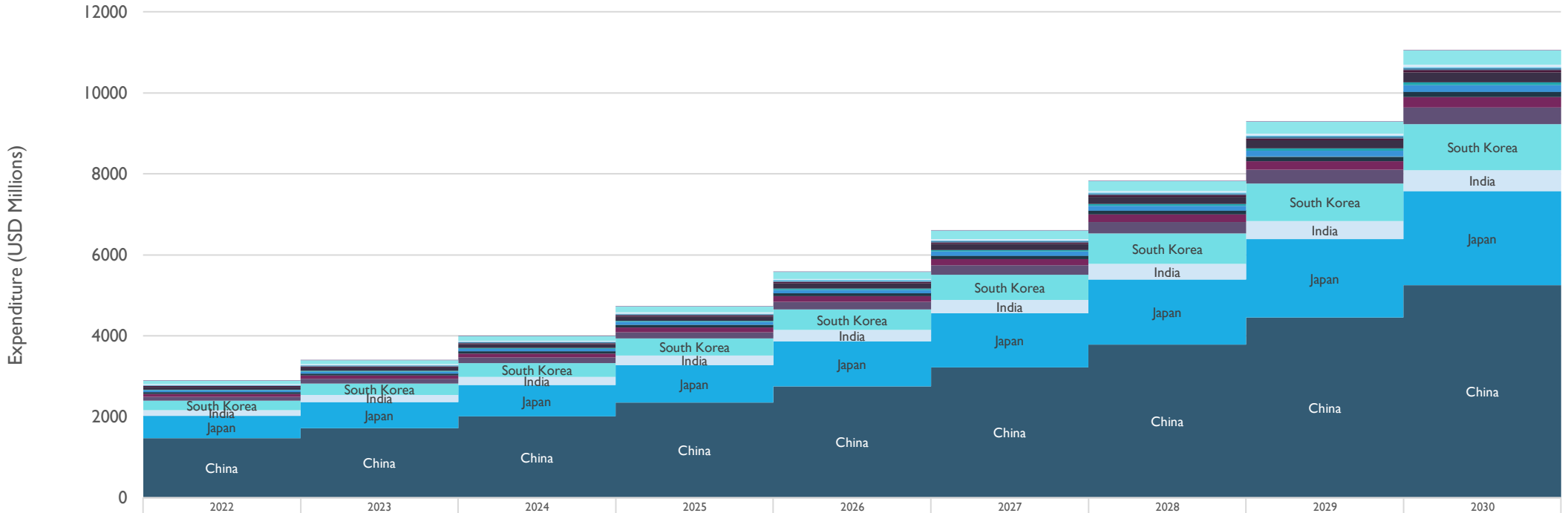
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	33	36	40	44	48	52	57	63	69
Basic Metals	37	40	43	47	50	54	59	64	69
Chemicals & Chemical Products	202	234	272	317	368	429	499	580	675
Refineries	161	186	214	247	286	330	382	442	511
Mining	22	25	27	30	33	37	40	44	49
Oil & Gas	107	127	151	180	215	257	307	368	442
Air, Logistics & Warehousing	40	46	54	63	73	85	99	116	136
Maritime	26	29	33	38	43	49	55	63	72
Rail	67	76	88	101	115	133	152	175	202
Water & Wastewater Treatment	31	35	39	43	48	54	60	67	75
Energy Transmission & Distribution	255	306	368	442	532	641	772	932	1125
Power Generation	185	218	258	304	360	426	505	598	708
Pharmaceuticals	138	165	197	236	282	337	403	482	577
Food, Beverage & Tobacco	295	340	392	452	521	601	693	800	923
Other Discrete Manufacturing	23	25	27	29	32	35	38	41	45
Automotive	318	393	485	599	740	915	1131	1397	1728
Other Transport Equipment	52	60	68	78	90	103	118	136	156
Electrical	109	125	142	161	184	209	238	271	308
Semiconductors	181	224	279	346	431	535	665	827	1028
Computing & Electronics	309	374	453	549	664	805	975	1181	1431
Machinery	164	187	214	244	278	318	363	414	473
Other Non Metallic	34	36	39	42	44	48	51	54	58
Rubber & Plastics	27	30	32	36	39	43	47	52	57
Paper Products & Printing	21	23	25	27	29	31	34	37	40
Wood Products	9	10	11	12	13	14	15	16	17
Textiles & Leather	49	53	57	62	67	72	78	84	91

APAC High levels of automation in discrete manufacturing industries and offshoring are likely to contribute to ongoing investment in automotive, computing and electronics



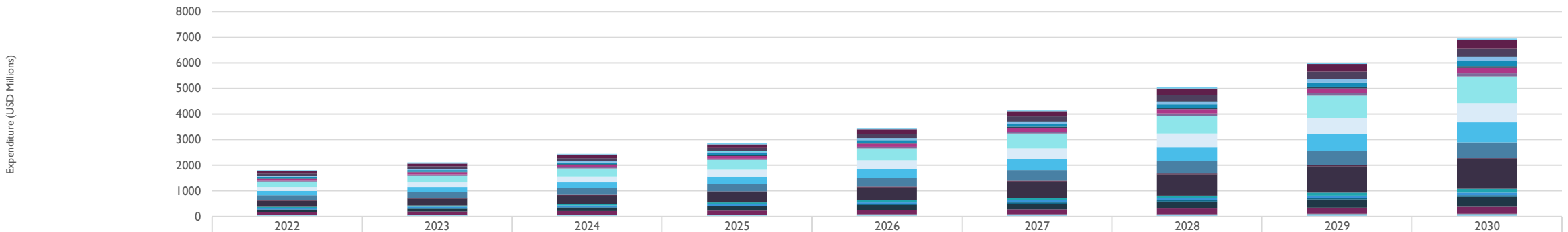


APAC China is the largest investor in OT cybersecurity and supports a strong ecosystem of local cybersecurity service providers. Japan and South Korea are significant markets



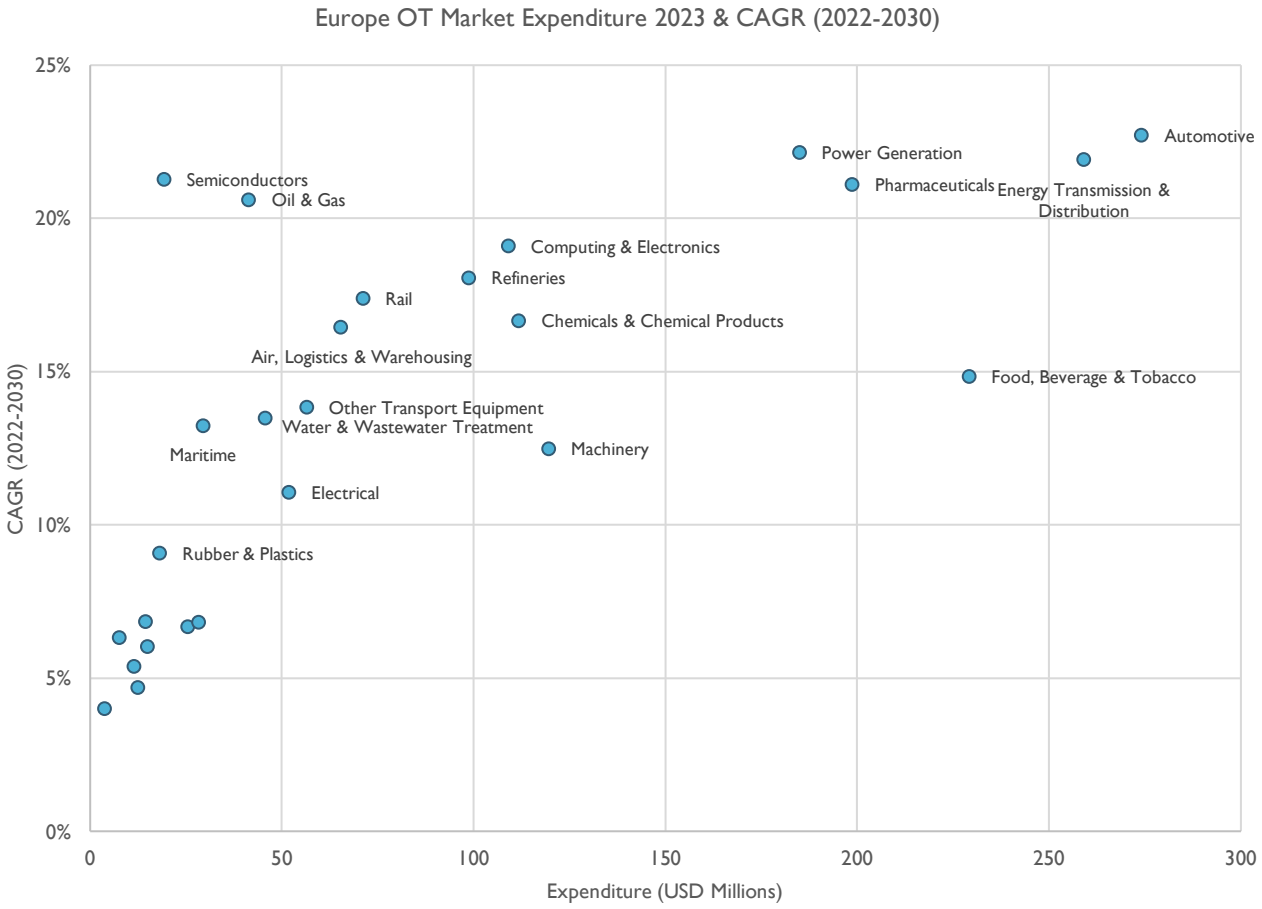
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other	9	10	11	11	12	14	15	16	18
Taiwan	82	98	118	141	169	204	245	295	356
New Zealand	17	19	22	26	30	35	41	48	57
Pakistan	14	14	15	16	17	18	19	20	21
Vietnam	19	21	24	26	30	33	37	42	48
Hong Kong SAR, China	19	22	25	29	33	38	44	50	58
Malaysia	66	78	91	107	126	148	175	207	246
Philippines	20	23	27	31	36	41	48	56	65
Singapore	42	50	59	70	83	99	118	140	168
Bangladesh	3	3	4	4	5	5	5	6	7
Thailand	37	43	50	58	67	79	92	107	126
Indonesia	74	86	100	116	135	158	184	214	251
Australia	93	112	135	162	195	235	285	345	418
South Korea	232	281	342	416	507	619	756	925	1132
India	151	176	205	238	278	325	379	444	520
Japan	546	651	778	932	1116	1339	1609	1935	2331
China	1470	1715	2003	2344	2746	3222	3785	4452	5245

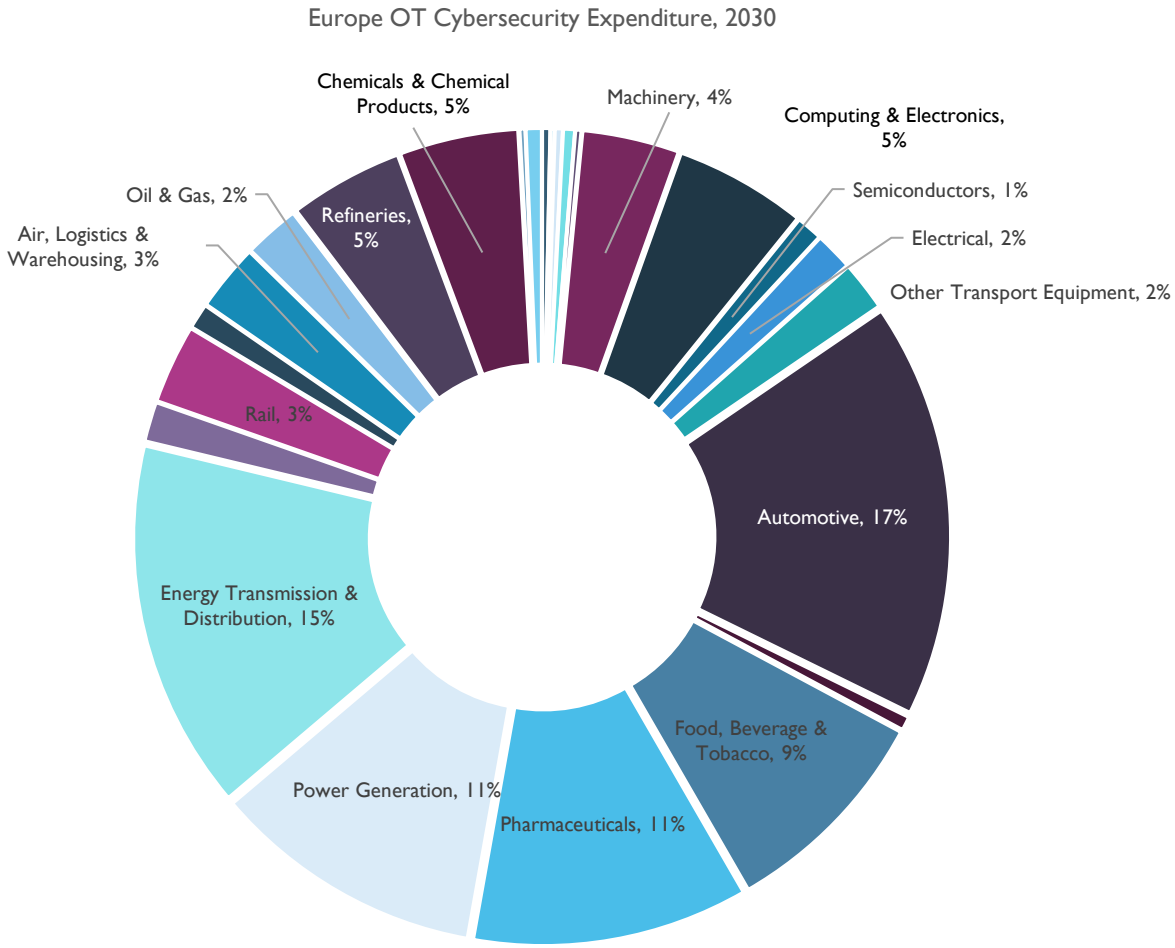
Europe TAM for 2023-2030 is $33B with a CAGR of 18%



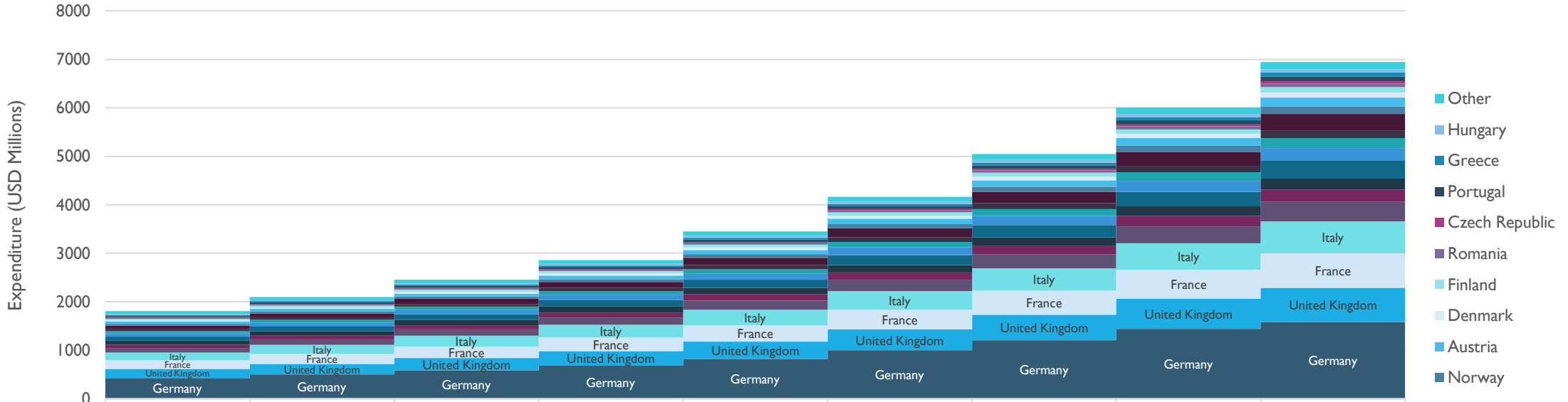
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	26	28	30	32	34	37	39	42	45
Basic Metals	11	11	12	13	13	14	15	16	16
Chemicals & Chemical Products	98	112	128	147	177	212	255	299	335
Refineries	85	99	114	132	161	195	237	281	322
Mining	4	4	4	4	4	4	4	5	5
Oil & Gas	35	41	49	57	71	88	110	133	157
Air, Logistics & Warehousing	56	65	76	89	103	120	140	163	190
Maritime	27	30	33	36	42	50	58	66	72
Rail	62	71	82	94	114	137	166	195	223
Water & Wastewater Treatment	41	46	51	57	66	77	91	103	112
Energy Transmission & Distribution	213	259	316	385	469	572	697	851	1039
Power Generation	154	185	222	266	335	421	529	648	764
Pharmaceuticals	167	199	236	280	350	437	546	663	774
Food, Beverage & Tobacco	203	229	259	292	345	409	484	557	615
Other Discrete Manufacturing	24	25	27	29	31	33	35	37	40
Automotive	227	274	332	401	509	647	822	1016	1166
Other Transport Equipment	50	57	64	73	83	95	108	123	141
Electrical	47	52	57	64	71	79	88	97	108
Semiconductors	16	19	23	28	34	42	51	61	75
Computing & Electronics	92	109	130	154	184	219	261	311	372
Machinery	106	120	134	151	170	191	215	242	273
Other Non Metallic	12	12	13	14	14	15	16	16	17
Rubber & Plastics	17	18	20	22	23	26	28	30	33
Paper Products & Printing	14	15	16	17	18	19	20	21	22
Wood Products	7	8	8	8	9	10	10	11	12
Textiles & Leather	14	14	15	16	18	19	20	22	23

Europe Smart grid investment and modernisation across the region will result in continued demand from energy markets. Automotive and Pharma are also high growth sectors



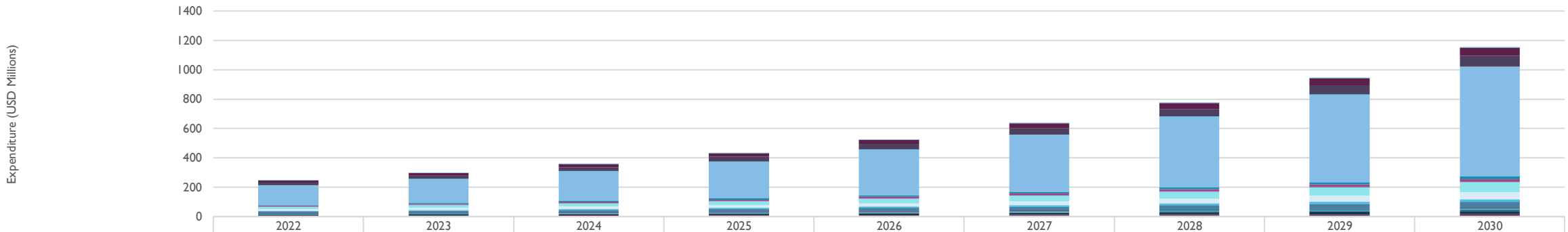


Europe The significant manufacturing base and supply chain in Germany means that it will continue to be the dominant regional market for DX and investment in OT cybersecurity



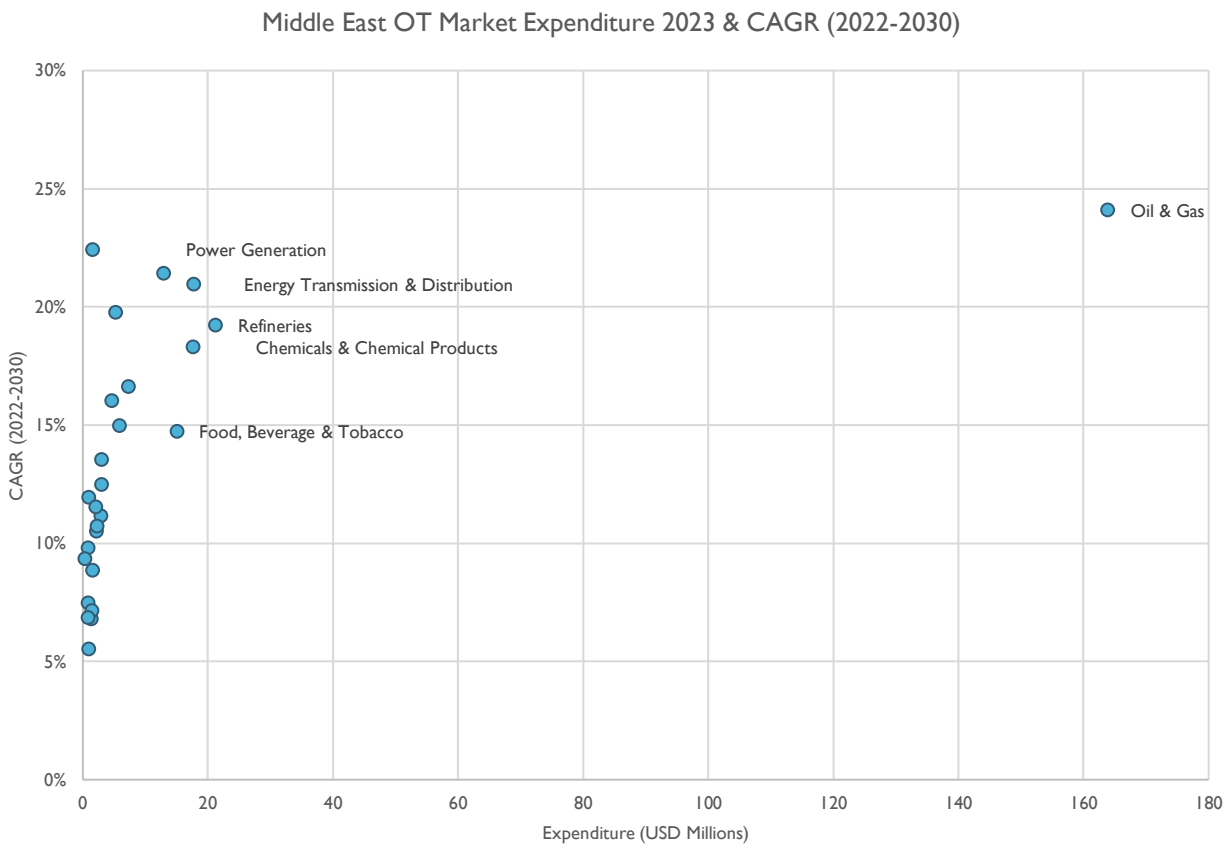
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other	59	65	72	79	90	103	118	134	151
Hungary	23	26	30	34	40	47	55	63	73
Greece	22	26	30	34	41	50	60	71	82
Portugal	27	31	36	42	50	59	71	84	97
Czech Republic	10	12	14	17	20	25	30	36	43
Romania	17	20	23	28	34	42	52	63	76
Finland	31	36	41	48	57	67	80	95	110
Denmark	29	34	39	45	54	65	78	91	106
Austria	45	52	62	72	88	106	130	155	185
Norway	35	41	49	57	71	87	108	131	155
Ireland	75	88	105	124	154	190	236	285	340
Belgium	40	47	55	64	77	93	113	135	158
Sweden	47	56	65	77	94	115	141	170	202
Poland	67	78	91	106	128	155	189	226	267
Switzerland	81	96	114	136	167	205	252	306	365
Turkiye	84	95	107	121	137	155	175	199	226
Netherlands	64	74	87	102	123	148	179	213	250
Spain	94	111	131	155	190	232	285	344	409
Italy	167	194	227	265	319	384	465	553	652
France	171	201	236	278	338	411	500	600	711
United Kingdom	189	220	256	298	359	432	521	619	706
Germany	428	499	583	681	822	995	1206	1438	1583

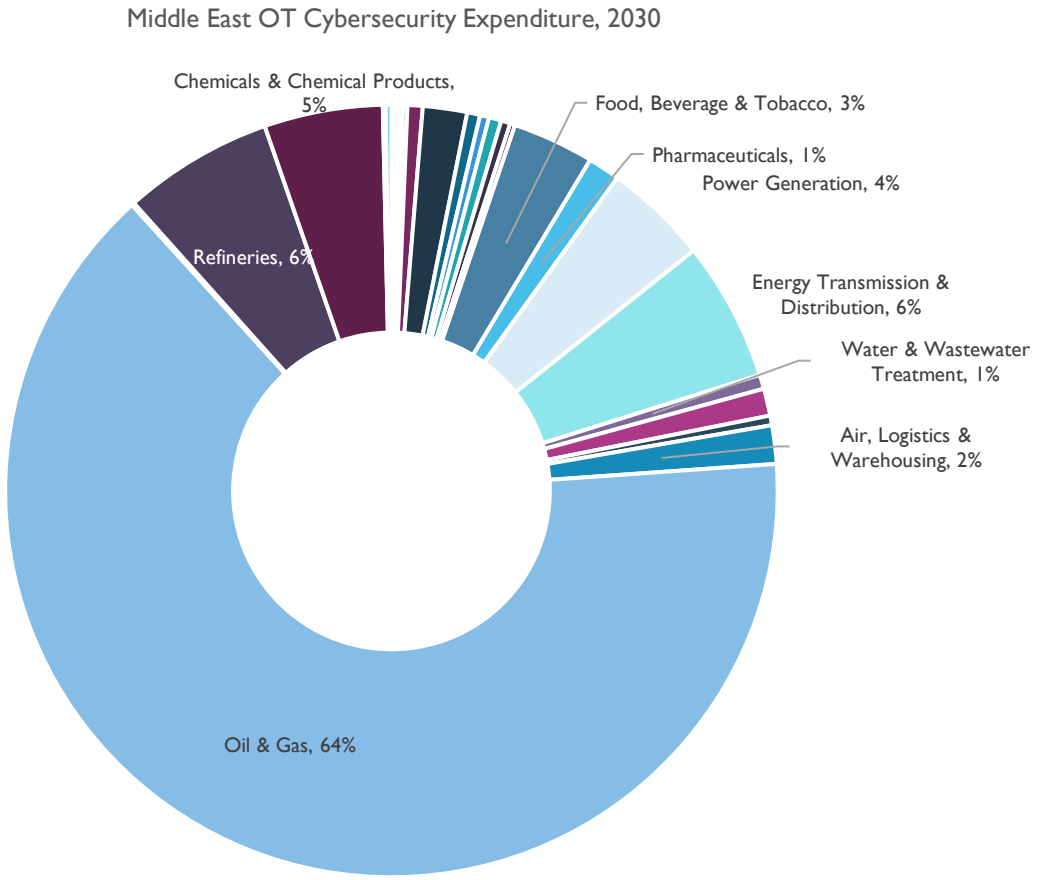
Middle East TAM for 2023-2030 is $5.1B with a CAGR of 21%



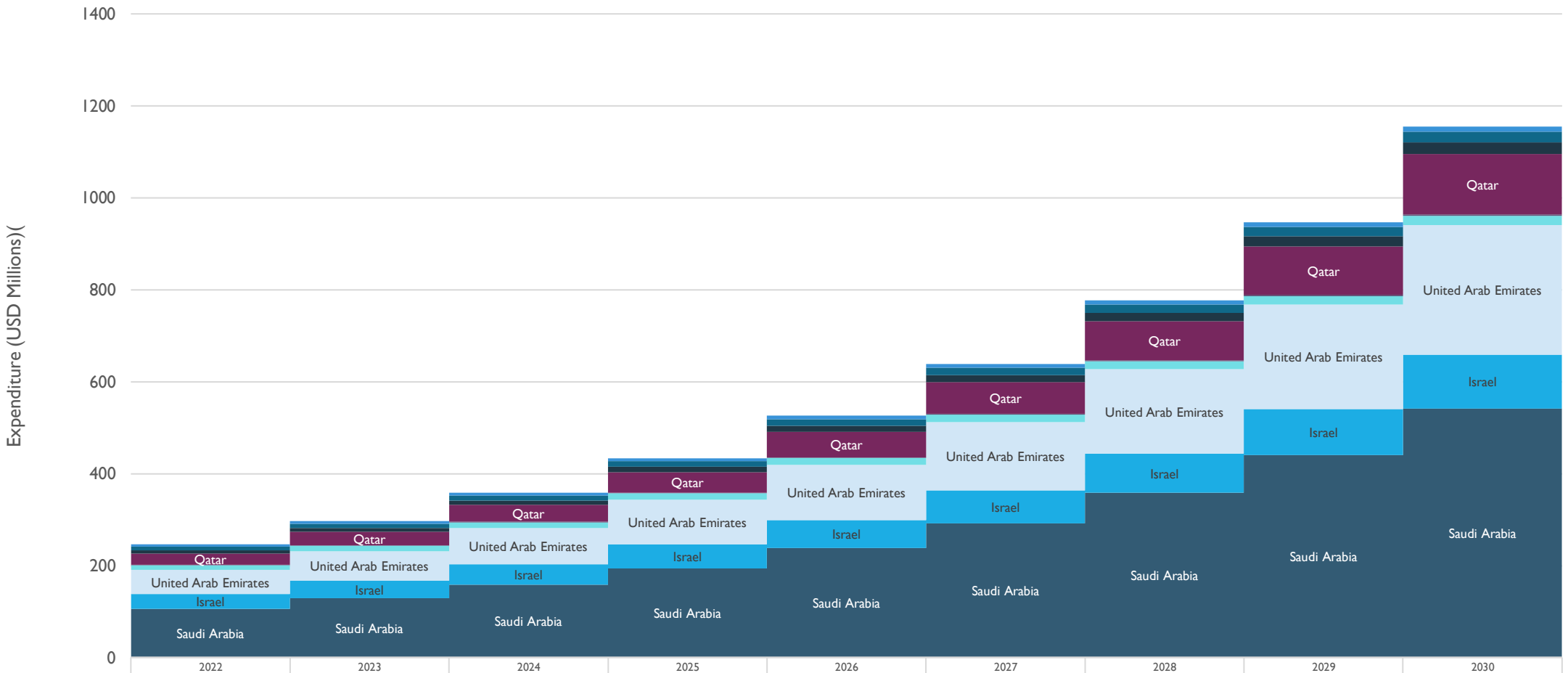
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	1	2	2	2	2	2	2	3	3
Basic Metals	1	1	1	1	1	1	1	1	1
Chemicals & Chemical Products	15	18	21	25	29	34	41	48	57
Refineries	18	21	25	30	36	43	51	61	73
Mining	1	1	1	1	1	1	1	1	1
Oil & Gas	132	164	203	252	312	388	481	598	744
Air, Logistics & Warehousing	4	5	6	8	9	11	13	15	19
Maritime	2	2	3	3	3	3	4	4	5
Rail	4	5	5	6	7	8	10	11	13
Water & Wastewater Treatment	3	3	3	4	4	5	5	6	7
Energy Transmission & Distribution	15	18	21	26	31	38	46	56	67
Power Generation	11	13	16	19	23	28	34	41	50
Pharmaceuticals	5	6	7	8	9	10	12	13	15
Food, Beverage & Tobacco	13	15	17	20	23	26	30	34	40
Other Discrete Manufacturing	1	1	2	2	2	2	2	2	2
Automotive	2	2	2	3	3	3	4	4	5
Other Transport Equipment	3	3	3	3	4	4	5	5	6
Electrical	2	2	2	3	3	3	4	4	4
Semiconductors	1	2	2	2	3	3	4	5	6
Computing & Electronics	6	7	8	10	12	13	16	18	21
Machinery	3	3	3	4	4	5	6	6	7
Other Non Metallic	1	1	1	1	2	2	2	2	2
Rubber & Plastics	1	1	1	1	1	1	2	2	2
Paper Products & Printing	1	1	1	1	1	1	1	1	1
Wood Products	0	0	0	0	0	0	1	1	1
Textiles & Leather	1	1	1	1	1	1	1	1	2

Middle East Oil & Gas and related industry sectors including refining and chemicals will remain the dominant OT cybersecurity market in the region despite various diversification plans



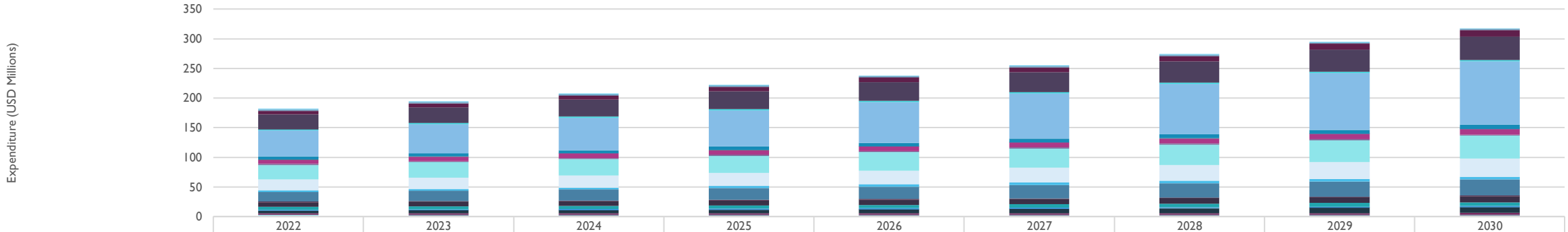


Middle East Petroleum economies are the main investors in OT cybersecurity in the region



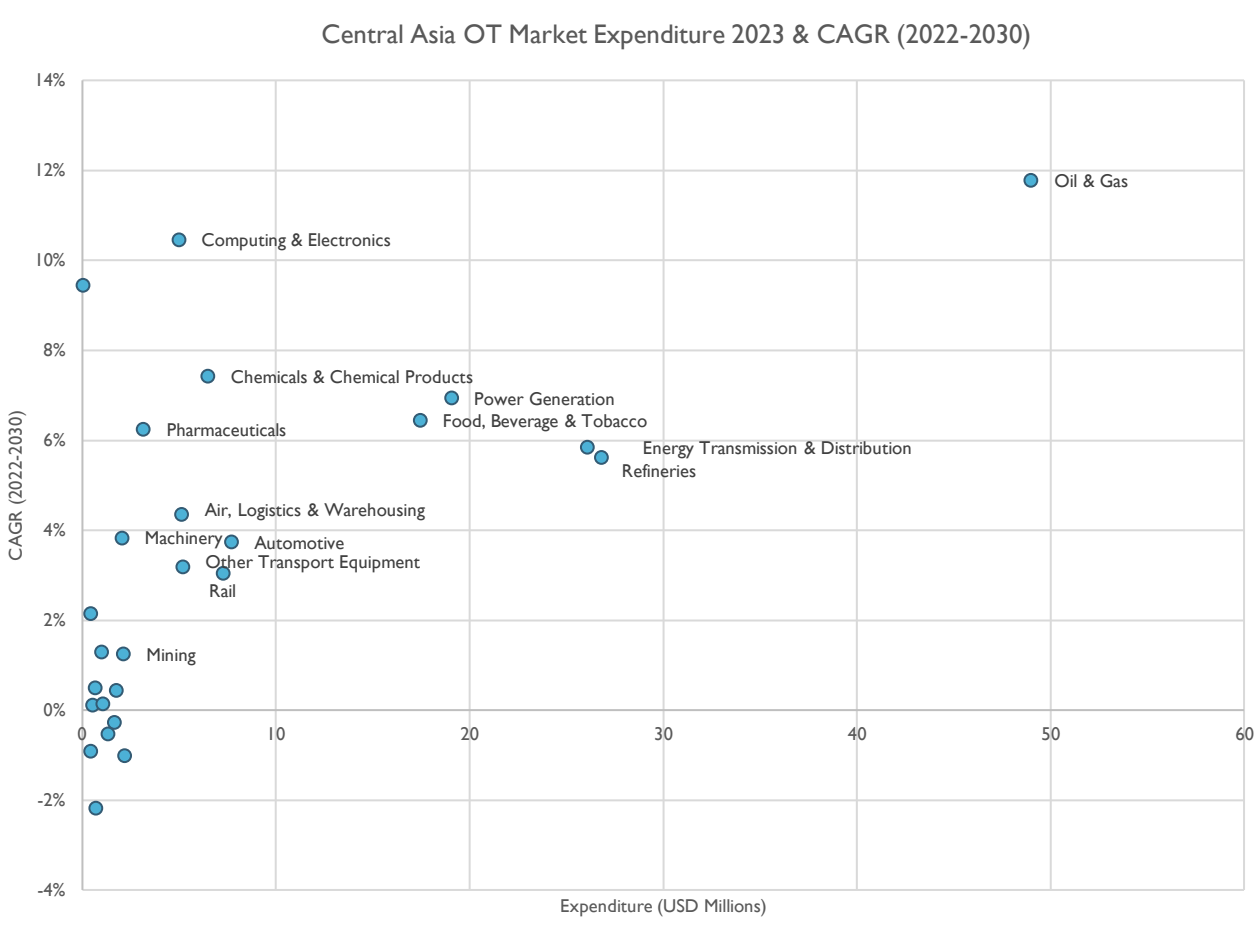
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other	5	6	6	7	7	8	9	10	11
Oman	9	10	11	12	14	16	18	20	23
Kuwait	7	8	10	11	13	16	18	22	26
Qatar	24	29	36	45	56	69	85	106	131
Iraq	1	1	1	1	2	2	2	2	3
Iran	11	11	12	13	15	16	17	19	21
United Arab Emirates	52	64	79	97	120	149	184	227	281
Israel	32	38	44	52	61	72	85	100	117
Saudi Arabia	106	130	159	194	238	292	359	441	542

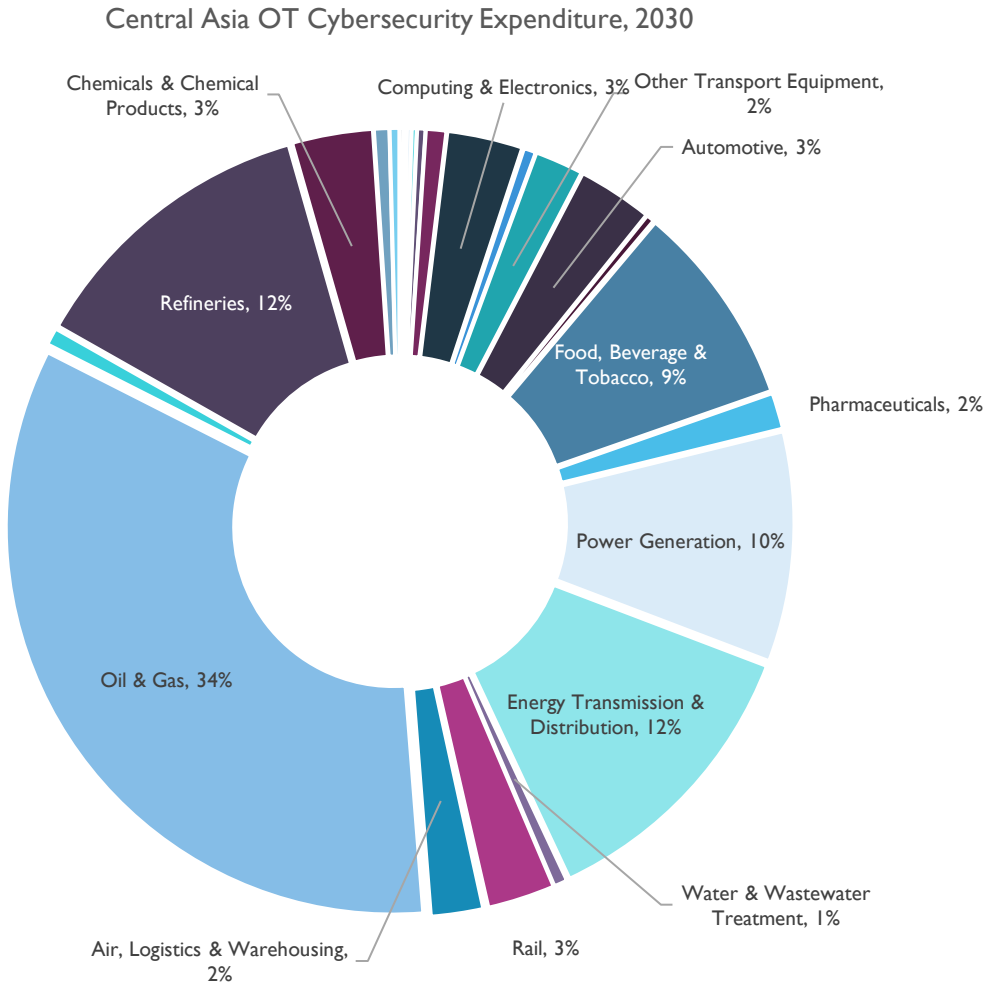
Central Asia TAM for 2023-2030 is $2B with a CAGR of 7%



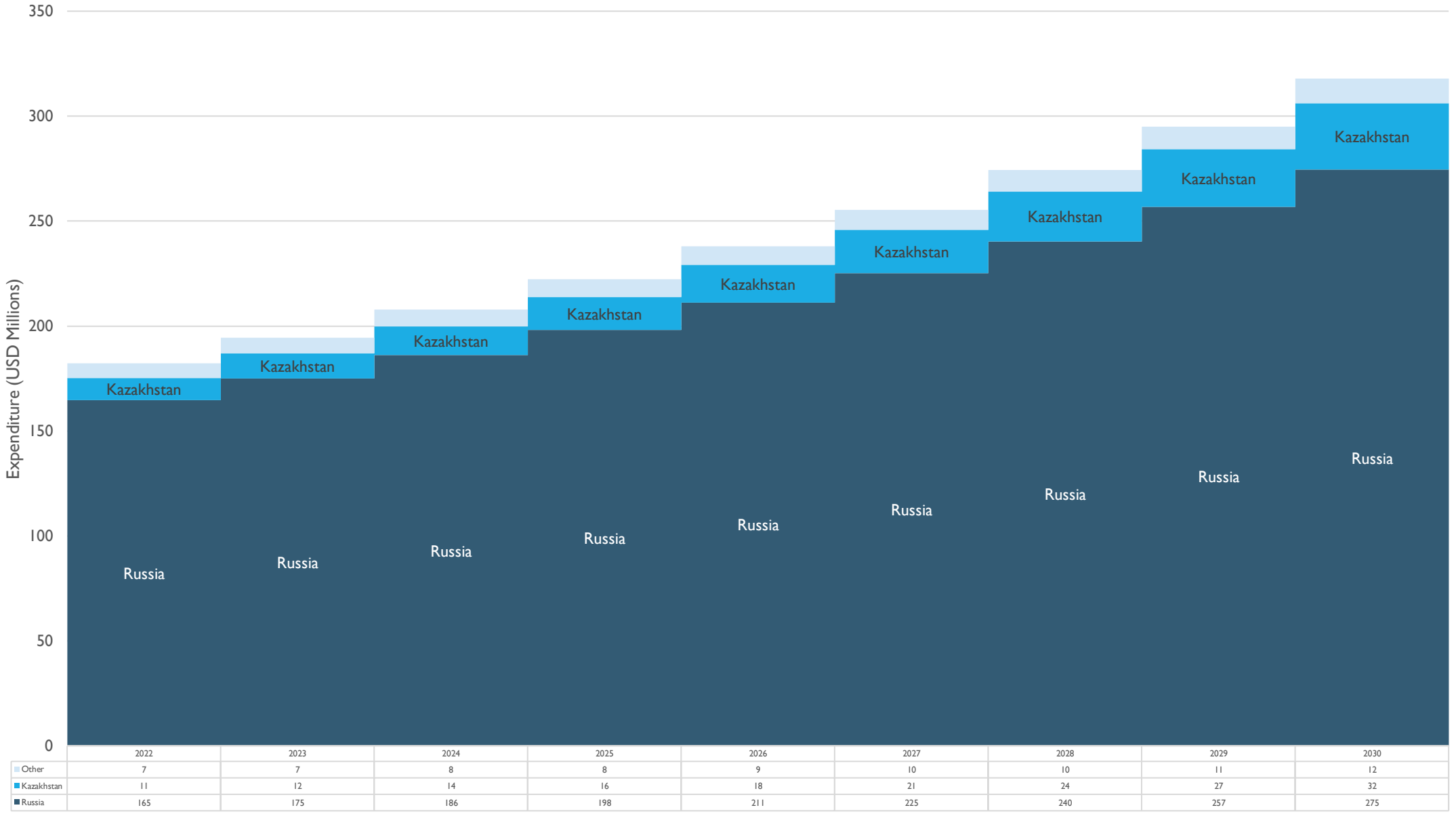
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	1	1	1	1	1	1	1	1	1
Basic Metals	2	2	2	2	2	2	2	2	2
Chemicals & Chemical Products	6	6	7	7	8	9	9	10	11
Refineries	25	27	28	30	32	33	35	37	39
Mining	2	2	2	2	2	2	2	2	2
Oil & Gas	44	49	55	61	68	76	85	96	107
Air, Logistics & Warehousing	5	5	5	6	6	6	6	7	7
Maritime	0	0	0	0	0	0	0	0	1
Rail	7	7	7	8	8	8	8	9	9
Water & Wastewater Treatment	2	2	2	2	2	2	2	2	2
Energy Transmission & Distribution	25	26	28	29	31	33	35	37	39
Power Generation	18	19	20	22	23	25	27	29	31
Pharmaceuticals	3	3	3	4	4	4	4	5	5
Food, Beverage & Tobacco	16	17	19	20	21	22	24	25	27
Other Discrete Manufacturing	1	1	1	1	1	1	1	1	1
Automotive	7	8	8	8	9	9	9	10	10
Other Transport Equipment	5	5	5	6	6	6	6	6	6
Electrical	2	2	2	2	2	2	2	2	2
Semiconductors	0	0	0	0	0	0	0	0	0
Computing & Electronics	5	5	6	6	7	7	8	9	10
Machinery	2	2	2	2	2	2	3	3	3
Other Non Metallic	1	1	1	1	1	1	1	1	1
Rubber & Plastics	1	1	1	1	1	1	1	1	1
Paper Products & Printing	1	1	1	1	1	1	1	1	1
Wood Products	0	0	0	0	0	0	0	0	0
Textiles & Leather	1	1	1	1	1	1	1	1	1

Central Asia Oil & Gas production and refining is the main segment accounting for ~50% of OT cybersecurity expenditure. Low investment is expected from the small manufacturing base.



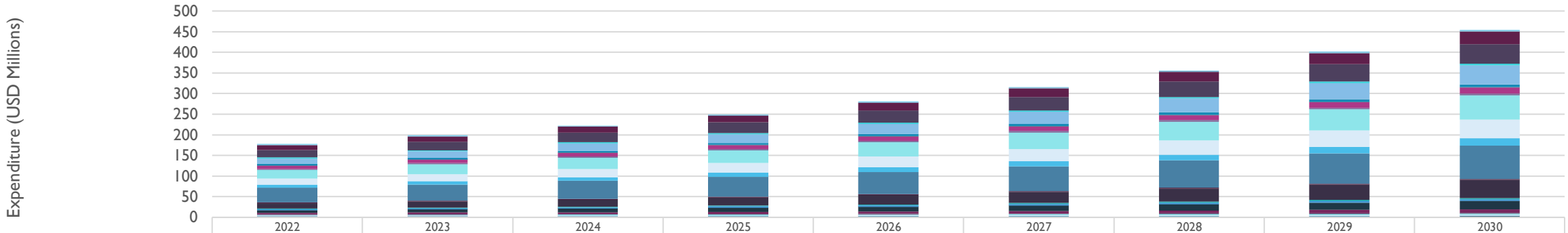


Central Asia Russia dominates the region and whilst the economy is shrinking due to sanctions, high O&G demand from China and India will likely sustain investment in infrastructure



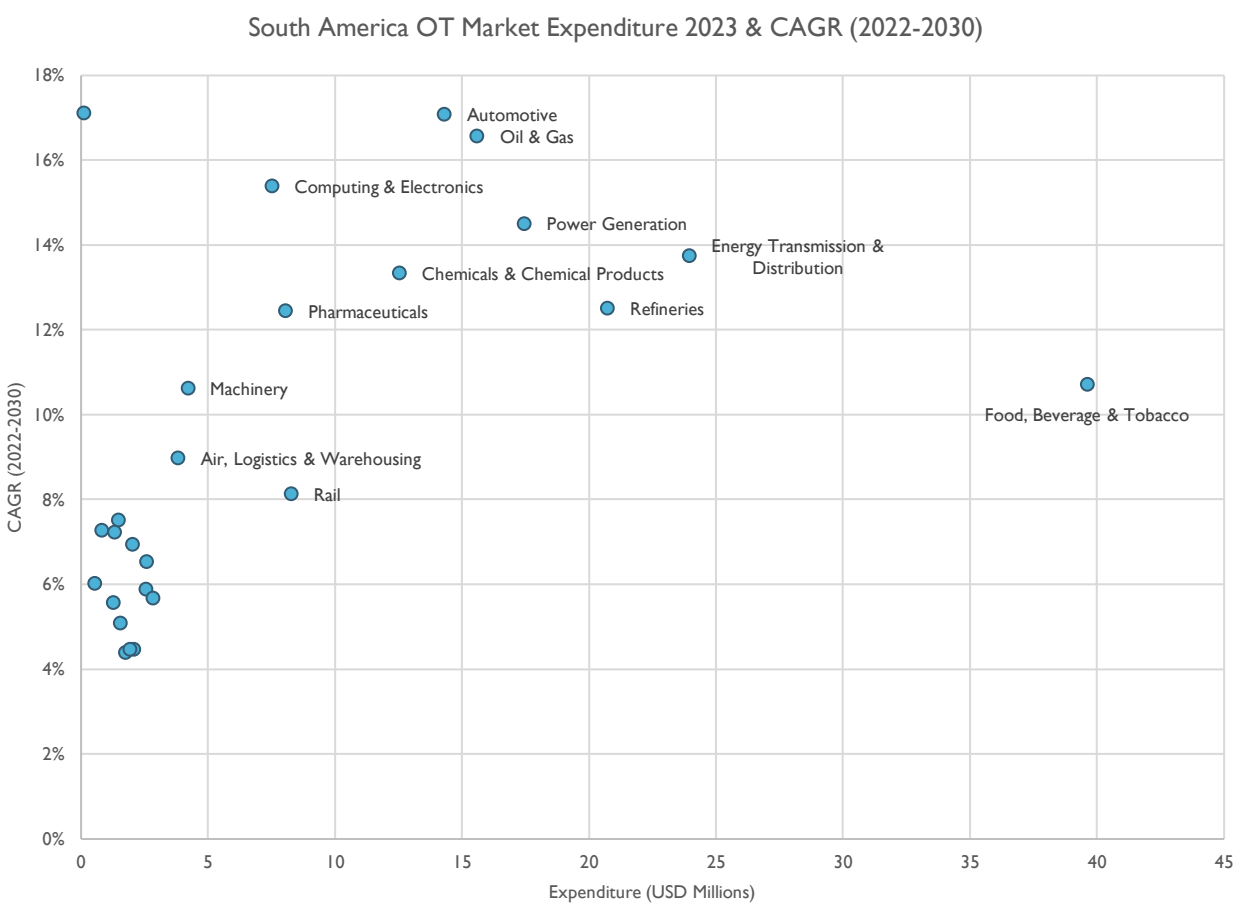
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other	7	7	8	8	9	10	10	11	12
Kazakhstan	11	12	14	16	18	21	24	27	32
Russia	165	175	186	198	211	225	240	257	275

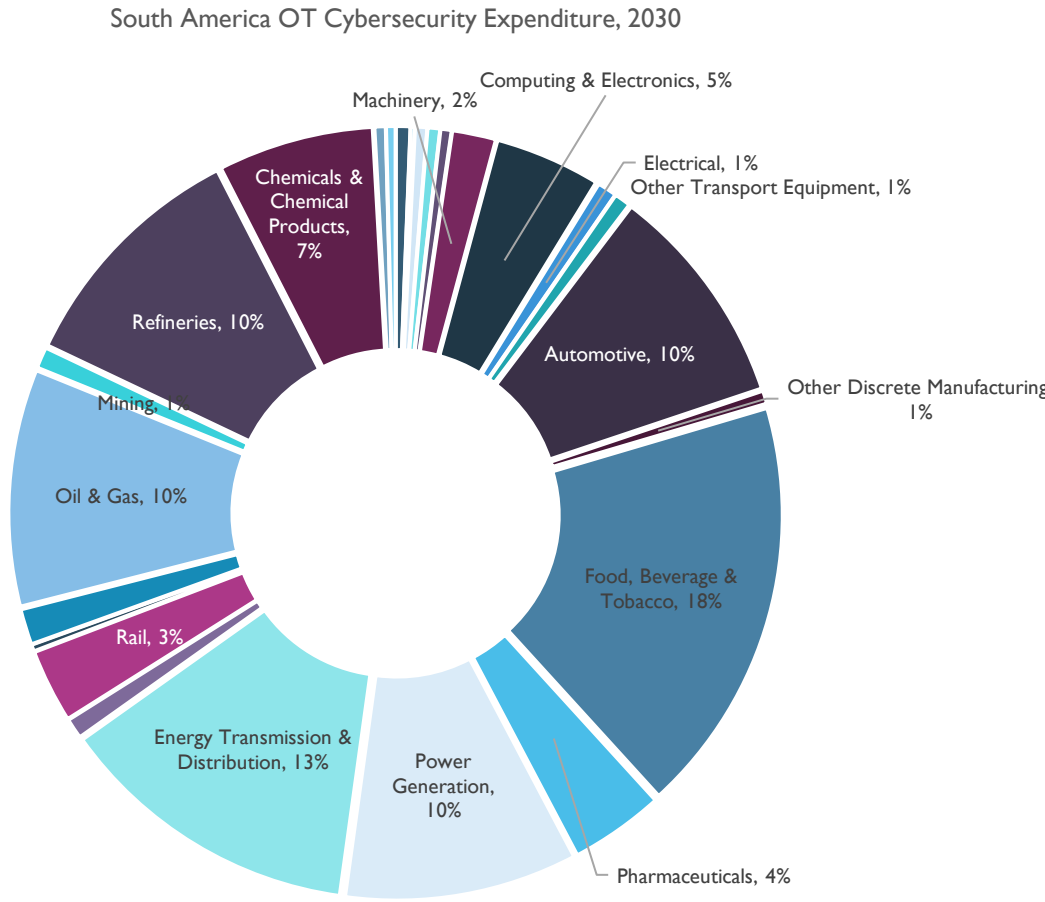
South America TAM is $2.5B with a CAGR of 13%



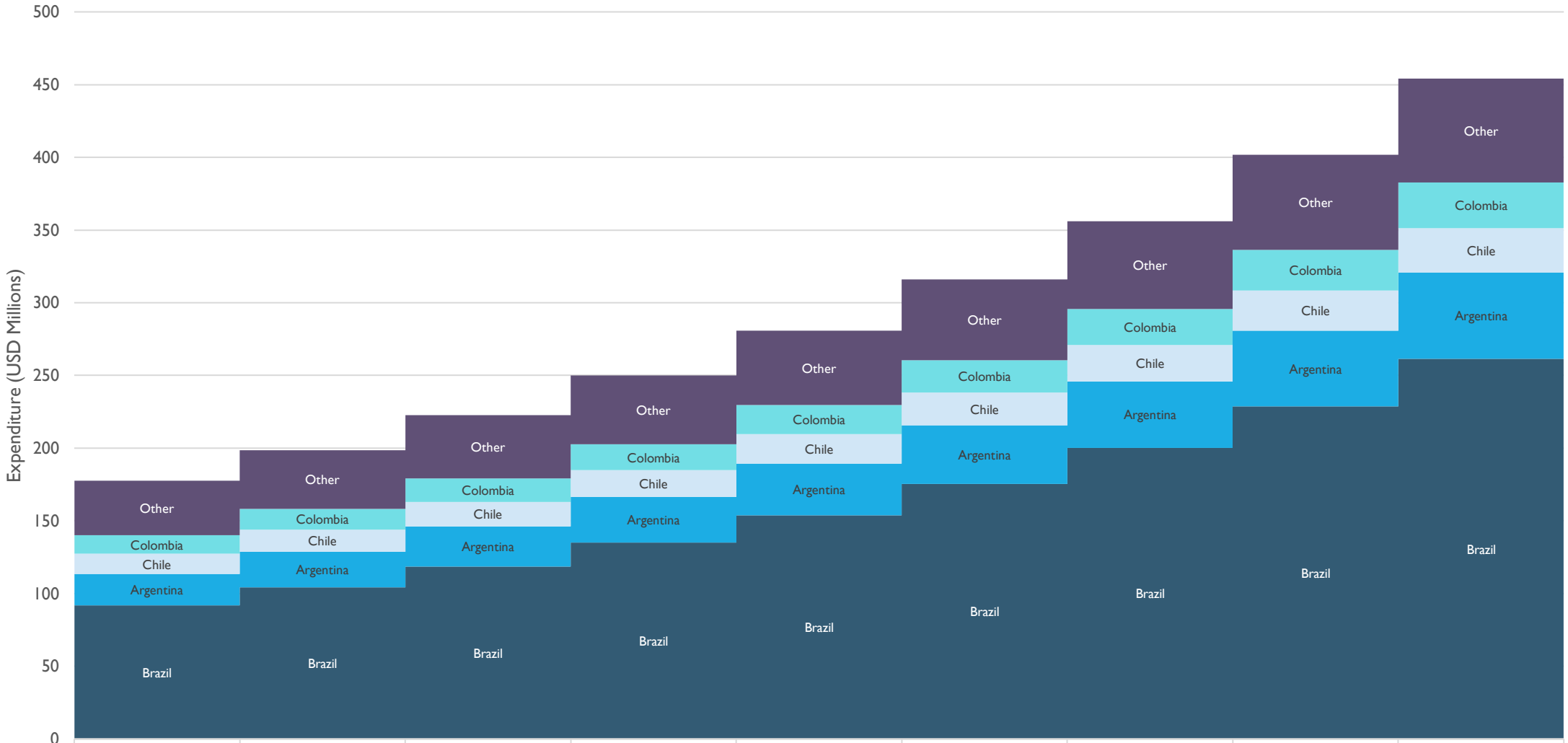
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	1	1	1	1	1	2	2	2	2
Basic Metals	1	2	2	2	2	2	2	2	2
Chemicals & Chemical Products	11	13	14	16	18	21	23	27	30
Refineries	18	21	23	26	29	33	37	42	47
Mining	3	3	3	3	3	4	4	4	4
Oil & Gas	13	16	18	21	24	29	33	39	46
Air, Logistics & Warehousing	3	4	4	5	5	5	6	6	7
Maritime	1	1	1	1	1	1	1	1	1
Rail	8	8	9	10	10	11	12	13	14
Water & Wastewater Treatment	2	3	3	3	3	3	4	4	4
Energy Transmission & Distribution	21	24	27	31	35	40	46	52	59
Power Generation	15	17	20	23	26	30	34	39	45
Pharmaceuticals	7	8	9	10	11	13	14	16	18
Food, Beverage & Tobacco	36	40	44	48	54	59	66	73	81
Other Discrete Manufacturing	2	2	2	2	2	2	2	2	3
Automotive	12	14	17	20	23	27	31	37	43
Other Transport Equipment	2	2	2	2	2	3	3	3	3
Electrical	2	3	3	3	3	3	3	4	4
Semiconductors	0	0	0	0	0	0	0	0	0
Computing & Electronics	7	8	9	10	11	13	15	18	21
Machinery	4	4	5	5	6	6	7	8	9
Other Non Metallic	1	1	1	2	2	2	2	2	2
Rubber & Plastics	1	1	2	2	2	2	2	2	2
Paper Products & Printing	2	2	2	2	2	2	2	2	2
Wood Products	1	1	1	1	1	1	1	1	1
Textiles & Leather	2	2	2	2	2	2	3	3	3

South America High F&B production in the region is the largest OT cybersecurity investment area whilst process industries including O&G and Energy are also significant sectors.



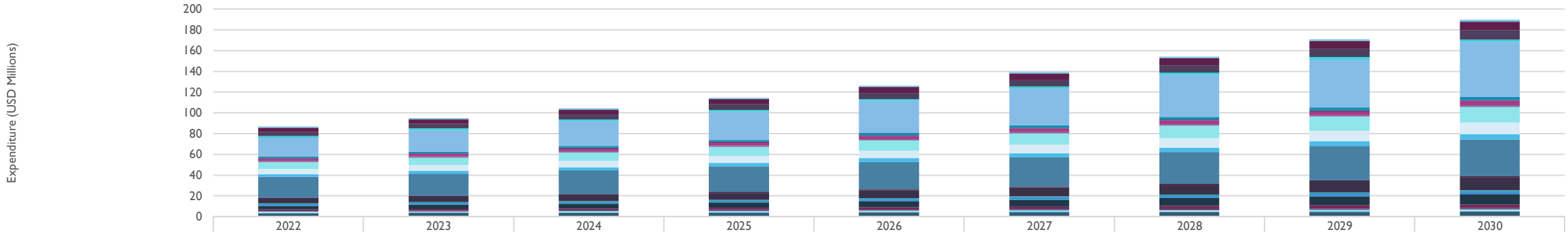


South America Brazil is the largest economy in the region and is characterised by a large F&B sector and growing investment in O&G.



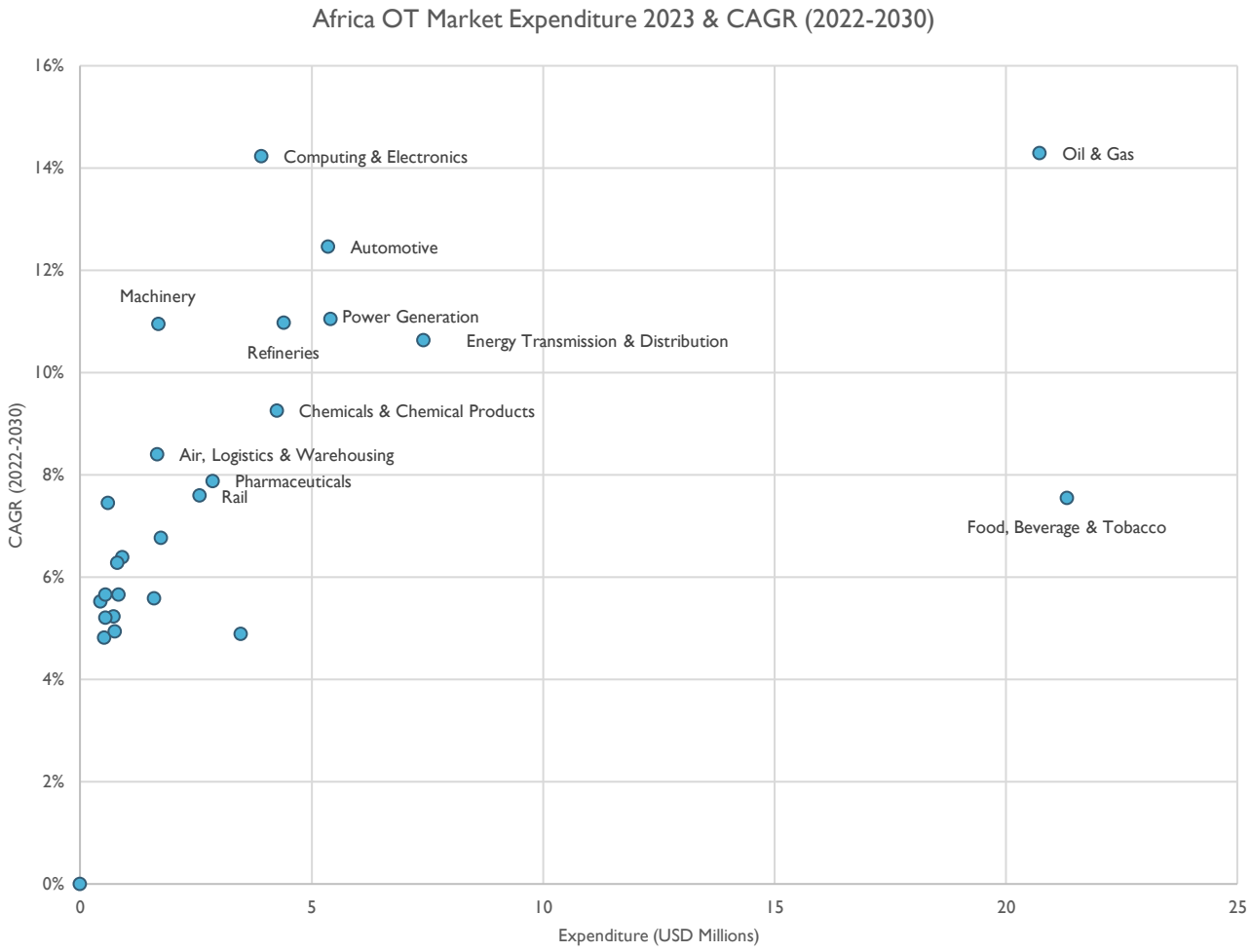
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other	37	40	44	47	51	56	60	66	71
Colombia	13	14	16	18	20	22	25	28	31
Chile	14	15	17	18	20	23	25	28	30
Argentina	22	24	28	31	36	40	46	52	59
Brazil	92	104	119	135	154	175	200	229	261

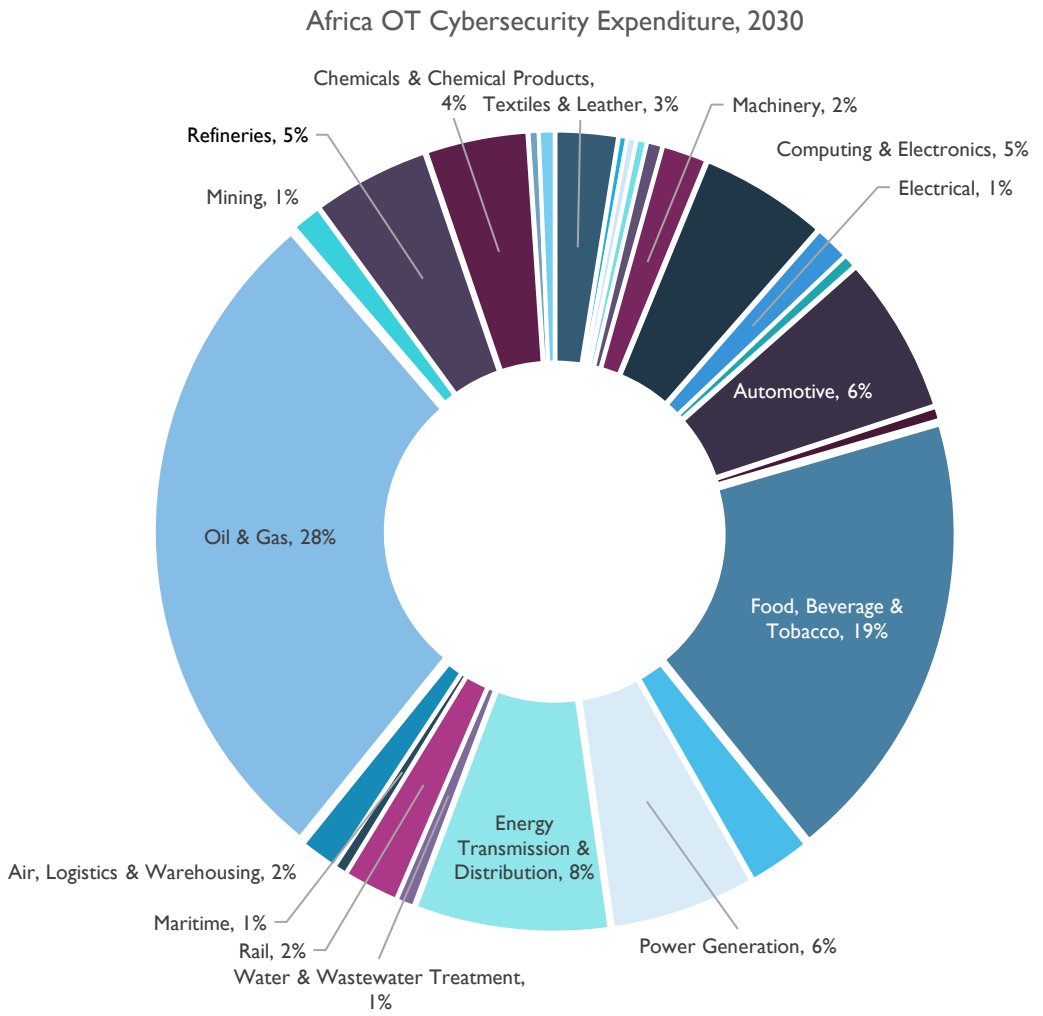
Africa TAM for 2023-2030 is $1.1B with a CAGR of 10%



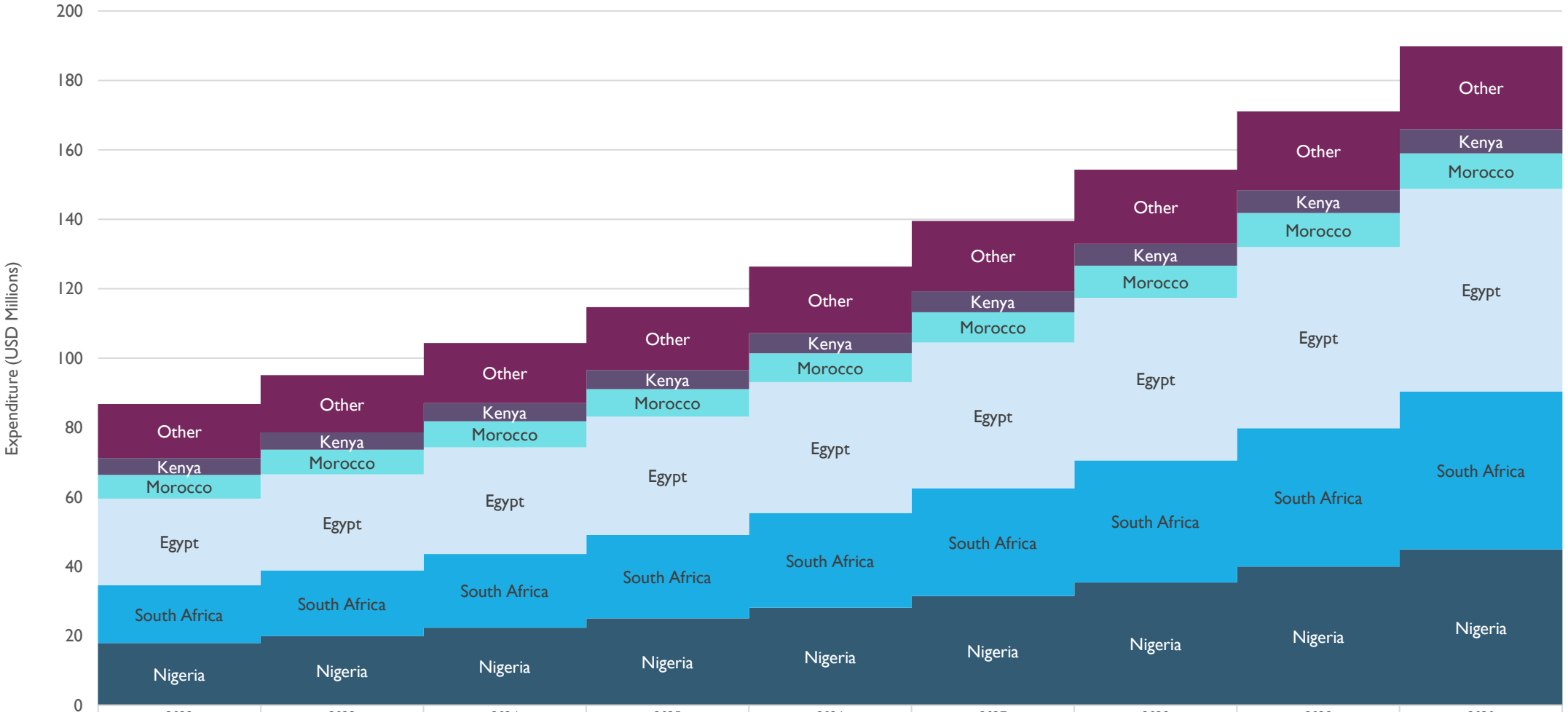
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Fabricated Metals	1	1	1	1	1	1	1	1	1
Basic Metals	1	1	1	1	1	1	1	1	1
Chemicals & Chemical Products	4	4	5	5	5	6	7	7	8
Refineries	4	4	5	5	6	7	7	8	9
Mining	2	2	2	2	2	2	2	2	2
Oil & Gas	18	21	24	27	31	35	40	46	53
Air, Logistics & Warehousing	2	2	2	2	2	2	2	3	3
Maritime	1	1	1	1	1	1	1	1	1
Rail	2	3	3	3	3	3	4	4	4
Water & Wastewater Treatment	1	1	1	1	1	1	1	1	1
Energy Transmission & Distribution	7	7	8	9	10	11	12	14	15
Power Generation	5	5	6	7	7	8	9	10	11
Pharmaceuticals	3	3	3	3	4	4	4	5	5
Food, Beverage & Tobacco	20	21	23	25	26	28	31	33	36
Other Discrete Manufacturing	1	1	1	1	1	1	1	1	1
Automotive	5	5	6	7	8	8	10	11	12
Other Transport Equipment	1	1	1	1	1	1	1	1	1
Electrical	2	2	2	2	2	2	2	3	3
Semiconductors	0	0	0	0	0	0	0	0	0
Computing & Electronics	3	4	4	5	6	7	8	9	10
Machinery	2	2	2	2	2	3	3	3	3
Other Non Metallic	1	1	1	1	1	1	1	1	1
Rubber & Plastics	1	1	1	1	1	1	1	1	1
Paper Products & Printing	0	1	1	1	1	1	1	1	1
Wood Products	0	0	0	0	1	1	1	1	1
Textiles & Leather	3	3	4	4	4	4	4	5	5

Africa Expenditure on OT cybersecurity services is small and mainly related to O&G producing countries or pockets of manufacturing mainly related to F&B production.





Africa Nigeria, South Africa and Egypt are the largest investors in OT cybersecurity whilst the remaining countries have very low levels of expenditure.



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other	16	16	17	18	19	20	21	23	24
Kenya	5	5	5	6	6	6	6	7	7
Morocco	7	7	7	8	8	9	9	10	10
Egypt	25	28	31	34	38	42	47	52	58
South Africa	17	19	21	24	27	31	35	40	46
Nigeria	18	20	22	25	28	32	35	40	45

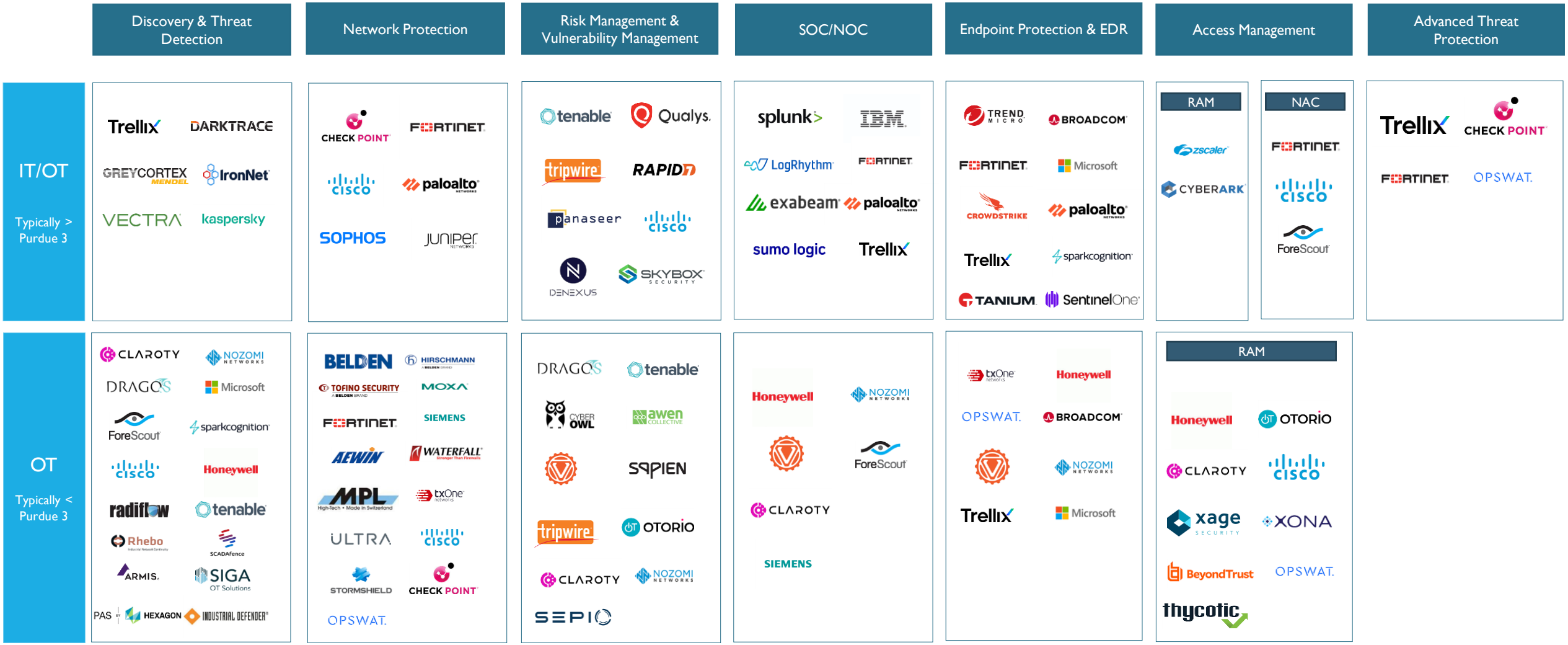
Industrial Cybersecurity Ecosystem

WESTLANDS ADVISORY

Summary

1	There has been no notable consolidation or expansion of the OT cybersecurity ecosystem over the last 12 months with no significant vendor breakthroughs or Mergers & Acquisitions. We have also not observed any notable new consulting or managed security service providers entering the market space.
2	However, there continues to be a high level of strategic activity in the market including significant investment in upgrades and new products. There is a notable trend towards OT vendors expanding product portfolios and investment in cloud delivered services with most vendors now offering on-prem and cloud versions of their products. OT is also a strategic priority for many services firms and there has been increasing investment in staff and infrastructure. We expect this to continue.
3	There is an increasing number of partnerships. This includes integrations between OT vendors, more strategic collaborations between IT and OT vendors, and a growing number of channel partnerships. Apart from expanding channels to market or customer choice, the main reason for partnerships relates to IT/OT convergence.
4	Services firms have invested heavily in developing OT related skills and services and competition is high between organisations. Competitors continue to differentiate themselves through providing an end-to-end service with global capabilities related to product testing, simulations and managed security services.
5	OT Cybersecurity has mainly focused on the industrial network and particularly on identify, protect and detection. Service providers are increasingly focussing on delivering value added services around respond and recover with a focus on operational resilience.
6	Secure-by-Design and Supply Chain Security services are likely to become more prominent over the next few years as regulation strengthens and the concept of operational resilience is extended to product design and suppliers.

The cybersecurity ecosystem remains largely similar to previous years – key differences include increasing product portfolio, start-ups beginning to scale, and new partnerships



*Vendors are illustrative

Innovation remains high; organisations are improving product performance, adding new capabilities and expanding integrations and partnerships

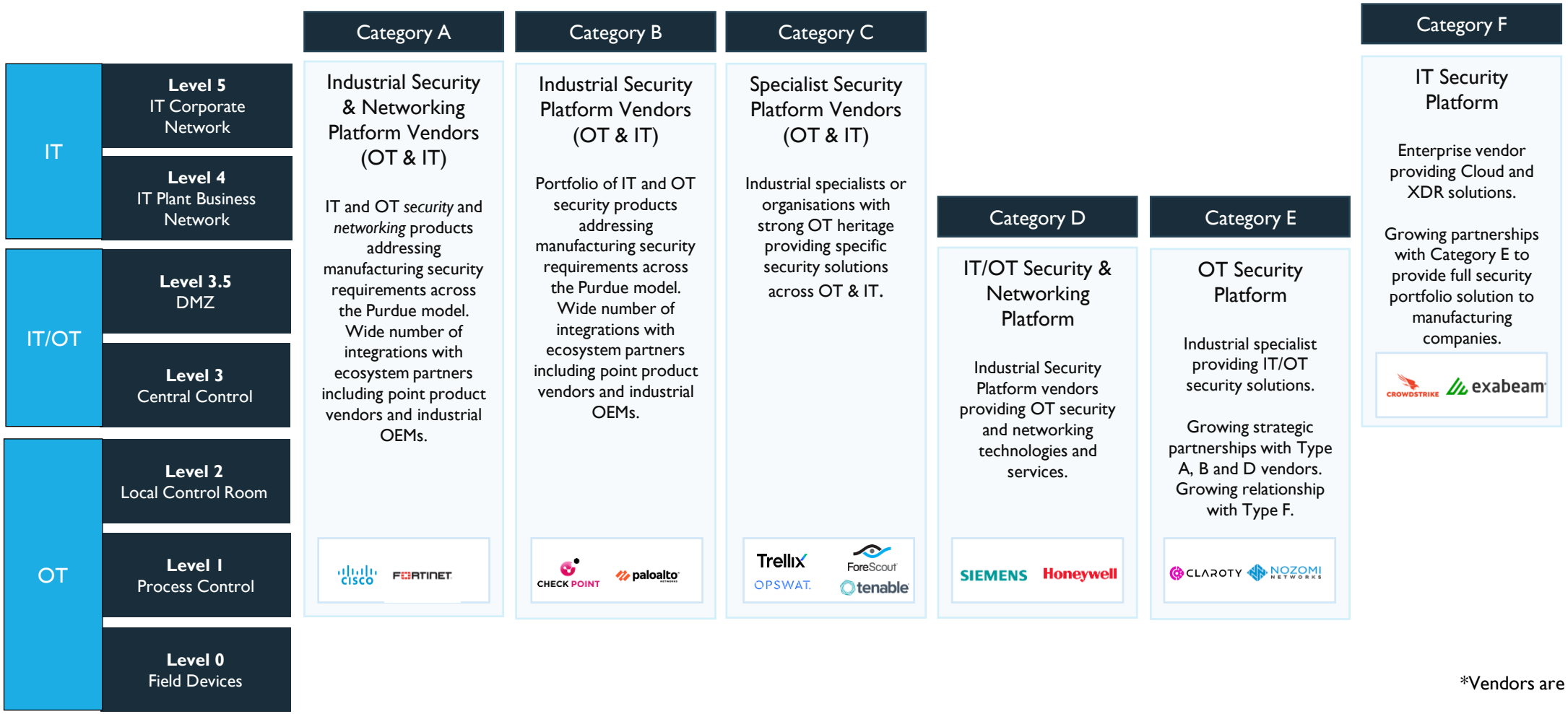
New Capability Capability

*Incomplete list - vendors are illustrative

Despite IT & OT convergence, vendors have not evolved portfolios to include IT security solutions but have focussed on cloud services and strategic partnerships with IT security vendors

WESTLANDS ADVISORY

The following remains largely unchanged from previous years – organisations within Categories are not introducing new solutions to satisfy use-cases at either higher or lower levels in the Purdue model. Innovation has focussed on expanding product portfolios within the Category (for example new endpoint, detection, analytics or risk tools). There is increasing strategic activity between the Categories, partly in response to increasing convergence between IT & OT.



*Vendors are illustrative

Managed Security Services is a growing requirement within OT and includes a range of company types with different skills and capabilities

	MNO's	MDR	IT Services	Engineering & Cyber
	Orange Cyberdefense, T-Systems, NTT, BT	Secureworks, Kudelski Security, Optiv, Trustwave, Mandiant	Atos, IBM, Fujitsu	Jacobs, Thales
S	Strong relationships with industrials, globalised, and networking expertise	Specialised managed security service provider, strong IT security expertise and partner network	Customer relationships, strong IT security services and products, manufacturing DX capability	Strong OT networking experience and consulting in critical, complex industries. Vendor agnostic
W	OT engineering expertise particularly around operations management	Regional specialism, OT security expertise may be lacking	Lower level of expertise related to monitoring of industrial processes	High priced for manufacturing sectors, sometimes lacking global coverage

	Automation Vendors	Professional Services Firms	Security Vendor Services	Vertical Market Specialists
	Siemens, Honeywell, Schneider Electric, Rockwell Automation, Yokogawa, ABB	EY, KPMG, Accenture, Capgemini, Deloitte., pwc	Dragos, Verve	SkyHelm, Mission Secure, Applied Risk (a DNV company)
S	Deep OT networking and operations experience, global and strong installed base and customer relationships	Scale and experience of providing solutions to complex problems. C-level relationships	OT expertise with platform and products	Vertical market specialists in regulated industries. Strong local market expertise and customer management
W	IT security and convergence. Lack of vendor independence	Sometimes lacking deep OT expertise	Scale, globalisation and maturity of operations	Convergence, scale and globalisation of operations

*Vendors are illustrative

The competitive themes remain similar to 2021/2 with continuing investment. New in 2023 is a growing focus on supply chain resilience and secure-by-design

WESTLANDS ADVISORY

Services

End-to-End Service

Growing service portfolios and capabilities addressing NIST CSF and IEC 62433

Secure-by-Design

Sector expertise supporting product and engineering teams designing cyber secure products

Supply Chain Resilience

Advisory services to help asset owners with implementing and monitoring supply chain resilience and risk

Innovation

OT Competency Centres

Centres of Excellence including OT Cyber Ranges, Training, and Co-Innovation

Collaboration

Partnerships between service providers to fill capability gaps

Innovation

New products and services to increase customer value including asset management, cyber simulations, and threat intelligence

Platforms

OT Security Platform

Development of OT security platforms based on MDR principles

IT & OT Security Platform Convergence

Enterprise visibility of networks and risk based on XDR principles

Managed Service Provides continue to improve and expand services through strategic relationships and investments in SOCs and capabilities

WESTLANDS ADVISORY

Technology Expertise

- Familiarity with ICS systems and processes
- Translation of security risk strategy into security controls and response planning
- Familiarity with using best-in-breed technologies
- Breadth and depth of ecosystem relationships
- Ability to integrate threat intelligence into operations

Strategy Alignment

- Ability to meet future business requirements including 'cloudification' of OT
- Experience of managing IT and OT convergence including ability to monitor IT threats and mitigate the risk to OT
- Experience with customer security operating model (customer vs 3rd party SOC)
- Cultural Fit

Industry Knowledge & Performance

- Understanding of local market regulation
- Experience of working within the industry sector including astute understanding of systems and processes including what 'normal' looks like.
- Experience with all relevant ICS vendor protocols
- Demonstrable experience of working with peers

Service Performance

- Full service portfolio including risk consulting, implementation, Managed Detection & Response, and OT Incident Response
- 24/7 SOC in more than one location to guarantee availability.
- Ability to use industry relevant threat intelligence and conduct threat hunting (L3 SOC specialists)
- Reporting and dashboarding
- Performance against SLA's and MTTD and MTTR targets
- Customer Service
- Security Training & Awareness
- CMDB and Asset Management competencies

WA Navigator & Vendor Profiles

WESTLANDS ADVISORY

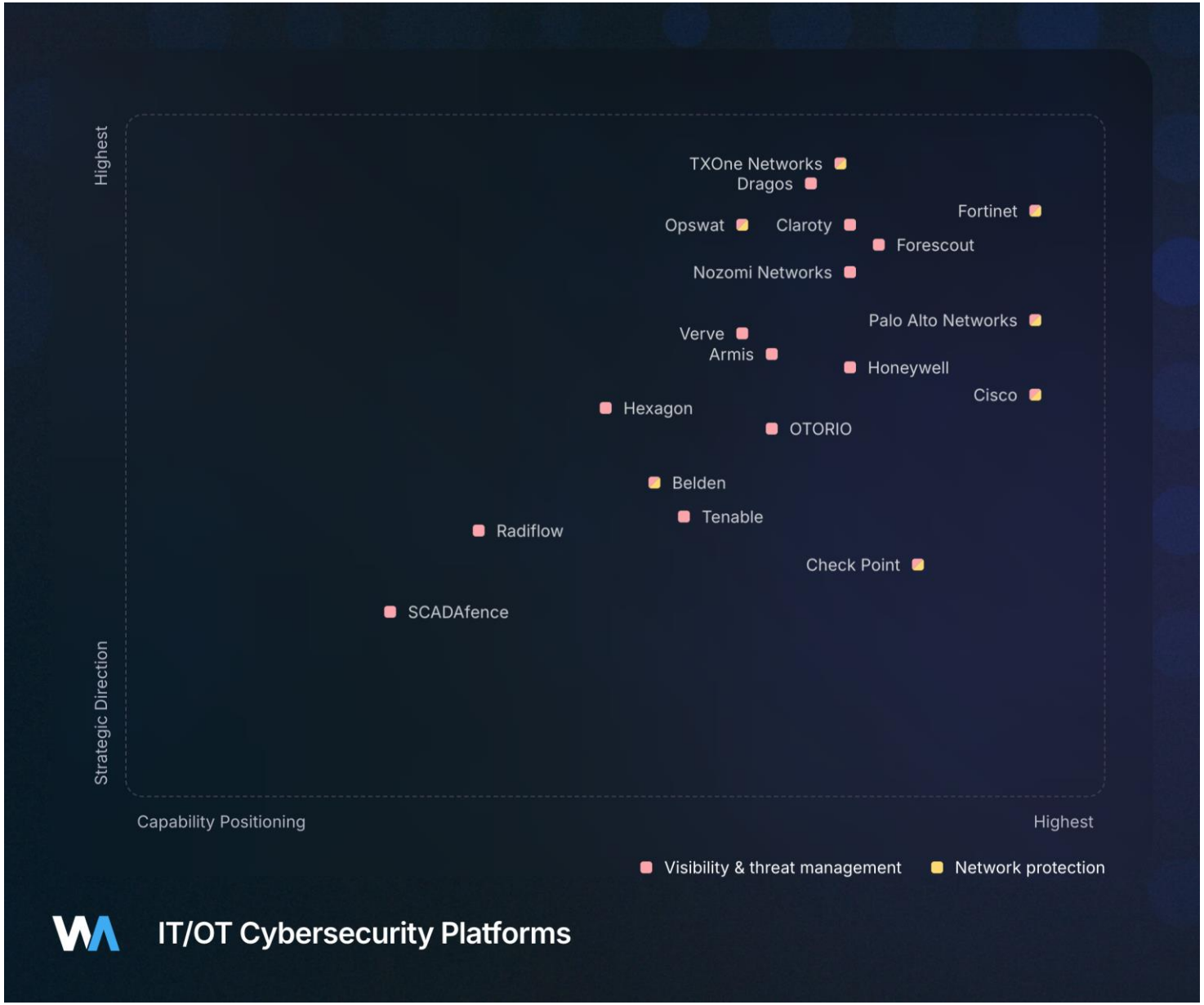
WA Vendor Analysis and Profiles

The following section is an analysis of the leading vendors and relative positioning.

The Navigator measures competitors according to their current **Capability** and the **Strategic Direction** of their business. The insight can be used by Security Leaders to evaluate partners, by competitors to develop strategic planning, and by investors to inform their investment strategy. Our methodology includes an evaluation of the solution and nine strategic categories, using Key Performance Indicators to position competitors against two criteria.

- **Capability** ranks a competitor's current product or service offer according to coverage, the relative market maturity, and the support go-to-market strategy. An organisation with a strong capability score is expected to maintain its market position in the short term.
- **Strategic Direction** is a relative measure of a competitor's organisational trajectory, product roadmap and investment priorities. A strong Strategic Direction indicates an organisation is expected to improve their market performance.

IT/OT Cybersecurity Platform Navigator



Qualification Criteria

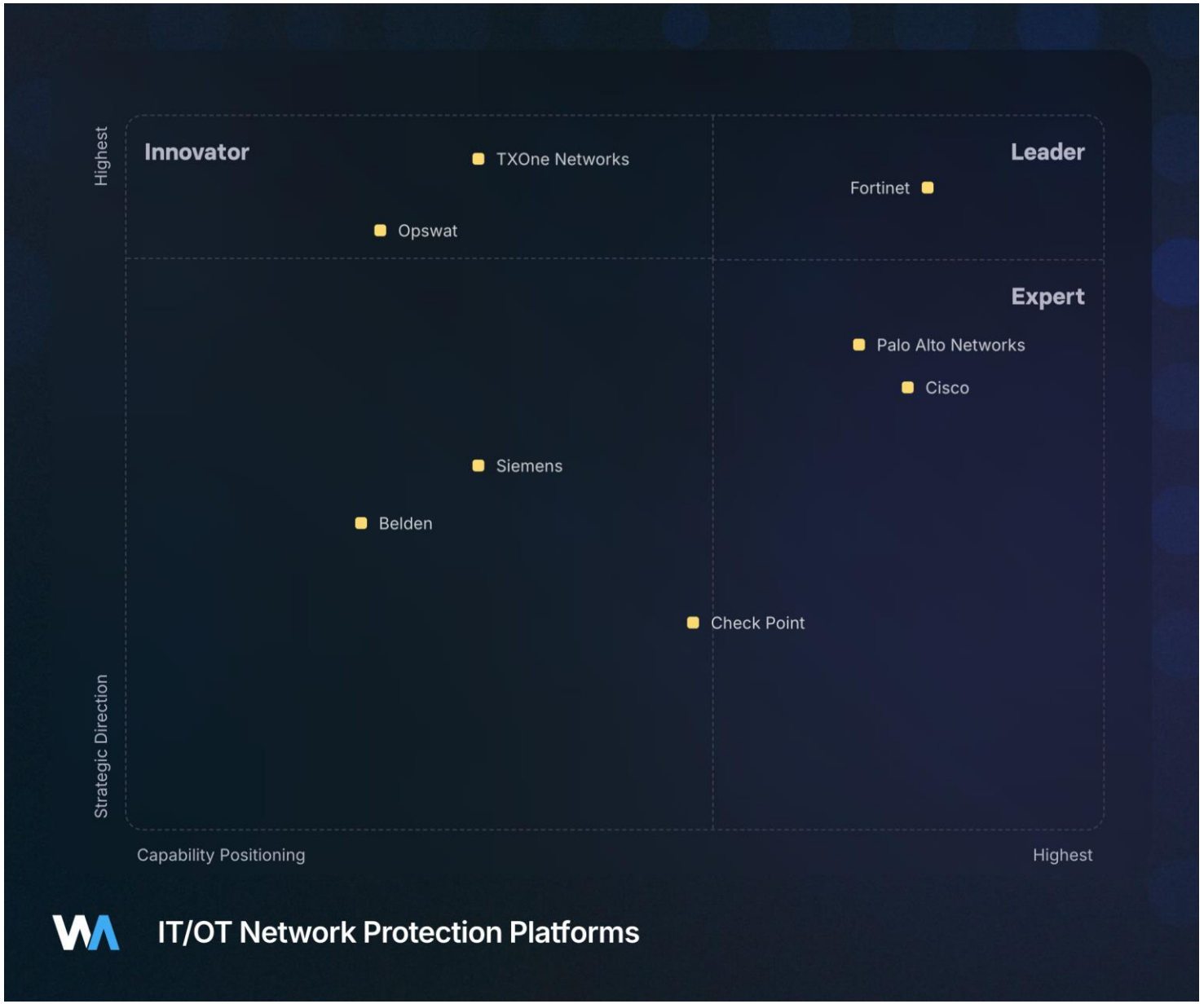
- Company must provide native solutions in 4 of the following categories including a strong customer base.
  - Asset Visibility
  - Network Protection
  - Network Segmentation
  - Vulnerability Management
  - Risk Management
  - Endpoint Protection
  - Secure Access
  - Threat Detection
  - Security Ops & IR
  - Back-up & Recovery
- The relevant products integrate into a centralised platform
- The platform ingests information from other platforms or sources to enrich the data
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations.
- The platform has SIEM capabilities or integrates with SOAR platforms.
- The company has strong coverage in more than one geographical region.

IT/OT Visibility & Threat Management Platform Navigator

Qualification Criteria

- Company must provide native solutions for asset visibility and threat detection
- The relevant products integrate into a centralised platform
- The platform ingests information from other platforms or sources to enrich the data and provide context
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations.
- The platform has SIEM capabilities or integrates with SOAR platforms.
- The company has strong coverage in more than one geographical region

IT/OT Network Protection Platform Navigator



Qualification Criteria

- Company must provide native solutions for OT network protection including all or one of NGFW, IPS and Data Diode.
- The relevant products integrate into a centralised platform with other network protection products including access management.
- The platform ingests information from other platforms or sources to enrich the data and provide context
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations, providing network and device visibility and management
- The platform has SIEM capabilities or integrates with SOAR platforms.
- The company has strong coverage in more than one geographical region

Technology Classifications

Asset Visibility	Passive and Active Scanning, Agent based discovery
Network Protection	Firewalls, IDS and IPS, unidirectional gateways and data diodes
Network Segmentation	Including Firewalls, VLAN's, Access Control Lists (ACL), Software Define Networking, and agentless Micro Segmentation through identification and logical grouping of assets and devices and applying policies to each.
Vulnerability Management	Vulnerability Management
Risk Management	Risk Scoring, Configuration Management, Compliance Management
Endpoint Protection	Endpoint Protection (Malware Scanning, Application Whitelisting, Patch Management) and USB Protection
Secure Access	PAM, VPN, ZTNA
Threat Detection	ML, UEBA, Signatures including deviations from baselines, network flows and event correlation
Security Ops and IR	SIEM, SOAR, XDR, EDR, Playbooks
Back-up & Recovery	Business Continuity Management, Disaster Recovery

Armis

Summary

Armis was founded in Israel in 2015 and is now headquartered in San Francisco. The company has raised $537M over 6 funding rounds and now employs 700+ staff in several offices, the largest of which are in the US, Israel and UK.

The company has grown significantly in recent years, tracking >3.5B assets for customers in 165 countries and has over $100M in ARR. The growth and customer mix has led to a valuation of over $3B.

The Armis proposition is based on its 'Asset Intelligence & Security Platform' that provides passive, real-time and continuous monitoring. This includes:

- Asset discovery across OT and IT networks
- Asset intelligence through profiling and enrichment of the data
- Contextualisation including device relationships and connections
- Identification and prioritisation of vulnerabilities, threats and risks
- Management and orchestration of tasks

Armis' main security use cases include Asset Visibility, Vulnerability and Risk Management and Threat Detection. Through providing complete asset visibility, the Armis platform can augment NAC and Firewall implementations and improve network segmentation.

In addition to the security use cases, the asset visibility and enrichment process can improve an asset owner's operational resilience by delivering insight into asset and network health and performance.

Positioning

Armis has arrived at its OT solution from a different starting position to alternative solutions. The platform is a hybrid solution with SaaS-only management, providing onsite visibility and detection with data sent to the cloud for further analysis and enrichment. The platform monitors both wired, wireless, cloud and remote networks. The benefits of its cloud delivered service includes ease of implementation, scalability and ability to rapidly respond to new and emerging security threats. Future platform investments will focus on improvements to automation, orchestration, threat management and compliance.

The Armis proposition is strong at the executive level, particularly as part of transformational programs across IT and OT, and multiple sites. The customer base reflects a strength in providing solutions to complex industries that are reliant on OT/IoT/IT networks across complex, diversified sites (e.g. airports, maritime, building management networks and medical facilities).

The partner ecosystem is well developed, including many of the main SI's and industrial OEM's who are familiar with Armis' platform. The company also has a wide set of integrations, including the main firewall vendors, MDR partners such as Kroll and Expel, and with OEM's (Siemens and Rockwell Automation). Armis has a strong relationship with Tenable, who share the same investors, and with EDR platform vendor SentinelOne to extend visibility across OT, IoT and IT networks. As a result, Armis can be integrated in large, complex, multi vendor deployments, including SOC/NOC, EDR and CMDBs. Further integrations and industrial partners are expected to follow in 2023/4.

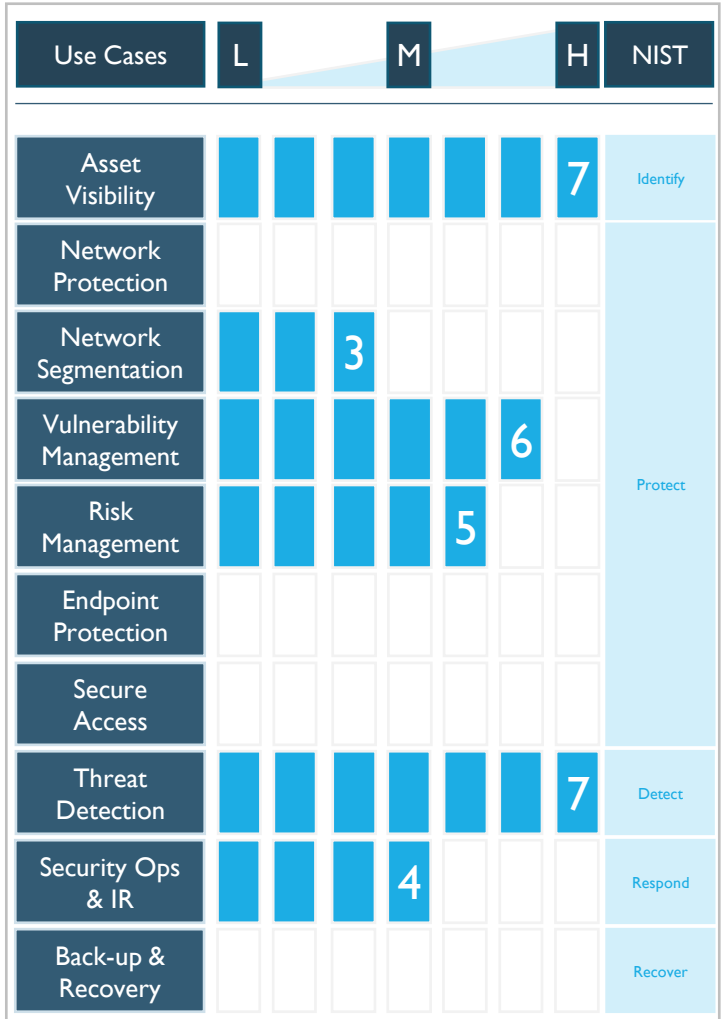
Known for

Mature SaaS Platform

Visibility from device to cloud

Detection across IT/IoT/OT

Native Technology Capability



Check Point

Summary

Check Point is a global cybersecurity solutions provider with sales of $2.3B in FY 2022, a 5% growth in revenues from 2021. In Q1 2023, 45% of company revenues were reported in the EMEA region, 43% Americas and the remainder in APAC.

Check Point's product offering is broad, providing enterprises with a range of solutions to protect the modern enterprise.

- Quantum – Network Security including NGFW, SD-WAN and Zero Trust
- CloudGuard – Cloud Security
- Harmony – User and Access Security including Endpoint, SASE and email.
- Horizon – Security Operations

The product portfolio addresses many categories across the MITRE ATT&CK Framework, providing customers with "Comprehensive, Collaborative and Consolidated" coverage and management of security operations.

Check Point IoT Protect for Industrial is the lead offer for OT and forms part of the Quantum Network Security proposition. The service combines network segmentation and policy enforcement with asset discovery.

Check Point launched Infinity Global Services in 2023 to provide partners and customers with support to advance security programs. The services include risk assessments, design and architecture review, cybersecurity training and awareness and managed detection and incident response.

Positioning

Check Point's customer proposition is based on securing industrial operators' infrastructure, operations and data across IT and OT networks, both on-prem and in the cloud. The Infinity licencing agreement – subcriptions now comprise 50% of Check Point's business – includes the software, hardware, security services and support required for coverage of IT and OT networks.

The OT security service, Check Point IoT Protection for Industrial, provides engineering and security teams with OT asset and network visibility, network segmentation and virtual patching, and management of remote access to industrial assets. The Check Point product range includes the wired and wireless1570R, providing advanced threat protection through SandBlast and visibility into >1,400 protocols and commands.

The partner ecosystem includes industrial visibility and threat detection vendors (Claroty, Nozomi Networks, RAD, SACADfence and Armis) and security operations platforms (Splunk, Servicenow etc.)

Known for

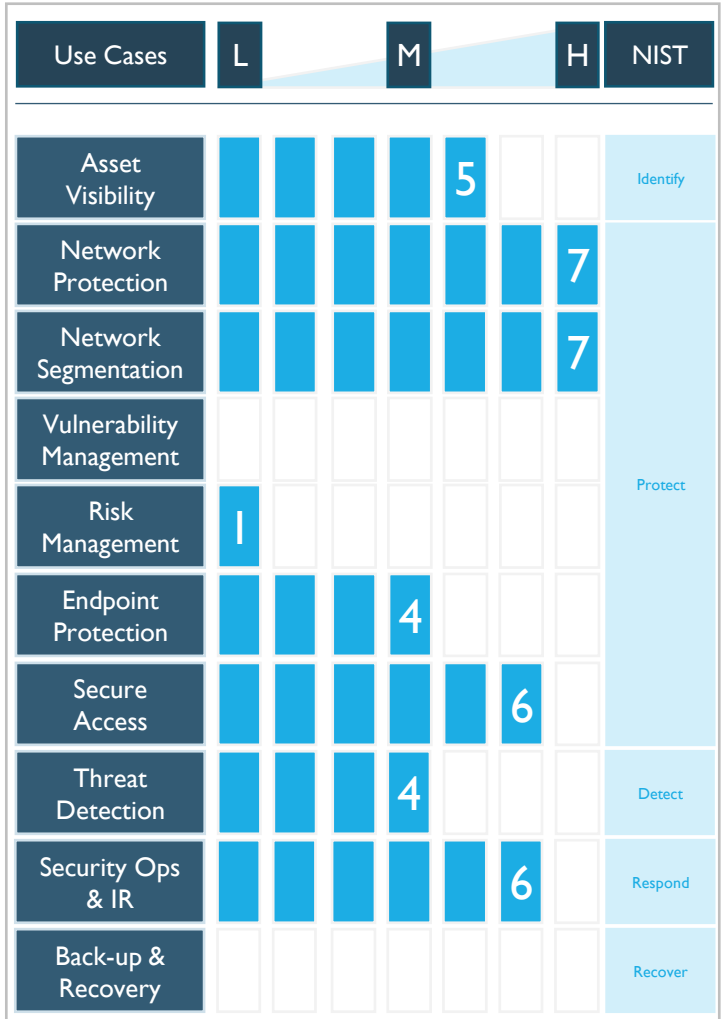
Comprehensive Security Portfolio

Reliable Partner

Advanced Threat Protection including Sandboxing

Global Partner Network

Native Technology Capability



Cisco

Summary

Cisco is a publicly listed company headquartered in San Jose, United States. The company is one of the leading networking and cybersecurity vendors with an extensive product portfolio for industrial customers. The industrial segment has consistently been one of the fastest growing businesses within Cisco, reporting double digit growth for a number of years. The company has provided industrial networking products for over 20 years, developing a broad portfolio of solutions through investment in product development and acquisitions.

Products include:

- Secure Firewall (ISA3000)
- Industrial Switches (IE1000, 3100, 3300, 3400, 4K, 5K, 9300)
- Industrial Wireless (IW9167EH, 9165E, 9165D, 6300H & ESW6300)
- Industrial Router (IR1101, IR1800, IR8100, IR8300)
- Asset Visibility & Threat Detection (Cyber Vision)
- Secure Endpoint
- Secure Equipment Access
- Zero Trust Network Access (Duo)
- Operational Visibility (Edge Intelligence, Industrial Asset Vision)
- Network Access Control (Identity Services Engine)
- Security Operations (Cisco XDR (formerly SecureX))
- Cisco's range of enterprise security products and services including Talos and Security Service Edge solution (Umbrella)

Cisco addresses all OT cybersecurity uses cases through its extensive portfolio, offering customers on-prem and cloud deployments. The range of IT security products provides customers with the option of IT and OT coverage from a single vendor or as part of a multi-vendor solution.

Positioning

- Cisco's Industrial Threat Defense proposition provides customers with a comprehensive portfolio of industrial networking solutions with an extensive range of cybersecurity products that can be integrated into a single, scalable solution. Customers benefit from Cisco's deep experience of industrial networks and architectural design experience across the spectrum of industrial markets.
- Cisco's 4 step approach to industrial security includes protection between IT and OT networks, visibility, segmentation, and management of security operations, providing an end-to-end security proposition covering NIST CSF.
- Cyber Vision, formerly Sentryo, is the visibility and detection solution, and offers customers on-prem and cloud deployment options and a range of buying options. Cyber Vision is available as both a network sensor integrated into Cisco network-elements (e.g. IE3300 and 3400 switches), providing DPI and eliminating the need for SPAN solutions, or as a hardware sensor in mainly brownfield, multi-vendor operations.
- The OT solution is supported by threat intelligence from Cisco Talos which has proven experience in industrial markets including incident response support.
- Cisco offers a wide range of integrations to allow customers to choose 3rd party products. The company also has historical relationships with major industrial OEM's including Rockwell Automation (Stratix and Cyber Vision services), Yokogawa, Schneider Electric and Emerson.

Known for

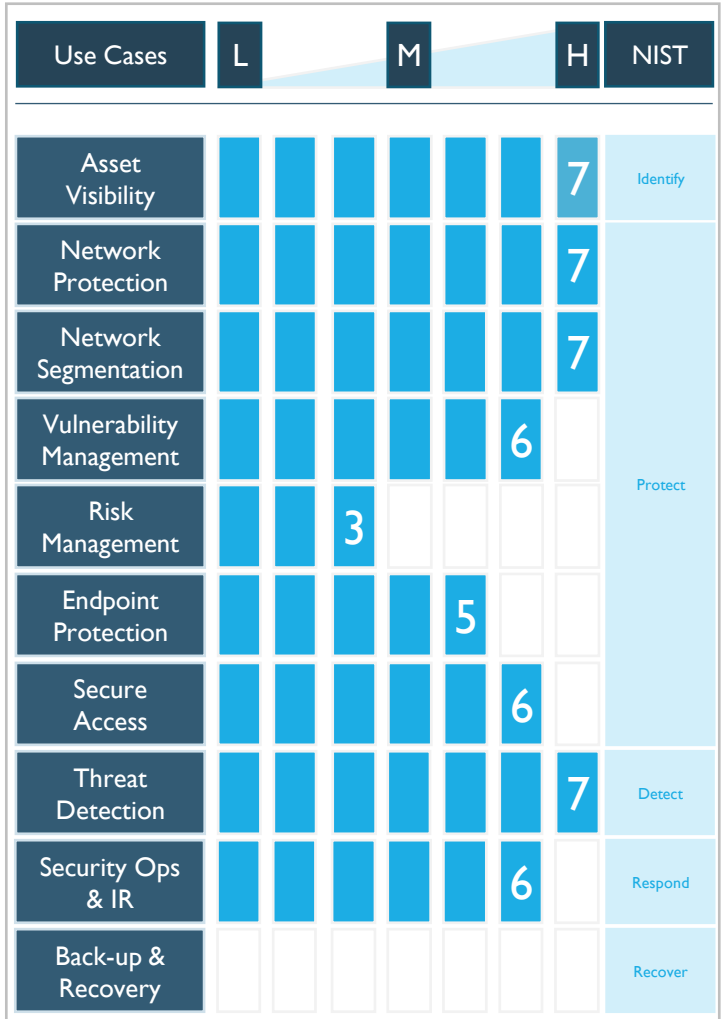
Global leader in industrial networking with a high installed base

End-to-End OT cybersecurity solution and equivalent IT capability

Visibility and detection integrated into networking elements

Technical expertise and experience in process and manufacturing industries

Native Technology Capability



Claroty

Summary

Claroty is a cyber-physical systems protection company, founded in 2015. It is headquartered in New York City with the engineering team largely based in Israel. The company is currently at Series E funding ($635M in total), with investors including notable industrial OEMs and VCs. This has enabled ongoing investment in the product, marketing and sales teams resulting in high employee and revenue growth.

Claroty's positioning has evolved from its initial focus on providing visibility and security controls for industrial environments to now include commercial and healthcare environments as well, as part of its Extended Internet of Things (XIoT) proposition.

The industrial platform proposition includes products that enable customers to achieve 4 critical cybersecurity outcomes for OT networks and connected devices at the plant (e.g. cameras, lighting systems etc.)

- Continuous vulnerability and risk management
- Zero Trust-based network protection
- Threat detection and mitigation

The key product offering includes:

- xDome - SaaS platform with subscriptions available for different use-cases including Risk Management powered by Team82's Threat Research to score risk and prioritise remediation.
- Secure Remote Access (SRA)
- Continuous Threat Detection (On-prem service with subscriptions available for different use-cases)

Use cases addressed by Claroty include Asset Discovery, Asset & Change Management, Network Segmentation, Vulnerability and Risk Management, Secure Access, Threat Detection and Security Operations.

Positioning

Claroty positions itself as the leading industrial Visibility company, using 5 methodologies and covering >450 protocols to identify, map and monitor assets, networks and processes. This includes Claroty Edge, a windows-based edge data collector, passive monitoring, Safe Queries, Project File Analysis, and Ecosystem Enrichment, to provide a "unified, single source of truth". Asset Visibility is one of several cybersecurity use cases addressed by the Claroty platform which also includes vulnerability management and threat detection, and additional outcomes through integrations (e.g. OT context for VMS and SOAR platforms). The proposition extends beyond 'Cyber Resilience' to 'Operational Resilience' including Change Management, Lifecycle Management and Operational Intelligence use cases.

Claroty's industrial partner ecosystem is extensive, and the relationships are mature, integrating with all leading security platforms and tools (NGFW, VMS, EDR, SIEM and CMDB vendors). This includes strategic relationships with Rockwell Automation and Schneider Electric and a new partnership with CrowdStrike which enables customers to deploy EDR safely in industrial operations.

Innovation and investment has focused on improving customer choice, providing on-prem and cloud deployment options, and developing a range of agent/agentless and active/passive detection techniques. Claroty has a relatively higher percentage of engineers and product managers to its peers and has a strong product roadmap. Further platform enhancements and expanded XIoT asset libraries are expected in 2023 alongside other innovations.

Known for

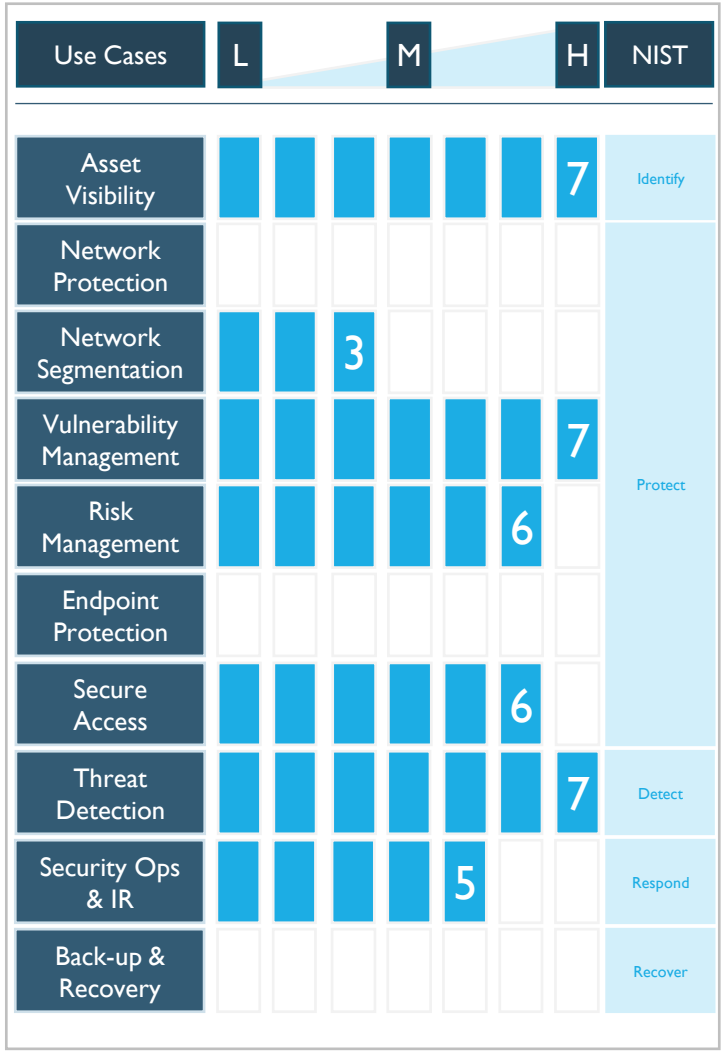
Mature OT Visibility and Threat Detection Platform

Extended Internet of Things (XIoT)

Strong US presence

Ecosystem Partnerships

Native Technology Capability



Dragos

Summary

Dragos was founded in 2016 and has since developed a reputation as an industrial partner, offering a comprehensive set of cybersecurity solutions and services.

Dragos is a private company based in Maryland. The latest funding round was completed in 2021 and to date the company has raised $364M. This has funded investment in the platform and staff – there are currently ~500 employees based mainly in the US. This also reflects Dragos' customer base which is largely North American though the company has expanded to the UK, Canada, Australia, New Zealand and Dubai, and is growing its network in Asia.

Dragos is both a platform and full cybersecurity services vendor. The Dragos Platform discovers and maps assets and networks, identifying vulnerabilities, quantifying risk and automating remediation. The threat detection is supported by industry leading OT-specific intelligence providing SOC analysts with context and supported by playbooks to accelerate response and support investigation.

The platform can be managed by the asset owner, 3rd parties or by Dragos' internal team of experts. The managed services team, OT Watch, augments customer SOC teams, providing ongoing advice, monitoring networks, and proactively hunting for threats. This service includes Incident Response retainers. Aside from managed services, Dragos also provides advisory services from architecture design to penetration testing and tabletop exercises.

Positioning

Dragos is both a technology and services company, providing full partner support for customers including risk assessment, architecture design, platform management and incident response. This differs from industry peers who have a greater focus on using channel partners to consult, integrate and manage OT SOC operations.

Dragos' reputation as a service partner has been developed through its founder's expertise and the assembled team of industry professionals who have deep experience and knowledge of Industrial Control Systems. This highly skilled team has resulted in Dragos being widely recognised as an ICS security consulting partner with a reputation for incident response. The adversary-centric approach that Dragos takes to OT includes a focus on evaluating the Tactics, Techniques and Procedures (TTPs) of threat actors. This is an important component to Dragos' industry leading OT-specific threat intelligence service – Worldview which includes critical alerts, weekly reports, industry specific threat perspectives, quarterly insights, and actionable defensive recommendations.

Dragos is an active contributor to the ICS community and is recognised as a collaborative organisation. This is evident in its advisory roles to governments and participation in international forums. Initiatives also include Neighbourhood Keeper which is a free, anonymised opt-in program for Dragos customers to share insights, and the OT industry's first OT-Cyber Emergency Readiness Team (OT-CERT) which provides free OT cybersecurity resources for small- and midsized organisations.

Known for

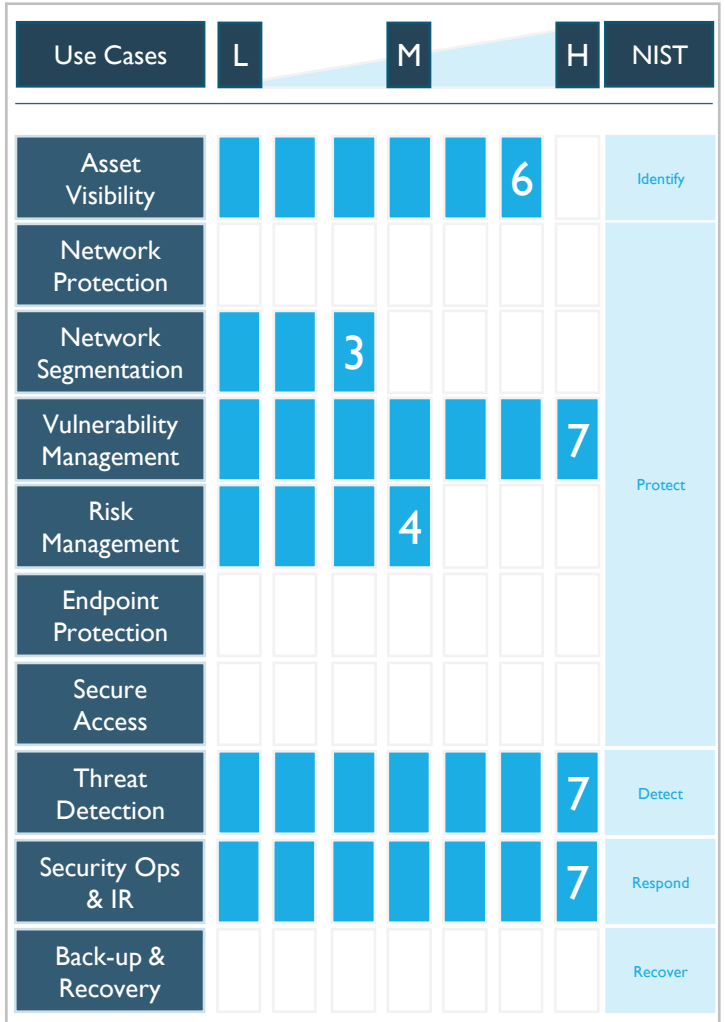
Unique positioning as an OT Platform and Managed Security Services provider

Incident Response

Leading OT-specific threat intelligence and curated vulnerability database

Strong U.S. government relationships

Native Technology Capability



Forescout

Summary

Forescout is a private company Headquartered in San Jose with over 20 years of cybersecurity experience. The company positions itself as the cybersecurity automation company, providing customers with the products and integrations to Discover, Assess & Detect, and Govern assets and network operations. The Forescout Platform is a cloud service that connects with Forescout products, and integrates with SIEM and EDR vendors, to ingest and enrich data with Forescout's threat intelligence from Vedere Labs.

Forescout is a globally recognised company with significant OT expertise. They continue to invest in building regional presence (e.g. Europe and Japan) and developing the network of alliance and channel partners including leading OEM's, Systems Integrators and Service Providers.

Forescout's OT relevant products include;

- 'eyeInspect' asset visibility and threat detection from the acquisition of Security Matters (who offered a product formerly known as, SilentDefense)
- 'eyeSegment' for network segmentation / enforcement
- 'eyeControl' products for device access and compliance
- XDR launched in 2023 through the acquisition of Cysiv, providing visibility, detection and automated response across IT and OT networks.
- 'Assist' is a subscription service providing customers with access and support to Forescout expertise

Product deployment options include on-prem and cloud, using a range of agent/agentless and active/passive detection techniques. Use cases addressed by Forescout includes Asset Visibility and Network Visualisation, Vulnerability Management, Risk Management, Endpoint Protection, Threat Detection, Segmentation, and Incident Response.

Positioning

The Forescout Cybersecurity platform enables asset owners to 'Identify Risk & Exposure' and 'Detect & Respond to Threats'. Platform innovation has focussed on providing cloud and on-prem deployment options, visibility across networks, and improving understanding of the attack surface with technology to automate and remediate. Innovation continues to focus on the user experience to simplify analyst tasks.

The new XDR platform provides customers with visibility across IT/OT networks, ingesting data from >180 data sources, and automating detection and response. Forescout uses a blend of asset discovery techniques including passive, active and hybrid techniques providing customers with non-SPAN options. This includes passive DPI monitoring of over 250 protocols, active endpoint and network infrastructure-based discovery, and API integrations, to provide customers with a variety of options based on their OT network. The threat detection methodology includes 5 techniques, including signatures, UEBA, statistical and context aware ML. Other features include MITRE ATT&CK integration for OT and over 1,500 OT-specific detection rules, models and compliance checks.

The platform is supported by Forescout's leading Threat intelligence team, Vedere Labs. The team uses > 70 global information sources and its own proprietary data lake (>30 billion datapoints collected from monitored IT, IoT and OT devices) to severity, provide context and prioritise risk.

Known for

Mature platform for IT and OT asset and network visibility

Network Access Control for IT and OT operations

Good coverage of NIST CSF and MITRE ATT&CK

Threat Intelligence

Native Technology Capability

Fortinet

Summary

Fortinet is a publicly listed company headquartered in Sunnyvale, United States. The company is one of the leading cybersecurity vendors with a broad, integrated offering of over 50 products that addresses multiple security use cases. The company continues to grow strongly, serving over 600K customers with billings of $5.6B in FY2022.

Investment in research and innovation has remained consistently high resulting in an extensive portfolio of patents (1,285). This is supported by a global network of Development Centers and Centers of Excellence including recent investment in Japan. Fortinet is a leading IT and OT cybersecurity solutions provider to the industrial and critical infrastructure sectors, with a high customer base and strong coverage of all industrial verticals.

The stated company priorities in 2023 are to be number 1 in Network Firewalls, SD-WAN and OT Security. The OT business has grown strongly, outpacing average market growth, due to increased investment in OT-specific products, staff and the sales and marketing operations.

Fortinet's OT Aware Security Fabric is comprised of an extensive range of security products enabling Secure Networking, Zero Trust Access and Security Operations, all supported by security services that includes OT specialized FortiGuard Services, over 3,000 OT application signatures and 600+ OT threat signatures.

Fortinet's native products strongly address most OT cybersecurity use-cases with Tech Alliance ecosystem partners providing complimentary solutions. This provides customers with an end-to-end cybersecurity platform that addresses IEC-62443, NIST CSF, MITRE ATT&CK for ICS and other relevant standards.

Positioning

The OT strategy is aligned to addressing fast emerging customer challenges related to securing increasing cloud connectivity, ensuring secure remote access, enabling secure and converged IT/OT operations, and the effective management of threats and vulnerabilities. This is achieved through the OT Aware Security Fabric which includes Threat & Vulnerability Management vendors, Fabric-Ready OEM partners and System Integrators.

Fortinet's strength is its ability to provide security solutions across the entire Purdue Model from sensor to cloud. Industry partners and customers often cite Fortinet's solutions as easy to deploy, use and scale.

Fortinet's commitment to OT cybersecurity is evident in its continued product investments. The portfolio has grown significantly over the last 3 years and recent additions include new use-cases such as Secure Remote Access Management (FortiPAM) and asset and network visibility (FortiOS 7.2.0 OT View). Developments also include improved visualization and reporting and there have also been significant releases related to MITRE ATT&CK for ICS.

Future developments are likely to include FortiNDR's addition to the OT Aware Security Fabric, improvements to compliance management, and the inclusion of new capabilities from recent acquisitions (ShieldX (now FortiPolicy) and Volon (now FortiRecon). Beyond products and solutions, Fortinet's focus on being number 1 in OT Security has been accompanied by an expanded team of experts, experience centers, and training and awareness courses to improve customer value and experience.

Known for

Leading global Cybersecurity company

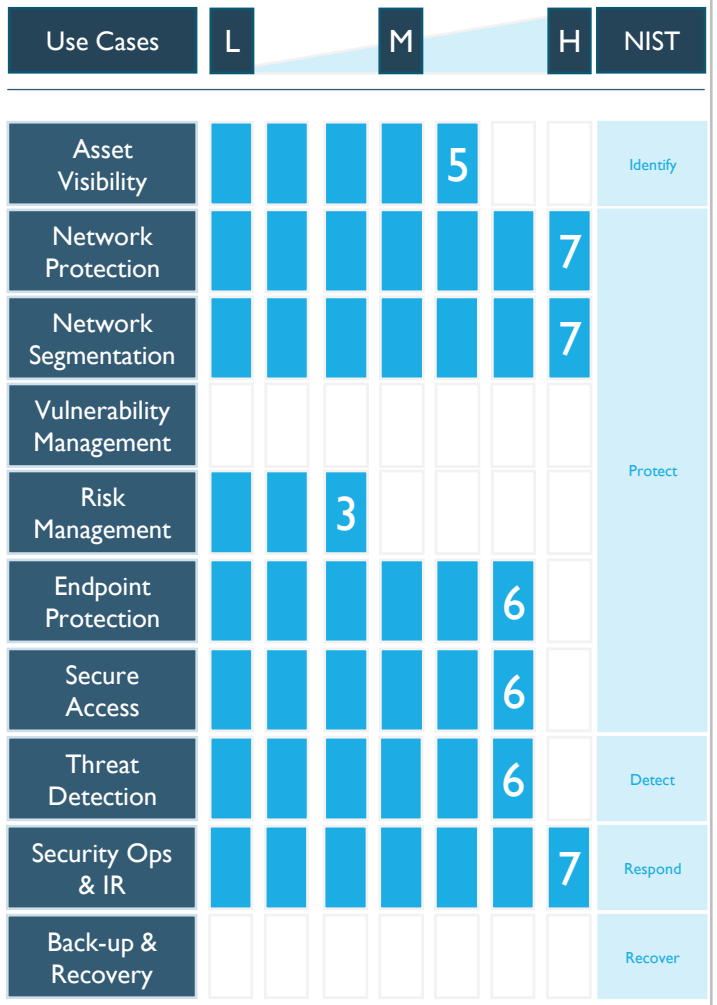
Wide and integrated set of security solutions

Innovation in cybersecurity and networking

Large Partner Ecosystem

Growing OT cybersecurity market presence

Native Technology Capability



Hexagon

Summary

Hexagon (Nasdaq Stockholm: HEXA B) is a diversified organisation providing a range of digital solutions to government, critical infrastructure operators and manufacturers. This includes geospatial, positioning, and asset lifecycle management solutions. Group sales grew by 8% to EUR 5,176M in 2022.

Hexagon's OT/ICS cybersecurity capability was gained through the acquisition of PAS Global, LLC in 2020. PAS technology is the foundation for the security and risk management capabilities in Hexagon's Asset Lifecycle Intelligence division portfolio which achieved sales of EUR 2,639M in 2022. The division has a strong footprint across regions (Asia 36%, EMIA 35% and Americas 29%) and various industry segments.

PAS was founded in 1993 in Houston, Texas. PAS has a strong brand and customer base in process industries, including O&G, Refining, Chemicals, Power and Mining. This includes over 620 customers covering ~1,400 sites in ~70 countries. PAS started out as an integrator and developed a strong capability mapping operational assets and developing plant documentation. Investment in products to capture the documentation and automate processes resulted in PAS Cyber Integrity® which addresses three key requirements of industries operators:

- OT/ICS Cybersecurity
- Risk Management
- Asset Reliability

Hexagon's key capabilities includes Asset Visibility, Vulnerability Management, Risk Management and Back-Up & Recovery. This includes use-cases such as compliance and configuration management, attack surface management and inventory management.

Positioning

Hexagon's key capabilities and differentiators are related to the company's deep knowledge of plant assets. This includes Asset Visibility and Management through PAS Cyber Integrity which focuses on both IT endpoints running in the industrial facility and production-centric endpoints (Purdue Level 0 and 1).

The latest product release, Cyber Integrity 7.3, includes a Risk Management module that prioritises risk and remediates vulnerabilities based on all the Common Vulnerabilities & Exposures (CVE's) connected to that asset. The proprietary risk scoring methodology is based on the criticality of the asset which is determined through Hexagon's deep inventory and system knowledge, providing operational context.

Hexagon solutions are often used alongside other Asset Visibility & Threat Detection vendors, providing supplementary information to enrich asset data and provide additional context. Cyber Integrity integrates with many of the platforms and can provide insight through its own GUI or in a third-party platform, including the main SIEM functions, CMDB's and Threat Detection vendors.

Hexagon's recovery and back-up solution is unique when compared to most asset visibility and threat detection vendors. This capability enables asset owners to restore operations quickly if there is a cyber or operations related incident or outage. Hexagon's solution also supports OT/ICS incident forensics and investigation. The company has partnerships with most of the major industrial OEM's, either integrating with platforms or providing ICS backup options.

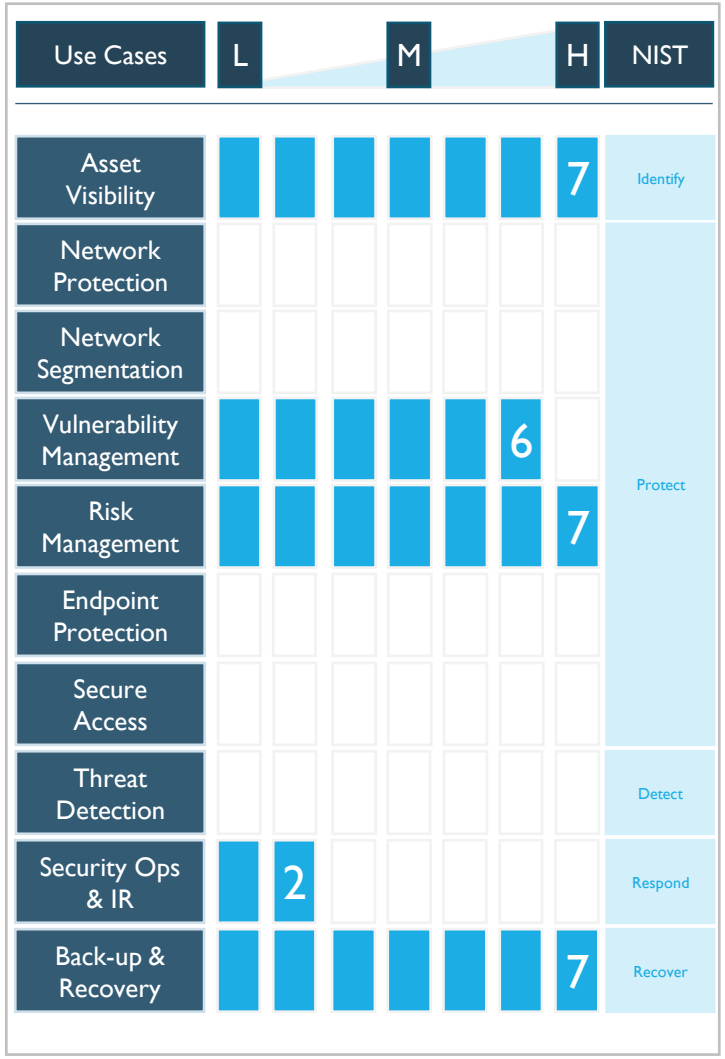
Known for

Strong partner in Process Industries

Mature Plant Asset Management Experience

Solutions to Improve Industrial Resilience

Native Technology Capability



Industrial Defender

Summary

Industrial Defender is a US based firm with a long-established record of delivering asset management solutions to critical industries. Founded in 2016, the company has been owned by Lockheed Martin, Leidos and Capgemini. The company has been privately owned since 2020 and currently employs ~40 staff in the US.

The company proposition is based on being the 'Single Source of Truth for OT', providing users with complete visibility of all connected and unconnected assets, depth of asset information, and historical context.

The Industrial Defender Platform addresses use cases related to asset management and risk rather than threat detection. The four platform capabilities include:

- OT Asset Management. Asset visibility and context
- Configuration Management. Enforcement of frameworks and policies
- Vulnerability Management. Prioritised vulnerabilities and patch management through FoxGuard Solutions
- Compliance Management. Auditing and reporting for all of the main standards and frameworks (IEC 62443, CIS, NERC CIP, NIST CSF, NIS Directive)

In addition to the platform Industrial Defender provides professional and managed services including commissioning and training.

Positioning

Industrial Defender is well positioned in process industries including oil & gas, energy and chemicals, counting 8 of the 10 largest power companies in the US as customers. The company reports that 99% of customers renew their service agreements.

The asset management solution is a blend of data collection methodologies, including manual ingestion of files, passive monitoring (e.g. network SPAN), direct database query, agentless techniques and agent-based discovery. Data is collected by the Industrial Defender Collector (IDC) and forwarded to the Central Manager (IDCM). Product innovation is a core focus of the new business direction. The platform continues to evolve and the latest release 7.5.0 includes asset risk scoring and prioritization. Future investment is likely to focus on hardware integrations, including sensing capabilities on the network switch and in a container, and improvements to the platform usability. Phoenix 1.0 is an important release in 2023 – an out of the box solution for small manufacturers and utilities requiring monitoring of up to 200 endpoints.

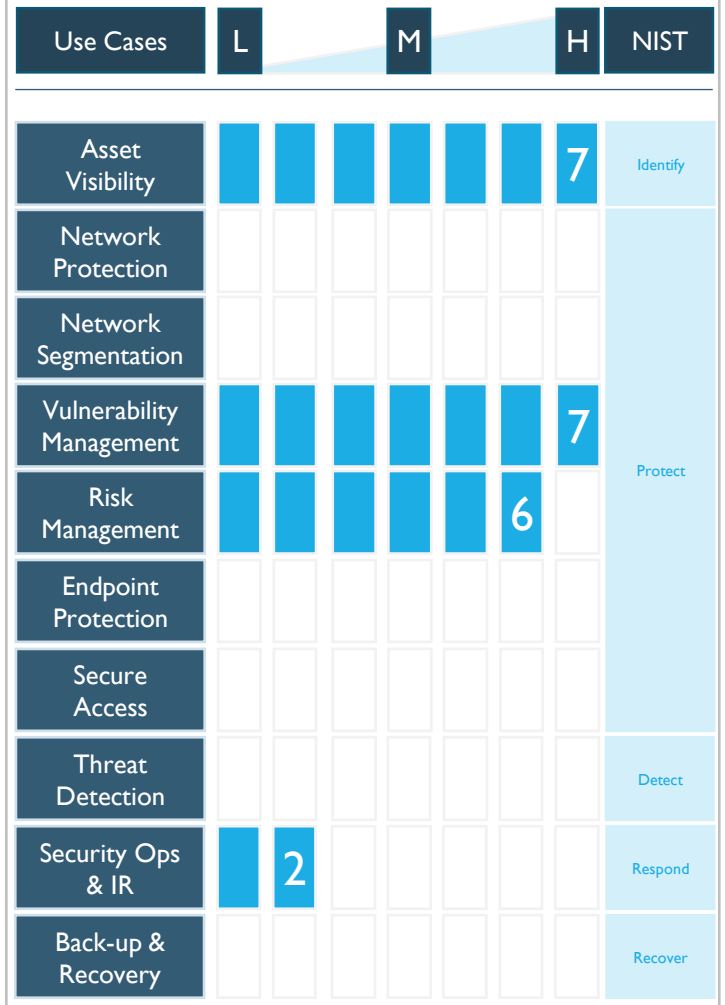
The company has a good partner network that includes strategic relationships, channel partnerships and integrations with important partners throughout the industrial ecosystem, The recent partnership with Nozomi Networks extends Industrial Defender's capabilities beyond network visibility, providing customers with threat detection through API-to-API integration. Integrations include Splunk and Servicenow whilst ABB and Schneider Electric are OEM partners.

Known for

Asset Management

Critical Industries including Energy, Oil & Gas and Chemicals

Native Technology Capability



Nozomi Networks

Summary

Nozomi is a leading OT cybersecurity company. Founded in 2013, the company is headquartered in the US and employs ~ 300 staff. The company has a strong European presence due to its Italian heritage and has large office presence in Italy and Switzerland.

The company is well respected globally, with a strong customer base that includes government customers. Nozomi is certified by several government agencies including ANSSI and is FIPS compliant.

The Nozomi Networks Platform provides engineering and SOC analysts with visibility of assets and networks, vulnerability and threat management tools, and response playbooks. Visibility is provided through both Passive Asset Discovery, or port mirroring, and Active Asset Monitoring. The Smart Polling add-on provides additional device context. The ML detection engine works with Nozomi's Threat Intelligence subscription, which includes current signatures and Indicators of Compromise, to detect anomalous activity. The response playbooks, dashboards, and further tools are designed to provide analysts with clear, actionable intelligence and remediation steps.

Vantage, the SaaS platform, and the Central Management Console, integrates with Nozomi's on-prem and virtualised products such as Guardian, and provides users with access to optional Threat Intelligence and Asset Intelligence subscriptions. Arc, Smart Polling and Vantage IQ completes the product portfolio.

Nozomi addresses a range of use cases including Asset Visibility, Vulnerability Management, Risk Management, Endpoint Protection and Threat Detection.

Positioning

Nozomi is an innovative organisation with a set of unique products such as Smart Polling. Recent product releases are aligned with emerging customer requirements and the market direction. This includes Arc, an endpoint agent that is complimentary to Guardian, providing additional endpoint visibility including user monitoring and malware detection. The sensor has been designed for OT networks and as such integrates with Nozomi's existing products, has low CPU usage and can work without connectivity. Additionally, the monitoring of USB drives, which are still widely used within OT, remains an important requirement in industrial sectors.

Nozomi's latest release is Vantage IQ, a Machine Learning based service that has been designed to reduce noise, prioritising and automating actions to simplify the end-user experience. Other recent updates include modifications to the UI and playbooks. This fits with the overall product roadmap of Nozomi which is based on providing customers with increased visibility and improved workflows across wired and wireless networks, including IoT devices.

Nozomi's strong market position has resulted from its reputation as an OT partner and the relationships it has developed with the ecosystem. This includes customers, industrial OEM's, resellers and MSSP's. Nozomi is one of the leading names in the industrial market segment and this is reflected in conversations with the channel, at industry forums and by the size of the company's following.

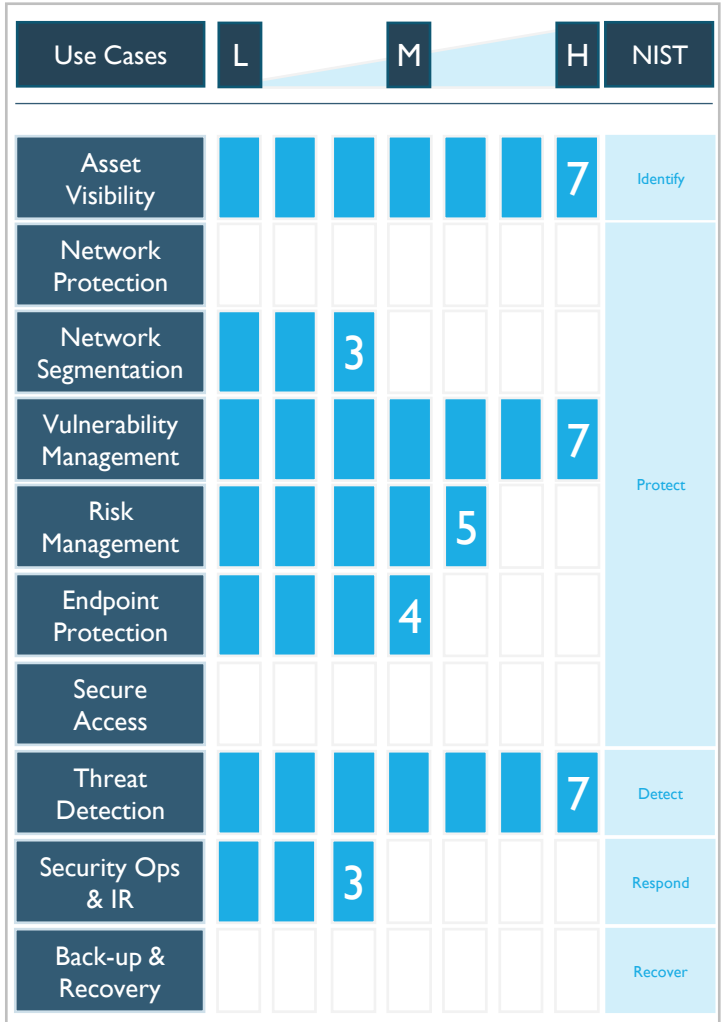
Known for

Large industrial customer base

Highly respected OT cybersecurity platform and user interface

Strong global network of partners and integrations

Native Technology Capability



OPSWAT

Summary

OPSWAT is a private company, founded in 2002. The company's growth is the result of investment in industry leading technologies (MetaDefender and MetaAccess) and strategic acquisitions to expand the product portfolio (Napera Networks, Red Earth Software, Impulse, Bayshore Networks, and SNDBOX).

OPSWAT received its first funding round in March 2021 - $125m from Brighton Park Capital which is being invested in go-to-market and ongoing product innovation.

Company revenue growth is tracking market demand. The company now employs ~650 staff and has over 1,500 active customers across critical infrastructure and manufacturing sectors. This includes a strong position in the energy sector. OPSWAT aims to increase the number of customers to over 2,200 by the end of 2023.

OPSWAT's approach, "Trust no file. Trust no device," is a proposition based on a Zero-Trust approach to security. The vision is to deliver end-to-end critical infrastructure protection, from Purdue Level 1 to 5, through a defence in depth approach. To deliver its goal of providing an integrated security solution, the company continues to focus a high percentage of sales on innovation. This resulted in new product releases in 2022 including Neuralyzer, an asset and network visibility product including vulnerability management and threat detection modules.

As a result of innovation and recent acquisitions, OPSWAT's extensive and integrated product portfolio addresses most OT cybersecurity use cases including Asset Visibility, Network Protection, Segmentation, Vulnerability Management, Risk Management, Endpoint Protection, Secure Access and Threat Detection.

Positioning

- OPSWAT's lead product is the MetaDefender platform, offering customers access to an integrated set of industry leading Advanced Threat Prevention technologies. This includes Threat Intelligence (IP & URL reputation), Content Disarm and Reconstruction (CDR) covering over 100 file types, Multiscanning using over 30 malware engines to ensure maximum prevention coverage, Data Loss Prevention covering over 40 file types, File-based Vulnerability Assessment and Malware Sandbox.
- Whilst OPSWAT has many OT security products, the company is mostly known for its Removable Media Security solution which remains the strongest performing product in the portfolio. The Netwall product line has also performed well, especially the diode which enables the safe transfer of data between the plant and cloud hosted services (e.g. historian).
- The roadmap includes investment in SOCaaS and Central Manager to provide a seamless user experience across the product range.
- OPSWAT's go to market includes OEM solutions, working with partners such as Palo Alto Networks and SonicWall through the OESIS framework (endpoint protection), direct and via an increasing number of channel partners.
- OPSWAT has a strong focus on customer services. This includes a leading training academy which has membership of ~5,000 customers and partners, sponsorship of CIP Cyber, and customer support centres providing 24/7 support.

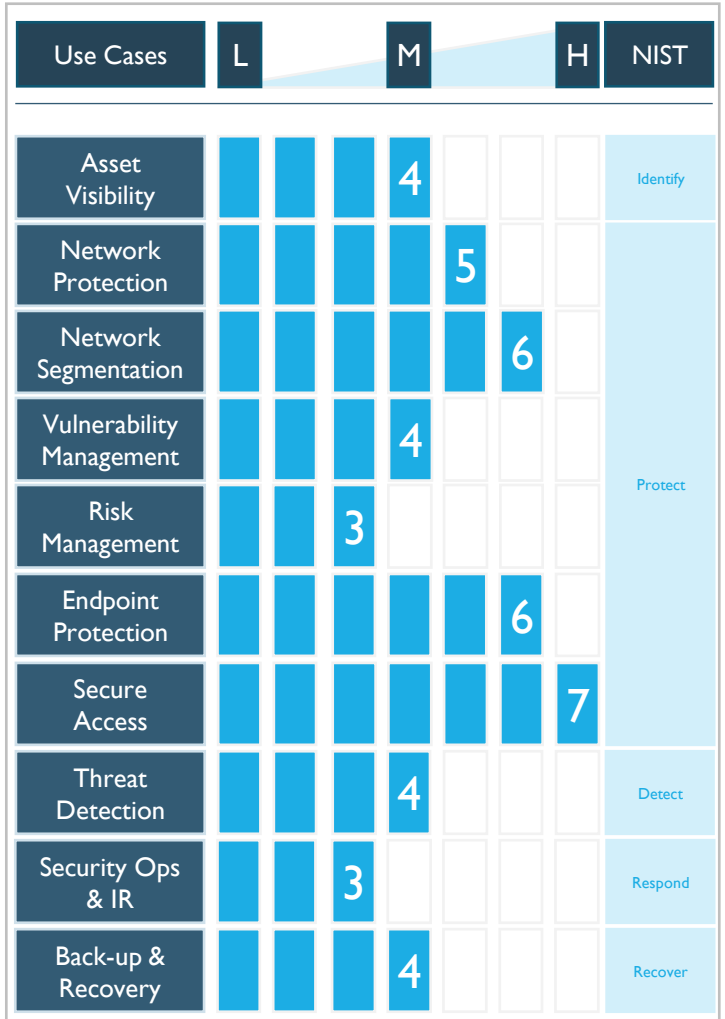
Known for

Innovation and product development

Critical infrastructure protection

Removable Media Security

Native Technology Capability



OTORIO

WESTLANDS ADVISORY

Summary

OTORIO was founded in Israel in 2017. The company currently employs ~100 staff who are located mainly in Israel and the US.

The company's mission is entirely focused on the protection of OT systems in critical infrastructure and manufacturing sectors. The customer base is global and includes energy intensive industries and advanced manufacturing sectors from automotive to pharmaceuticals.

The RAM^2 platform addresses the visibility and risk prioritisation challenge in OT environments, creating an asset inventory, identifying risks and automating response and mitigation plans. OTORIO also provides compliance and secure remote access solutions.

The 3 products are:

- RAM^2 – continuous OT/OT Cybersecurity Monitoring
- spOT – Supply Chain Cyber Risk Management
- remOT – Secure Remote Access

In addition to the platform OTORIO provides services that map to NIST CSF. This includes risk assessments, penetration testing, cyber threat hunting and incident response.

The main security use cases addressed by OTORIO includes asset visibility, vulnerability management, risk management and secure remote access. Integrations with SIEM platforms helps improve security operations and incident response.

Positioning

RAM^2 is a unique proposition in the market, collecting data from passive and active data sources, including firewalls, EDR, IDS, ICS among other sources, and then enriching with OTORIO's vulnerabilities database. The Central Manager provides engineers and security analysts with asset visibility and context and the 'Operational Risk Mitigation System' categorises risk and priorities action based on the severity level. The platform enables organisations to monitor and enforce compliance with industry standards and regulation, and to run attack simulations on a virtual replica of the network.

OTORIO offers two further products. spOT is an 'On Demand OT Cyber Risk Assessment' solution that provides onsite engineers and consultants with a quick and easy to implement asset discovery solution to assess asset and network compliance. Use cases includes meeting regulatory requirements and supports Factory Acceptance Tests, improving supply chain risk management. remOT is a Secure Remote Access solution that help asset owners transition to a Zero Trust Network strategy.

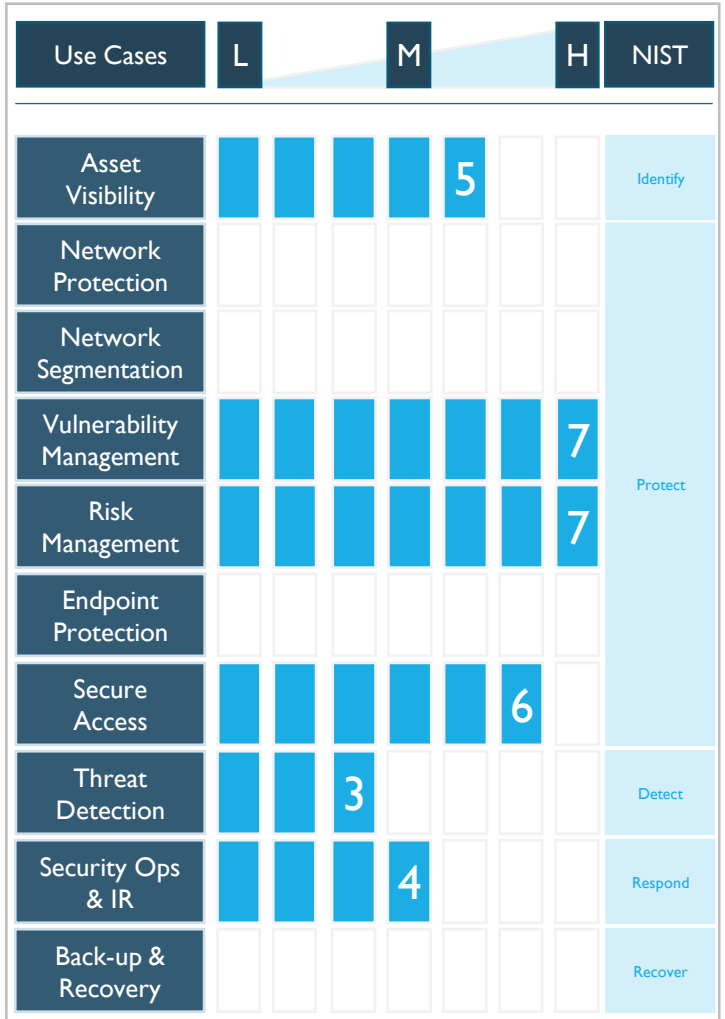
OTORIO offers a comprehensive range of services to improve the customer's product experience. Services range from onboarding to evaluation of risk profiles, and implementation of incident response plans. OTORIO's 'Onboarding Services' includes technical support and training whilst 'Advanced Professional Services' are designed to help customers improve and scale the use of the platform. 'Cybersecurity Consulting Services' includes Analyst Services to manage and monitor the customer platform, and incident response retainer services.

Known for

Risk and vulnerability management platform

Platform and services market offering

Native Technology Capability



Palo Alto Networks

Summary

Palo Alto Networks (Palo Alto) is a leading cybersecurity vendor with a wide range of products and services addressing network protection and the cloud. Guidance for revenue in FY2023 is $6.88B, 25% up on the previous year.

Palo Alto is comprised of 3 connected business areas.

- Network Security – hardware, software and cloud delivered solutions including NGFW, SD-WAN, ZTNA, SWG and subscriptions.
- Prisma Cloud – Cloud native platform protection including workload protection, CSPM and DevSecOps.
- Cortex – security operations including EDR, XDR, SOAR and Incident Response

Palo Alto has a significant footprint in the utilities and manufacturing sector with a large installed base of NGFW appliances at the OT perimeter and layers 2/3 of the purdue model. Despite the installed base Palo Alto's customer proposition has lagged behind that of its main competitors. This is being addressed through the 2023 launch of Zero Trust OT Security and Industrial OT Security.

Zero Trust OT and Industrial OT Security brings together existing products and new capabilities into a single market offer, expanding the coverage of Palo Alto Network's OT solution to most security use cases.

Native capability includes asset visibility, network protection and segmentation, endpoint protection, secure access, threat detection and security operations. The company also provides a range of services to help customers advance security programs. This includes Managed Detection & Response, Threat Hunting and Incident Response led by Unit 42.

Positioning

Palo Alto's OT proposition fits with the OT cybersecurity maturity model, starting with asset visibility, risk assessment, network hardening including segmentation, and implementation of least privilege principles for devices and remote access.

Visibility is delivered through in App-ID and Device-ID to passively detect and classify assets by ~80 attributes. Network segmentation (IT/OT) and zoning is enabled by Palo Alto Networks' enterprise and industrial NGFW's. Risk is monitored across the network including changes to device profiles and repeated access attempts. The Industrial OT Security service, supported by Palo Alto's threat intelligence, monitors ~650 OT specific threat signatures and ~350 unique OT profiles, providing continuous inspection of the network and identification of anomalies.

Palo Alto's OT Zero Trust Security leverages the visibility delivered through Industrial OT Security to enforce policies and access to OT assets, networks and users, including 5G networks. Continuous monitoring is managed through a single platform that can be deployed quickly and integrate with NACs, SIEMs and ITSM platforms.

Palo Alto has strong channel partnerships ensuring that most industrial SI's and OEM's are familiar with the platform, and integrations with OT vulnerability management and threat detection vendors.

Known for

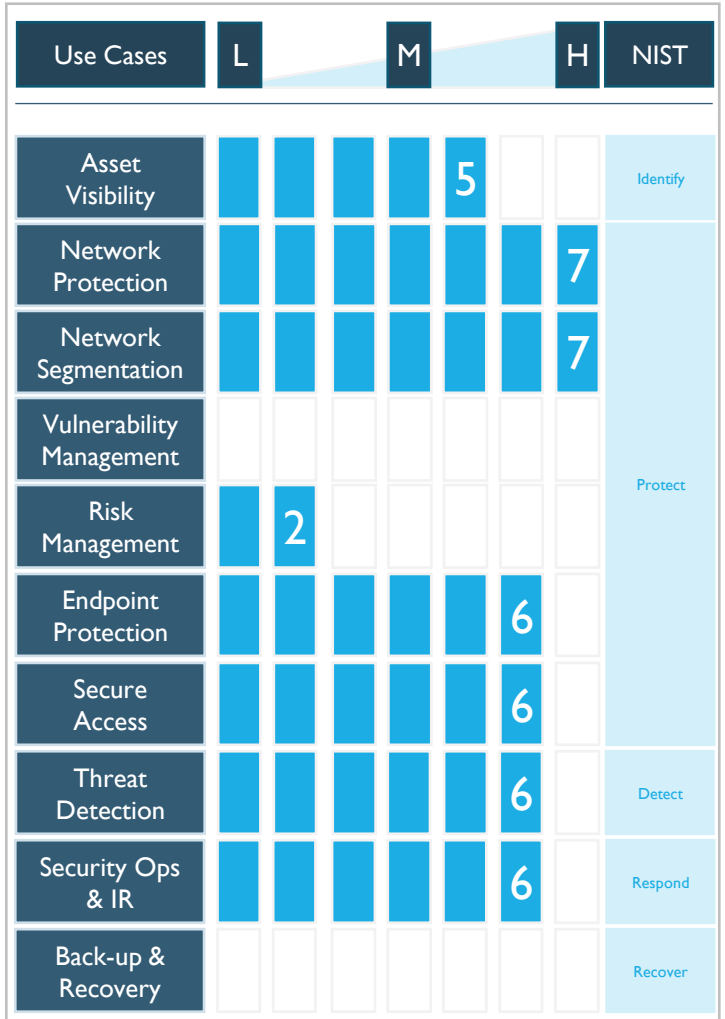
Leading global cybersecurity company

Trusted brand

Strong channel and partner relationships

Large installed base of IT solutions with industrial customers

Native Technology Capability



Tenable

Summary

Tenable is a leading vulnerability risk management and threat detection company providing protection across IT and OT systems. Organisational sales reached $683M in 2022. The customer base is diverse, totalling ~43,000 customers across a range of industries, including ~40% of the Global 2000. 63% of revenue is in the Americas, 26% in EMEA and 11% in APAC.

The company positions itself as the Cyber Exposure company - a platform vendor unifying data and managing risk across IT and OT networks, applications, cloud and identities. Tenable One, the company's exposure management platform, addresses several critical cybersecurity use cases, including asset inventory, attack pathway analysis and risk analytics.

Company strengths include the quality of its vulnerability coverage (number of CVE's) and research (high number of zero-day vulnerabilities discovered).

The OT cybersecurity solution is called Tenable OT Security and resulted from the acquisition of Indegy in 2019 to expand coverage for industrial and critical infrastructure customers. The solution addresses Asset Visibility, Vulnerability and Risk Management, and Threat Detection use cases.

The acquisition of Alsid in 2021 further broadened Tenable's portfolio and creates new use-cases for industrial customers. For example, the expanding platform includes management of remote users accessing industrial systems, combining Nessus (CVE), Identity Exposure (authorised access for remote user group) and Tenable OT (highlights pathways to compromise the operational network).

Positioning

Tenable's Exposure Management platform proposition is to provide users with visibility across all of its assets from a single, integrated and scalable platform. This provides customers with the ability to use a single vendor – the customer journey tends to start with expanding from on-prem solutions to additional services including Tenable Identity Exposure and Tenable OT Security. Tenable's proposition fits well with the IT/OT convergence trend that is leading to CISO's being more central to decision making related to OT cybersecurity.

The company is continuing to invest in Tenable One and this has resulted in better integration of the products and expansion of its coverage of attack pathways. The acquisition of Cymptom in February 2022 was a part of the strategy to provide increased visibility of vulnerabilities across the enterprise and visualise the threat by mapping to the MITRE ATT&CK framework. The analytics from Cymptom have since been built into Tenable One.

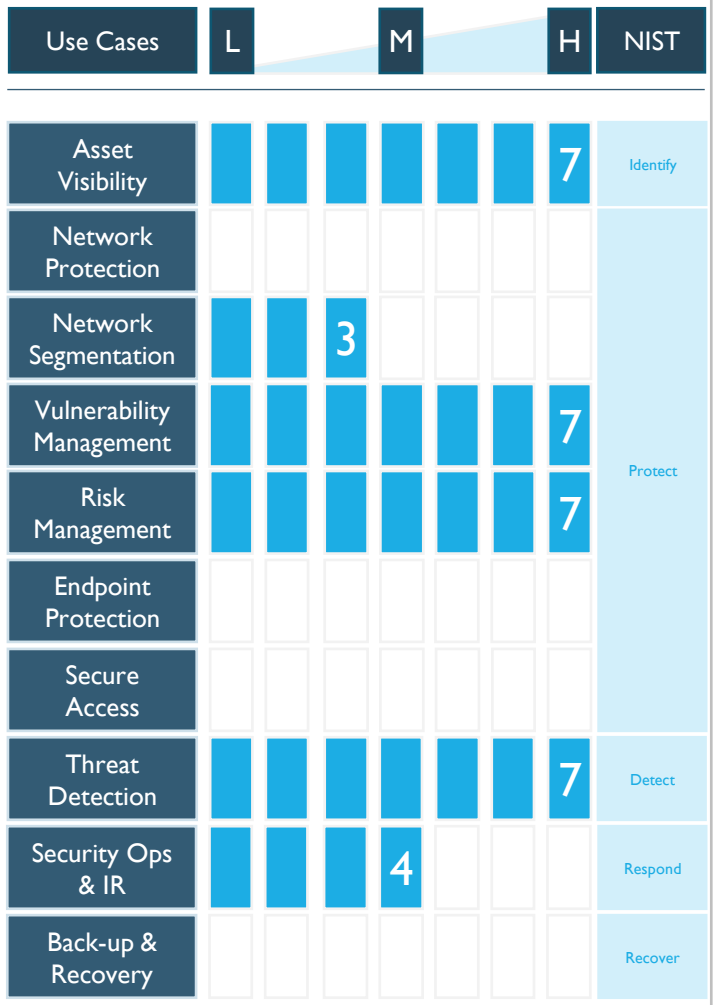
Tenable has a strong network of reseller and MSSP partners in the US reflecting its strong US market position. However, the company does not have strong industrial OEM relationships and Tenable OT does not have the same brand strength in the channel and amongst the OT community as some of its peers.

Known for

Integrated and scalable risk management solution

Coverage of CVE's and Threat Research

Native Technology Capability



TXOne

Summary

TXOne Networks is a Series B funded OT cybersecurity organisation that was spun out of Trend Micro.

Financial performance was strong in 2022 with high demand across all product lines. The company now employs over 300 staff, mainly in Asia, and plans to expand teams further in Europe and North America.

TXOne has a strong product roadmap with a number of significant releases planned over the next 12 months. The most recent release is the new primary capability, Cyber-Physical System Detection & Response. CPSDR provides engineering and security teams with increased visibility of cybersecurity and operational threats. The security component is based on centralised behavioural analytics and threat-based correlation, whilst operational risk is managed by agent-based behavioural analysis and device "fingerprinting" to detect changes to operational baselines.

The TxOne product portfolio includes three distinct offerings for network protection.

- Security Inspection which is a set of portable products for malware scanning.
- Endpoint Protection through Stellar, an on-prem, agent based solution managed through a centralised management console. Use cases include AV, asset visibility, industrial application control and patch management.
- Network Defense which includes EdgeIPS and EdgeFire OT security appliances. Use cases include network visibility, segmentation and virtual patching. EdgeFire 2.0, released in May 2023, includes VPN support and increased protocol analysis and control.

Positioning

TXOne's vision is to provide asset operators with a unified view of the OT network, providing context and increasing levels of orchestration to both security and operational teams. Currently EdgeOne is the industrial central management console for monitoring OT networks and provides an insight into the future direction of the company. The product integrates with Trend Micro Vision One (XDR) to provide both IT and OT network visibility for industrial manufacturers looking to consolidate security infrastructure and centralise visibility across its operations. EdgeOne integrates TXOne's Threat Intelligence, improving administration and OT protocol management, and provides a visual of the IT/OT network map.

The company's solutions are supported by a strong Threat Intelligence service. Insight is created through combining TXOne's intelligence with endpoint, network and 3rd party sources and is shared with the wider OT research community. The company has discovered over 30 ICS related CVE's.

TXOne's channels to market include OEM relationships, Trend Micro, and OT partners. Co-innovation and OEM integration is central to the company strategy and the company will continue to focus on building its alliance network.

The company has deep OT expertise including strong vertical market expertise in semiconductor and automotive manufacturing sectors and with critical infrastructure providers (energy, Oil & Gas)

Known for

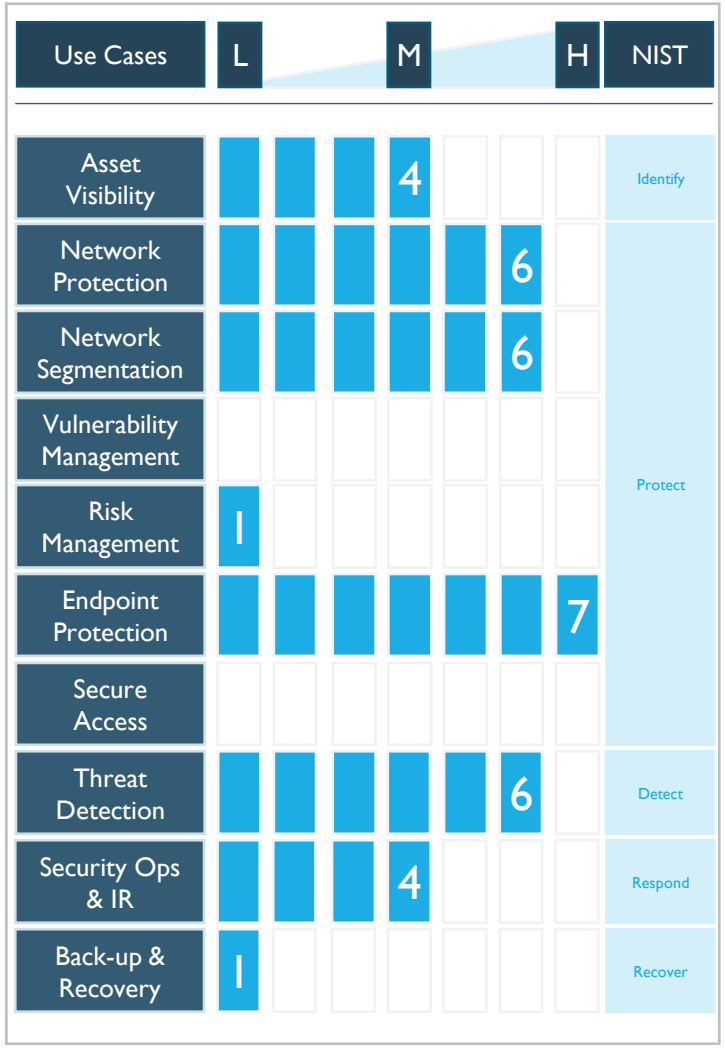
Strong customer base in APAC, particularly Japan

Trend Micro Partnership

OEM innovations and collaborations

OT sector expertise with notable strength in semiconductor and automotive

Native Technology Capability



Verve Industrial Protection

Summary

Verve Industrial Protection (Verve) is an OT security solutions provider headquartered in Chicago, Illinois. The company was founded in 1994 and currently employs ~120 staff based primarily in North America, reflecting its US customer base.

The company started out as an OT consulting company and gradually introduced software tools to help its customers gain better visibility into OT operations. This eventually led to the Verve Security Center, an OT endpoint management platform. The engineering expertise has been retained in the firm - the company has a relatively high percentage of engineers and technical staff compared to industry peers.

The platform and services offered by Verve align to the principles of ITSM in an OT environment. OTSM (Operational Technology Systems Management) includes asset discovery and classification, asset lifecycle management, systems management and configuration, security management, change management, incident response and back-up. This is supported by Verve's platform focus on OT attack surface management which includes enumeration, risk assessment, prioritisation, remediation and continuous monitoring.

The Verve Security Center addresses a range of use cases, including asset visibility, risk and vulnerability management, security operations and incident response, and back-up and recovery.

Services include risk assessment, security strategy, network design and segmentation, system hardening, and managed security services.

Positioning

The company is uniquely positioned as a platform and managed security service provider, offering customers an end-to-end solution. Verve provide much of the upfront consulting and integration capability which includes risk assessments, policies and procedures and technical implementation of firewalls and other controls. The Verve Security Center can be either managed by the asset owner, a third party or more typically by Verve analysts. Verve also provides automation engineering support including design and implementation of industrial networks. The company is most competitive in large, distributed environments that are using a mix of industrial control systems from different vendors. The platform provides visibility across sites and processes, identifying vulnerabilities and limiting the need to do costly, physical inspections, as well as integrating remediation actions within the same platform.

Verve's platform provides visibility through endpoint detection and management rather than passive monitoring of networks. The agent-based asset management solution does not require implementation of hardware appliances, enabling quick deployment outside of maintenance windows. This covers most vulnerabilities which are windows based. In Verve's opinion this is sufficient for effective OT cybersecurity posture management, covering ~99% of known vulnerabilities.

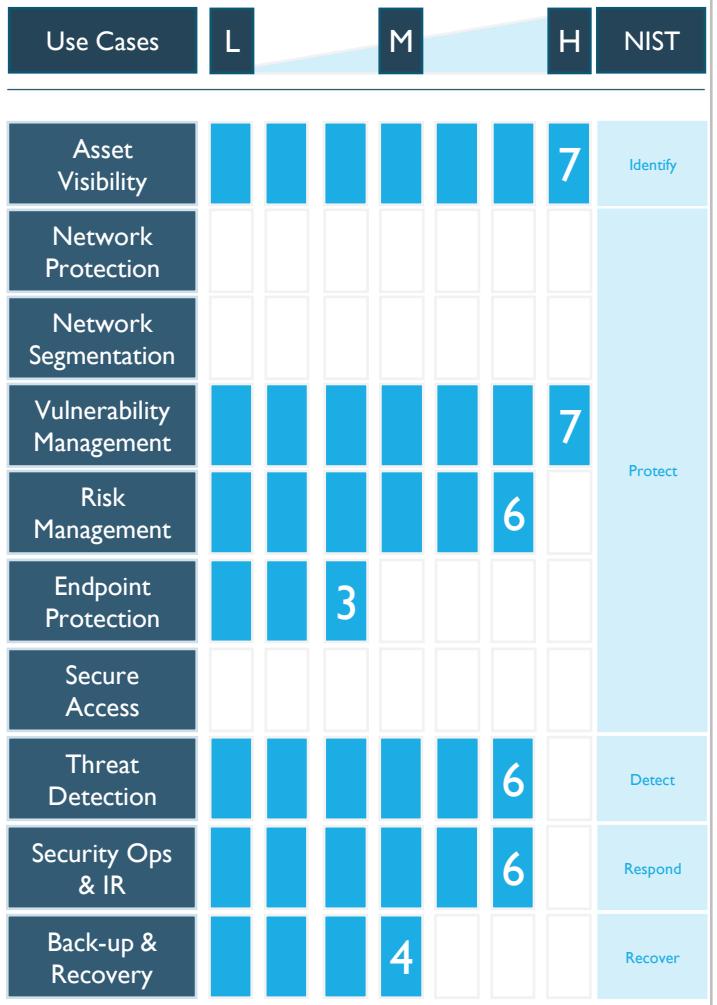
Verve's roadmap is likely to stay close to its focus on improving security efficiency – using less time and resource to maintain a high level of security. This will include providing increased context, accurate alerting and automated response, enabled by collection and correlation from an increasing number of data sources.

Known for

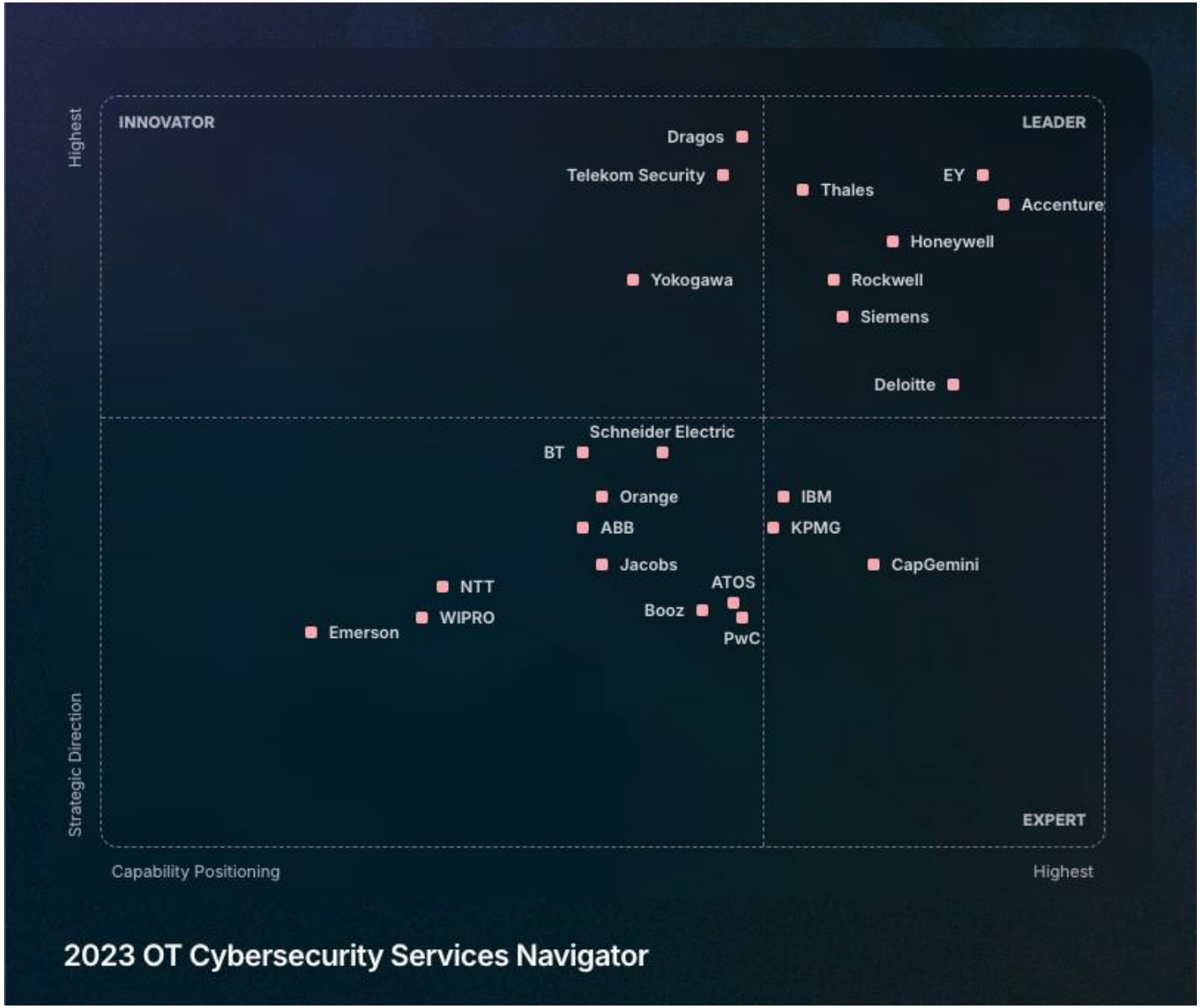
OT Attack Surface Management

End-to-end OT Service

Native Technology Capability



Industrial Cybersecurity Services and Managed Services



Qualification Criteria

- Service providers must meet the following criteria to qualify for consideration in the IT/OT Cybersecurity Service Navigator.
- Operational Technology expertise including people, OT specific SOC's and capability centres that includes cyber ranges.
- A wide range of services to support customers deliver against IEC 62443, NIST CSF and other relevant regulation or standards. This includes the ability to advise, integrate, monitor, and respond to incidents.
- Global capability with strong representation in more than two regions globally (NA, LATAM, Europe, Middle East & Africa, Asia)
- Strong set of customer references

Groupings for Vendor Profiles

WESTLANDS ADVISORY

Risk Assessment	Identifies and evaluates risks and vulnerability specific to OT. Tasks include asset inventory and classification, threat identification, vulnerability assessment, risk prioritisation
Cyber Strategy	Provides a comprehensive approach to managing cybersecurity across an organisation. Disciplines include governance and leadership structure, security policies and procedures, regulatory compliance, supply chain management and incident response
Security Architecture & Implementation	Design and implementation of security measures and controls to protect systems and data including testing of vendor products
Secure-by-Design	Advisory services related to integrating security measures into the design and development of industrial products and platforms
Awareness & Training	Services related to improving employee awareness about cybersecurity best practice and training of security staff
Threat Simulation	Simulation of cyberattacks to test and improve an organisation's security defences through identifying vulnerabilities and weaknesses
Threat Intelligence	Collection and analysis of OT threat intelligence providing insights into tactics, techniques and procedures
Managed Security Service	Management and monitoring of network and security controls
Managed Threat Detection	Monitoring and detection of potential threats
Incident Response	Manages and co-ordinates actions to contain, investigate and recover from security breaches

Leader > Accenture

Summary

Accenture has been recognized as a leader in industrial cybersecurity consulting and managed services for the second consecutive year. With robust capabilities and deep industry expertise, the company offers customers a comprehensive range of end-to-end security services.

As a global security services provider, Accenture generated revenues exceeding $6 billion in 2022. The company's security business encompasses four main sectors: Cyber Strategy, Cyber Protection, Cyber Resilience, and the cross-functional Cyber Industry business, which delivers industry-specific solutions. Accenture's security team has a strong presence across the Americas, Europe, the Middle East, India, Southeast Asia, Japan, and Australia.

Accenture is also a well-regarded thought leader in operational technology (OT) security, earning high-profile government engagements and a customer reference list that includes leading asset owners in the Oil & Gas, Energy, Chemicals, and Manufacturing industries. In 2023, the company led workshops with group members of the U.S. government's JCDC ICS program. Accenture's OT-specific industry event, Operation:Next, provides a platform for customers to share best practices in implementation.

Accenture's go-to-market strategy is vertically oriented, leveraging company-wide functional skills and industry expertise to address customer challenges. The OT cybersecurity team often collaborates with colleagues from across the wider customer business, tapping into the expertise of more than 5,000 engineers and 16,000 cybersecurity professionals.

Positioning

- Accenture offers a comprehensive OT cybersecurity service, categorised under three main pillars: Define, Deploy, and Sustain. These services are supported by skilled professionals, industry-specific architectural designs, deployment playbooks, and infrastructure that facilitates education, training, and security services management.
- Accenture's global reach is backed by local support and a network of 22 Security Operations Centers (SOCs) – three of which are dedicated to OT – 12 delivery centers, 10 Cyber Fusion Centers, 5 cyber ranges, and 1 cyber lab that provides specialised services to customers. Fusion centers aid customers in understanding their unique challenges, testing concepts, and accelerating deployments. The OT Cyber Fusion Center in Houston, for instance, has played a significant role in training both Accenture employees and customers, and has been pivotal in co-creating cyber solutions.
- Innovation and co-creation are central to Accenture's business and customer strategy. The company has developed over 200 unique "tools and enablers" through close collaboration with its customers, including cloud architectures, firewall configuration templates, assisted reality, and OT incident response solutions.
- Accenture's robust delivery performance is further bolstered by its technology alliances with security technology vendors such as Forescout, Armis, Nozomi, Fortinet, and Splunk, as well as ITSM vendors like ServiceNow and industrial OEMs including ABB and Rockwell Automation.

Known for

World-leading security capabilities

One of the largest cybersecurity professional services companies in the World

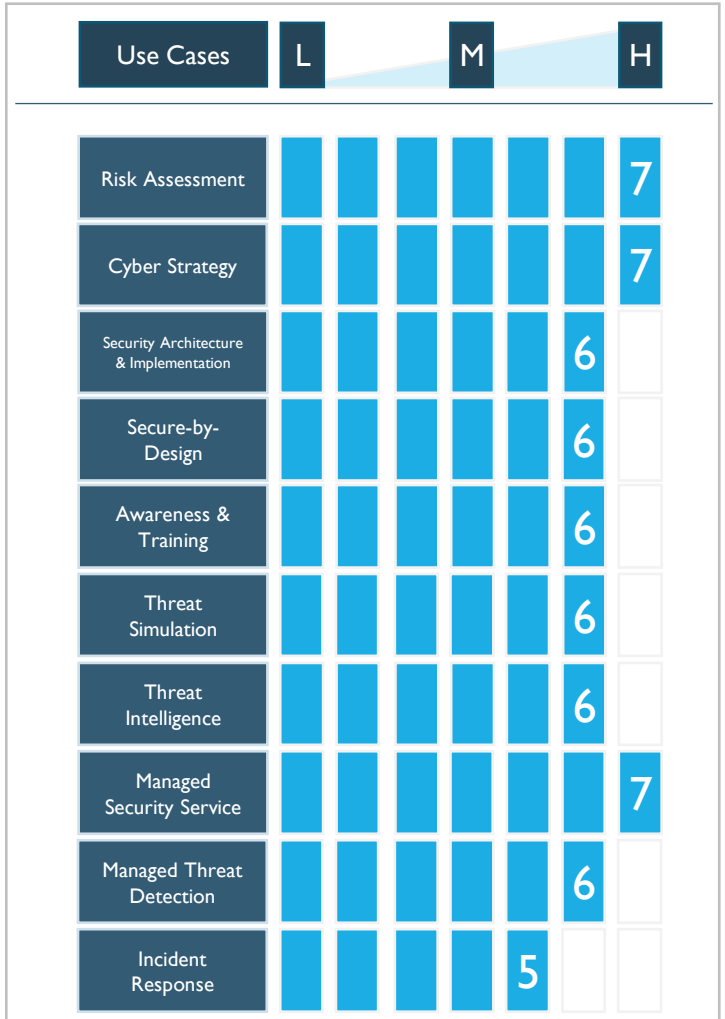
Strong OT alliance ecosystem and strategic partnerships with OT vendors

Significant investments in future technology

Cross-industry and geographical cybersecurity expertise

OT Cyber Fusion Centers

Service Capability



Leader > Deloitte

Summary

Deloitte's company revenue increased to $59.3bn in 2022, up from $50.2bn (2021) and $47.6B (2020). The company has a diverse customer base with a high percentage of business coming from Energy, Resources & Industrials ($8.6B). The company has a particularly strong business in the America's which represents over 50% of corporate revenues.

The cybersecurity capability sits primarily within the Risk Advisory practice with combined revenues of $7bn in 2022 and strong growth on the previous year. Deloitte employs ~22,000 cybersecurity and risk professionals worldwide.

The Cyber business includes a full range of services to address risk and security transformation challenges in the modern enterprise. This includes Application Security, Cyber Cloud, Cyber Strategy, Data & Privacy, Detect & Respond, Emerging Technologies, Identity, Infrastructure Security and Recover & Transform.

OT Cybersecurity is part of Cyber Physical Security (CPS) services, alongside IoT security and Product Security. The business is supported by ~400 global experts with qualifications and practical experience related to OT and IoT cybersecurity. This includes active roles in standards development.

OT cybersecurity is a mature service at Deloitte. The organisations has a strong track record of delivering services to manufacturing organisations over the last 20 years. This includes a large base of monitored sites.

Positioning

- Deloitte offers a comprehensive OT cybersecurity service: Assess, Design, Implement, Monitor and Lifecycle Management. The company has developed a range of specialised tools and methodologies for OT environments. The CyberPHA risk assessment framework is used to identify hidden risks and to develop a remediation roadmap that recognises the interdependencies of process safety, industrial automation and cybersecurity. TIBER (Threat Intelligence Based Ethical Red-teaming) is a further service developed for OT.
- MXDR by Deloitte is the fully managed cybersecurity service providing 24x7x365 hunting, detection and response for manufacturing organisations. The SaaS model allows customers to add and expand services across both IT and OT environments. The service is supported by over 3,000 staff and includes ~200 cyber threat intelligence analysts. The service also includes industry and geographic specific use cases and automated playbooks, providing customers with highly relevant solutions.
- The company has a strong partnership ecosystem including most industrial security technology vendors including Palo Alto Networks, Claroty, Dragos, Cisco and BeyondTrust
- The company is recognised as a strong product engineering company and this continues to strengthen through recent acquisitions of Optimal Design and Dextra Technologies, providing Deloitte with deeper knowledge of product design and engineering challenges and additional expertise.

Known for

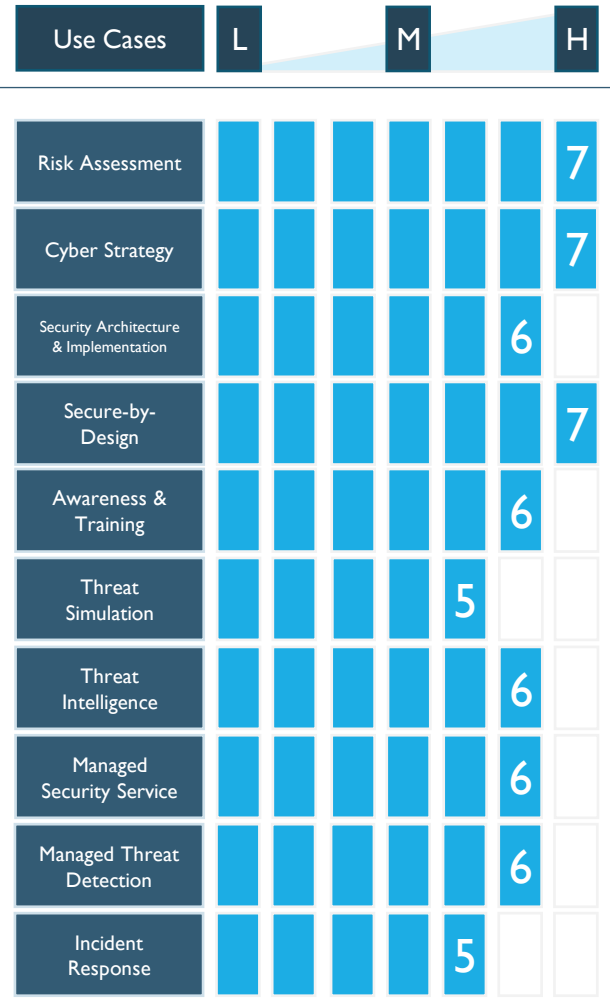
Global network of security operations

Product design and engineering expertise

Security innovation

Mature OT cybersecurity practice

Service Capability



Leader > EY

Summary

EY has been recognized as an industry leader in OT cybersecurity consulting and managed services for the second consecutive year.

The EY cybersecurity practice team is comprised of more than 13,700 risk professionals, augmented by an extended team with expertise spanning regulatory, engineering, change management, and legal fields, and it is present in over 150 markets worldwide. The team expanded by over 40% in 2022 to accommodate the growing demand for EY's cyber operations and OT cybersecurity services, which are among the company's fastest-growing sectors. EY's success in OT can be attributed to the firm's commitment to localising services, extensive and varied functional expertise, and sustained innovation in its cyber platform and services. These efforts have led to impressive customer retention, successful new customer acquisition, and substantial productivity gains for its clients.

The OT security practice at EY traces its roots back to 2007 and was followed by the establishment of competency centres in Warsaw, Poland (2008), Houston, US (2010), Singapore (2013), and Oman (2019). EY's experience and expertise encompass the delivery of more than 500 OT-related projects and a team of approximately 720 dedicated OT security staff, the majority of whom have backgrounds in industrial engineering. EY has a strong presence in industries such as Oil and Gas, Utilities, Chemicals, Manufacturing, Transport, Mining & Metals, and Pharmaceuticals.

EY's cyber ecosystem partner network continues to grow and now features Nozomi Networks as a recent addition. The company frequently receives accolades from its partners, including recognition from Microsoft (Global Security Partner of the Year, 2022) and CrowdStrike (Global SI Partner of the Year, 2022).

Positioning

EY has a strong reputation within government and critical infrastructure sectors, including advisory roles and contributions to regulations and standards. The company fosters a culture of innovation in OT cybersecurity, exemplified by a solutions design studio dedicated to enhancing the delivery of OT service management design and operation, OT cloud services, and the implementation of Zero Trust principles. As a full security lifecycle service provider, EY possesses robust capabilities in risk assessment, architecture design and implementation, and security operation management. This includes extending IT SOCs to IT/OT or exclusively OT SOCs. Innovative applications developed by EY include tools for risk assessment (EY Assess), testing, training and sandboxing (ASC), threat intelligence (CTI), and cyber metrics and operations (CRD and SMP).

EY continues to evolve its global cybersecurity service and has outlined a long-term investment plan focused on people development, infrastructure enhancement, and service innovation. EY's customers are currently supported by a network of local offices adhering to a hub-and-spoke model. This network comprises 73 cybersecurity operations centres, IoT/OT security-specific centres of excellence, and five global SOCs equipped with OT monitoring capabilities. EY's OT labs concept and flagship facility in Poland utilises over 350 ICS environments covering all sectors and the leading IoT/OT security solutions, enabling asset owners to develop Proof of Concepts as well as testing and deploying next-generation security services.

Known for

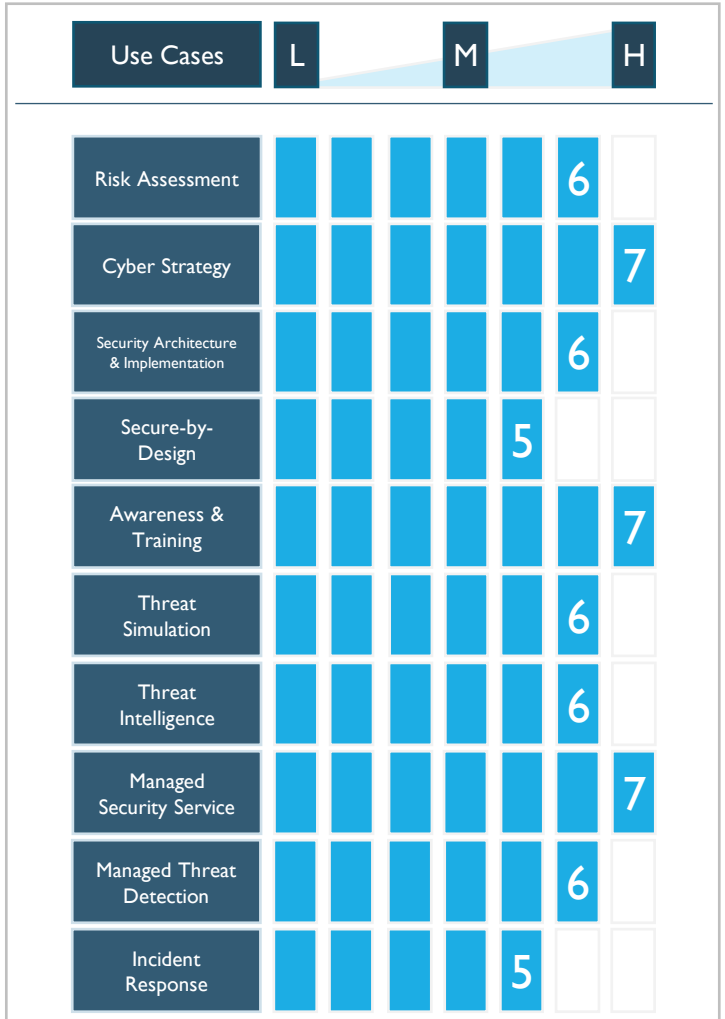
Security service innovation

World leading OT Lab in Warsaw, Poland

Complex program management

OEM agnostic with deep technical expertise in OT systems

Service Capability



Leader > Honeywell

Summary

Honeywell (HON) is an OT Cybersecurity Services industry leader with a mature portfolio of OT cybersecurity software and services.

HON is a diversified industrial firm with revenue of $35B (2022), 110,000 employees and operations at ~970 sites across four business areas.

- Aerospace
- Honeywell Building Technologies
- Performance Materials and Technologies
- Safety and Productivity Solutions

Honeywell Connected Enterprise was established in 2018 to accelerate software development and IIoT solutions across the four businesses divisions. This includes cybersecurity services that are integrated into the Honeywell Forge platform with capability covering NIST's Identify, Protect, Detect, Respond and Recover.

- Forge Cybersecurity Suite includes Asset Discovery (active and passive), Secure Remote Access and Monitoring of controls, risk monitoring, log forwarding, and threat analysis.
- Advanced Monitoring & Incident Response (AMIR) includes log aggregation, threat analytics and response workflows, and incident response
- Secure Media Exchange (SMX) removable media device control.
- Professional Security Services including risk assessments, penetration testing, design and build.
- Managed Security Services including threat detection and incident response

Positioning

- Honeywell has a distinctive market offering that includes software solutions, primarily the Forge Cybersecurity Software Suite, as well as a full spectrum of security lifecycle services encompassing assessment, design, build, and operation. The company has invested significantly in its products and services to achieve its current standing, highlighted by the acquisitions of Nextnine in 2017 and SCADAfence in 2023.
- Honeywell's vendor-agnostic approach to the market has contributed to strong performance with both traditional Honeywell customers and a newer clientele. This success is underpinned by Honeywell's robust partnerships with cybersecurity vendors. The company's global solution, which currently manages security for over 600 sites, is supported by local staff and infrastructure in key markets. This includes two managed security centers in Houston and Bucharest, five Cybersecurity Development Centers across the US, Europe, Middle East, and Asia, and three Cybersecurity Centers of Excellence in Atlanta, Dubai, and Singapore. These centers play a pivotal role in enhancing customer relationships by offering solution demonstrations, training Honeywell and customer staff, testing solutions, and conducting live simulations.
- Honeywell's innovative culture is sustained by initiatives like Cyber Customer Advisory Boards, customer innovation at Cyber Centers of Excellence, leadership roles in various user groups, and the application and monitoring of Honeywell's software and services at its own facilities

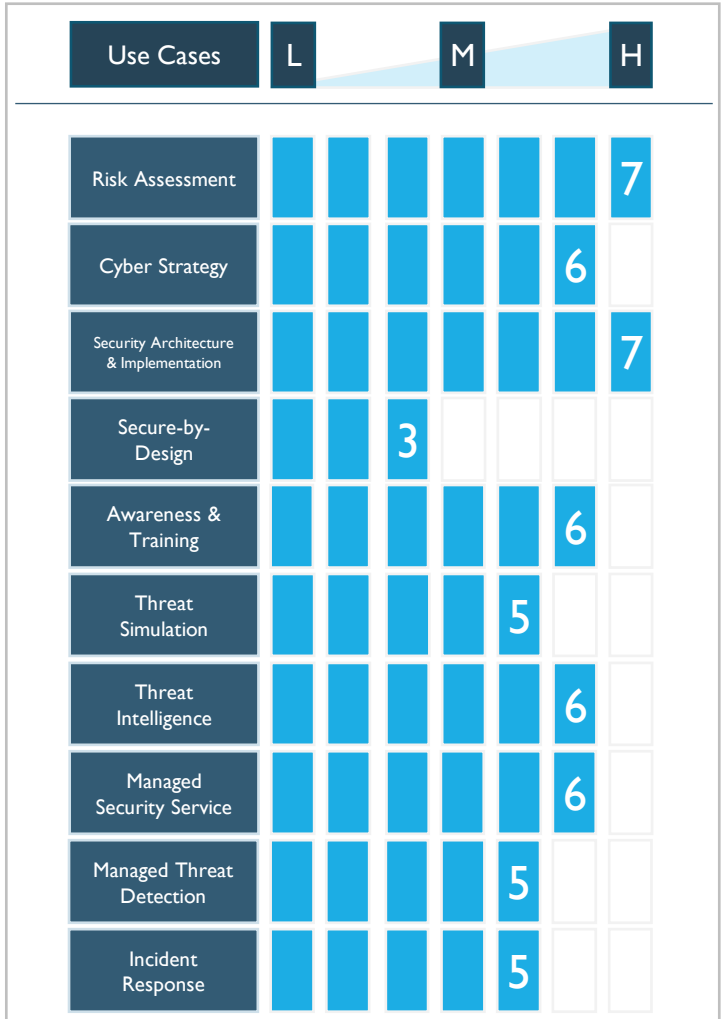
Known for

Full Cybersecurity Lifecycle Management

Honeywell Forge Cybersecurity Suite

Critical Infrastructure Protection

Service Capability



Leader > Rockwell Automation

Summary

Rockwell Automation (Rockwell) is a leading industrial automation vendor and service provider with revenues of $7.8bn in FY2022 and is a leading provider of OT cybersecurity services.

The company has a strong North American presence, contributing 61% of global revenues. The organisation is aiming to grow sales to $9bn by FY2025 through expanding presence in Europe and Asia, and by maintaining double digit growth in cybersecurity services.

The business was reorganised in 2020 from Architecture & Software and Control Products & Solutions to:

- Intelligence Devices ($3.6B)
- Software & Control ($2.3B)
- Lifecycle Services ($1.9B)

Security Infrastructure is included in Software & Control. Professional and Managed Security Services form part of Lifecycle Services and includes the acquisitions of Oylo and Avnet Data Security.

The Lifecycle proposition is based on Design, Innovate, Operate, Maintain, and a focus on helping customers to improve operational performance safely and securely.

Rockwell's global coverage includes 5,800 service professionals across over 80 countries and supported by 16 remote support centres.

Positioning

- Rockwell Automation has expanded its cybersecurity capability through acquisitions, partnerships and internal investment. The company offers customers hardware (industrial firewalls and switches) and a range of services. The acquisition of both Oylo and Avnet in 2020 provided Rockwell Automation with additional European presence and a cybersecurity services capability including risk assessments, integration, and managed security services and incident response. The acquisition of Kalypso in 2020 is also notable, providing Rockwell Automation with the skills and additional capacity to help guide customers through digital transformation of manufacturing operations.

- The cybersecurity services proposition is built on its Assess, Design, Implement, Monitor framework and a cybersecurity program that is Risk Informed, Repeatable and Adaptive. Rockwell provides good coverage of the NIST CSF model and core services include asset inventory, risk management, threat detection services and incident response.

- Managed Security Services includes management of the network, security appliances, applications, endpoints and secure remote access. The services are supported by partnerships with leading vendors including a long- established relationship with Cisco, a strategic investment in Claroty, and Crowdstrike and Dragos. In December 2022 Fortinet was added as a partner.

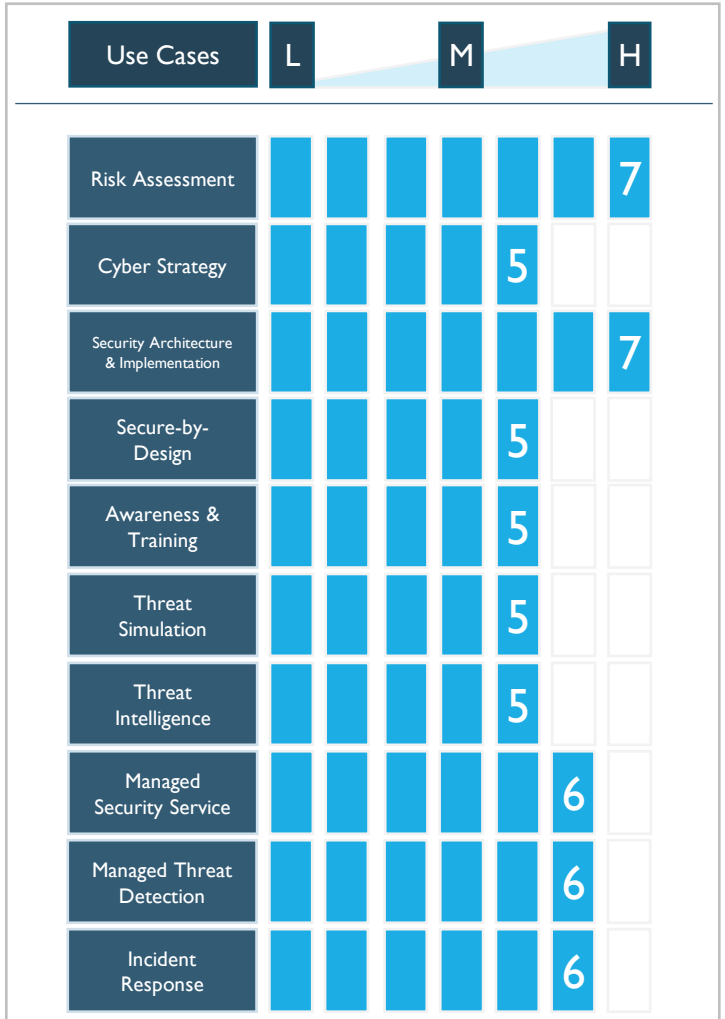
Known for

Maturing cybersecurity platform and services

FactoryTalk platform facilitating factory automation and transformation

Stratix range of switches, remote access routers and firewalls

Service Capability



Leader > Siemens

Summary

Siemens is a global technology company, providing hardware, software, solutions and services across four core industry sectors: manufacturing, healthcare, building & infrastructure, and mobility. In manufacturing, Siemens are a leading provider of OT security services, including professional and managed security services for protecting systems, networks and assets.

The company has strong relationships with leading industrial OEM's and end-users across a wide variety of industries including automotive, food & beverage, power and energy and chemicals.

Siemens' cybersecurity services have evolved from re-using and scaling solutions through shared investment and collaboration, as well as by protecting its own network of ~190 factories. This ongoing internal process led to the creation of a global governance and risk model that can be tailored at the local level to account for diverse needs and varying levels of cybersecurity maturity. Siemens' change management program emphasizes achieving minimum security standards, raising awareness and enhancing skills, and bolstering supply chain resilience.

Siemens also has an experienced internal design authority enforcing secure-by-design principles and ensuring high levels of Product Solution Security. This includes Siemens ProductCERT which issues CVE's and responds to incidents affecting Siemens products. Siemens is also a leading member of the Charter of Trust which advocates 10 principles related to collaboration, transparency, security-by-default and resilience throughout the digital supply chain.

Positioning

- In the manufacturing vertical, Siemens security proposition is based heavily on "defense in depth", a multi-layered approach to security based on IEC 62443. This encompasses plant security, network security and system integrity. For network security Siemens provides its own range of security appliances (SCALANCE S) and routers (SCALANCE M) to support network segmentation and remote access.
- Siemens provides a comprehensive cybersecurity service that includes professional consulting services, software solutions and a managed cybersecurity services. The consulting services includes risk assessments and a complete change management solution involving security architecture design, implementation, training and incident response planning. Services include SiESTA, an asset discovery and security testing platform using in-house tools and 3rd party solutions, as well as Vilocify, a vulnerability management platform that facilitates product lifecycle management and patch management.
- Siemens' security services has a differentiated security service by industry vertical, offering specific tools, services and solutions to customers based on their industry requirement, from rail and road to power systems. Siemens Xcelertator © also offers industry specific IoT hardware and software solutions through via a digital marketplace.

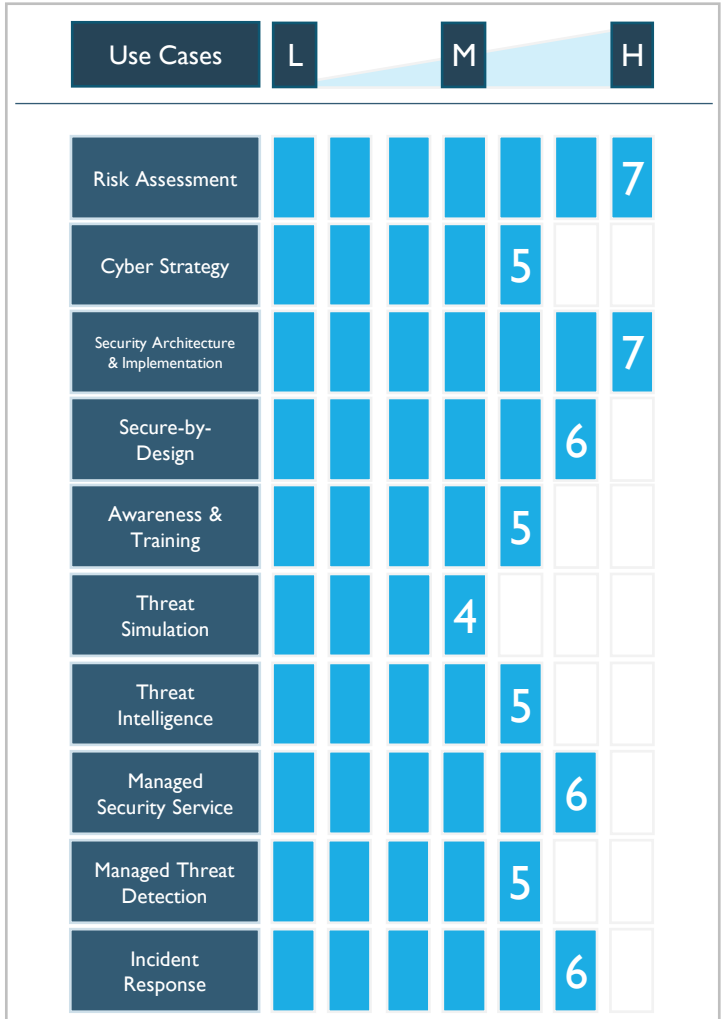
Known for

Leader in Industrial Automation and Software

Industrial Digital Services Innovator

Global OT Cybersecurity Service

Service Capability



Leader > Thales

Summary

Thales is a global technology and services organisation with sales of €17,6M in 2022 across Aerospace (27%), Defence & Security (52%) and Digital Identity & Security (21%). Organisational strengths includes a strong culture of R&D – the company invests 20% of sales into development – and engineering expertise.

The cybersecurity business consists of a market leading set of products related to data protection and IAM which form part of the Digital Identity & Security (DIS) group, and cybersecurity services which resides in the Defence & Security division. With the confirmed acquisition of Imperva, Thales' capabilities will extend to application security and total security revenues will exceed €2B. The intended acquisition of Tesserent, a cybersecurity services organisation with a strong customer base across critical infrastructure in Australia and New Zealand, will further expand Thales' capabilities and global coverage.

The cybersecurity services business grew in 2022 both organically and through the acquisitions of S21Sec and Excellium, expanding the Thales cybersecurity engineering team by over 500 additional staff to in excess of 3,000. The services business is based around the Cybels portfolio and includes:

- Risk & Threat Evaluation (Consulting services)
- Protect (Network and Data Security, Architecture Design and Integration)
- Train & Experiment (Training using immersive methods, testing in synthetic environments and cyber exercises using cyber ranges)
- Security & Operations (Build, Operate or Transfer capability including monitoring, detection and secure connectivity)

Positioning

- The OT cybersecurity business is a strategic priority for Thales and this has resulted in acquisitions, investments in OT SOC services, and an expanding network of experts. Thales provides an end-to-end OT cybersecurity service, delivered by a global team of OT subject matter experts and supported by a wider team of security engineers and consultants. Thales' strength is supporting clients in mission critical environments, including defence, critical national infrastructure and transportation. This includes providing sovereign solutions to meet national regulations. Thales' go-to-market model also addresses the needs of manufacturing customers that have a different risk profile and no sovereign requirement, providing a managed service from a global SOC.
- Knowledge and capability has been built through implementing OT security practices across its own manufacturing facilities and from decades of experience working with national infrastructure. World class facilities supporting the operational technology resilience challenge include training, exercising, system design and testing capability at the Thales Ebbw Vale site which also hosts the Welsh Government supported National Digital Exploitation Centre (NDEC). Similar facilities are also being created in Canada. There are also 11 CyberLabs covering NA, APAC and Europe that include cyber ranges and training facilities.
- The company has a strong position in Europe, with expertise in France, UK and through recent acquisitions Spain and the Netherlands. The business is supported by 11 SOCs (2 OT SOCs) globally

Known for

Trusted by Governments and National Infrastructure

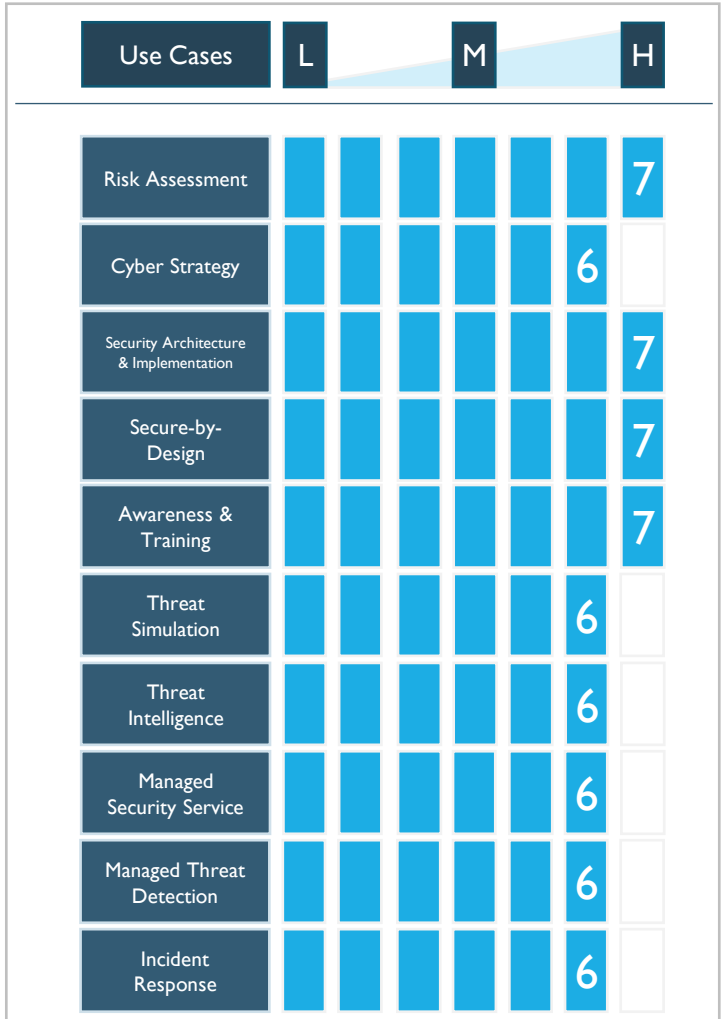
Security Products and Services

Global Leader in Digital Trust

Engineering Heritage

Cyber Sovereignty

Service Capability



Innovator > Dragos

Summary

Dragos was founded in 2016 and has since developed a reputation as an industrial partner, offering a comprehensive set of cybersecurity solutions and services.

Dragos is a private company based in Maryland. The latest funding round was completed in 2021 and to date the company has raised $364M. This has funded investment in the platform and staff – there are currently ~500 employees based mainly in the US. This also reflects Dragos' customer base which is largely North American though the company has expanded to the UK, Canada, Australia, New Zealand and Dubai, and is growing its network in Asia.

Dragos is both a platform and full cybersecurity services vendor. The Dragos Platform discovers and maps assets and networks, identifying vulnerabilities, quantifying risk and automating remediation. The threat detection is supported by industry leading OT-specific intelligence providing SOC analysts with context and supported by playbooks to accelerate response and support investigation.

The platform can be managed by the asset owner, 3rd parties or by Dragos' internal team of experts. The managed services team, OT Watch, augments customer SOC teams, providing ongoing advice, monitoring networks, and proactively hunting for threats. This service includes Incident Response retainers. Aside from managed services, Dragos also provides advisory services from architecture design to penetration testing and tabletop exercises.

Positioning

- Dragos is both a technology and services company, providing full partner support for customers including risk assessment, architecture design, platform management and incident response. This differs from industry peers who have a greater focus on using channel partners to consult, integrate and manage OT SOC operations.
- Dragos' reputation as a service partner has been developed through its founder's expertise and the assembled team of industry professionals who have deep experience and knowledge of Industrial Control Systems. This highly skilled team has resulted in Dragos being widely recognised as an ICS security consulting partner with a reputation for incident response. The adversary-centric approach that Dragos takes to OT includes a focus on evaluating the Tactics, Techniques and Procedures (TTPs) of threat actors. This is an important component to Dragos' industry leading OT-specific threat intelligence service – Worldview which includes critical alerts, weekly reports, industry specific threat perspectives, quarterly insights, and actionable defensive recommendations.
- Dragos is an active contributor to the ICS community and is recognised as a collaborative organisation. This is evident in its advisory roles to governments and participation in international forums. Initiatives also include Neighbourhood Keeper which is a free, anonymised opt-in program for Dragos customers to share insights, and the OT industry's first OT-Cyber Emergency Readiness Team (OT-CERT) which provides free OT cybersecurity resources for small- and midsized organisations.

Known for

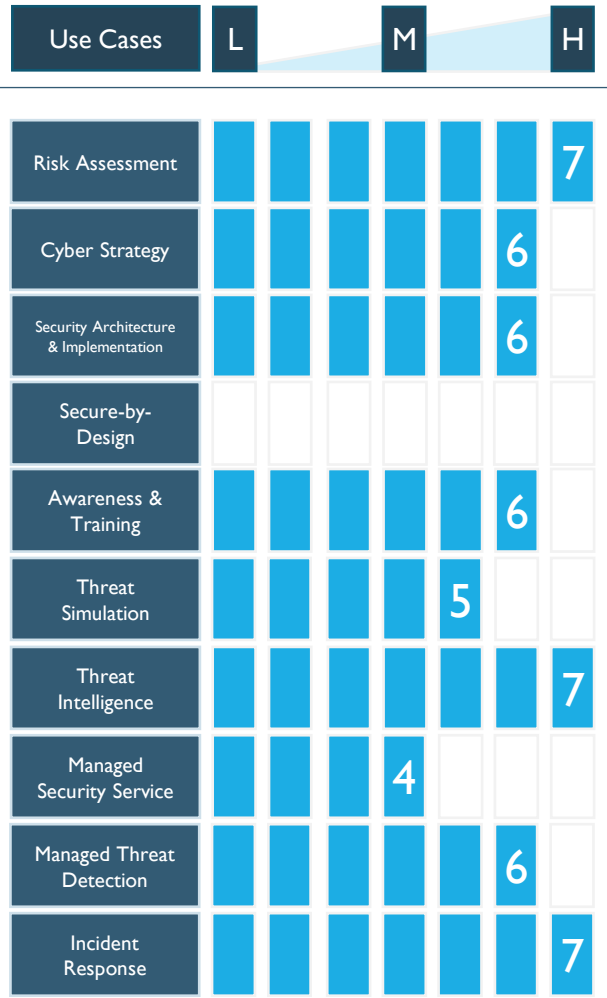
Unique positioning as an OT Platform and Managed Security Services provider

Incident Response

Leading OT-specific threat intelligence and curated vulnerability database

Strong U.S. government relationships

Service Capability



Innovator > Telekom Security

Summary

Telekom Security is a subsidiary of Deutsche Telekom Group, a global network service provider employing over 200,000 staff globally. Telekom Security (Deutsche Telekom Security GmbH) manages the security of Deutsche Telekom's European networks, is the security design authority for the group's solutions, and is responsible for delivering security services to the B2B customer segment.

Telekom Security has >1,600 specialists including ~1,300 technical staff including Threat Intelligence, SOC analysts, engineering and software development. The company operates 8 SOC's, providing global coverage to its customers from several sites in Europe, US, Mexico, and Singapore.

Telekom Security delivers an end-to-end IT and OT security service and a solution set that includes:

- Professional Security Services
- Cyber Defence (Managed Defence, Threat Intelligence)
- Infrastructure Security (Firewall, DDoS, SASE, SWG)
- Identity Security (including PKI & Key Management)
- Data Security (GRC services)
- Application Security (CSPM, CWP, WAF)
- Workplace Security (EDR)
- Industrial (OT SOC, SRA, Segmentation)

The OT cybersecurity business has grown from Telekom Security's relationship with leading manufacturers in Germany, including automotive OEM's. The company has a strong network of technology partners, and a team with knowledge of OT networks.

Positioning

- Telekom Security is a leading security services provider in Europe with a strong base of customers in the DACH region and global infrastructure and support to manage customer operations worldwide. As the managed security service provider of Europe's largest telecommunications network, and through its close working relationship with the German government and other critical infrastructure sectors, the company has privileged access to the security challenges and threats to national infrastructure. This has resulted in a leading Threat Intelligence service and other notable innovations including automated threat hunting technologies including blackhole monitoring and honeypots.
- The company has a strong record of providing both IT and OT security services, managing security transformation across both enterprise and industrial operations. The lead service is usually the 'Orientation Workshop' followed by security assessments, architecture design and management of security operations.
- The company has the technical experience and services to help organisations transition to wireless and cloud infrastructure, moving organisations to Zero Trust models through securing and monitoring IoT components and operations.
- The Threat Intelligence unit and service, built on a combination of open source, closed source, community sources and self-developed sources (DNS platform, Honeypot Network etc), provides customers with insight and bulletins on TTP's

Known for

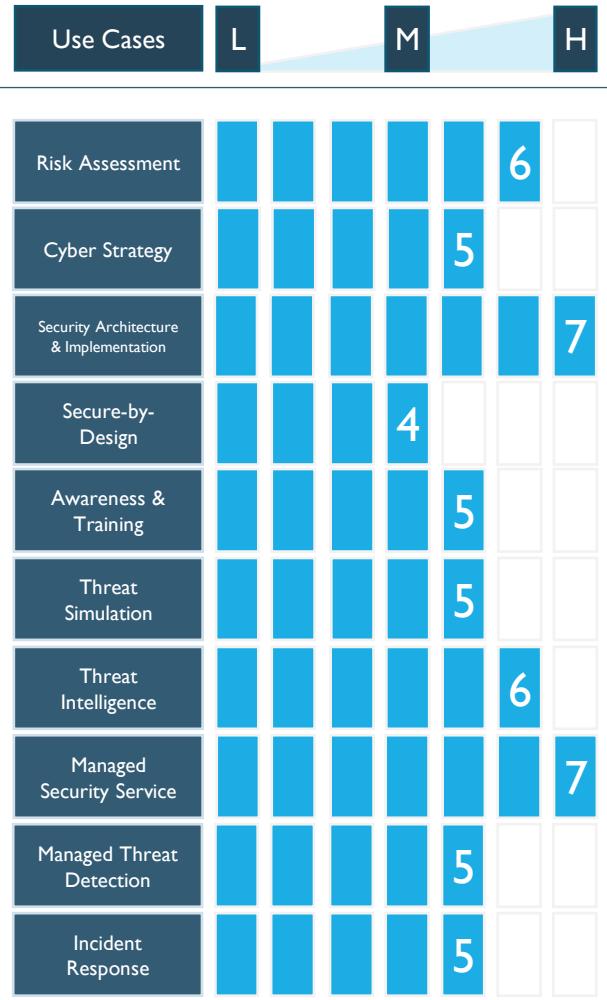
Management of Deutsche Telekom's networks

Technical expertise related to wireless networks, OT systems and security architecture

Advisor to German government on threats to national infrastructure

Threat Intelligence

Service Capability



Innovator > Yokogawa

Summary

Yokogawa is a Japanese headquartered industrial automation vendor with global operations. Company sales grew by 17% in 2022, reaching $3.4B.

The Controls business is the largest unit comprising ~94% of sales. Japan is the single largest country by sales, whilst Asia and Middle East & Africa are the largest regional sales territories. Upstream and downstream Oil & Gas, power generation and chemicals generate over 50% of revenues.

Yokogawa's strategic focus is on providing a growing portfolio of lifecycle services that aid the digital transformation of customer operations. This includes enabling remote management, asset lifecycle management, and improved IT/OT security operations.

The digital transformation program started in 2018 as part of the TF2020 mid-term business plan and has continued as part of Accelerate 2023 which is focussed on internal and external transformation. This has resulted in a shift to delivering cloud based business models, shifting traditional applications to the cloud and releasing new services including OT cybersecurity on Yokogawa Cloud.

OpreX Safety & Security, part of the Oprex Lifecycle business line, includes security consulting and managed security services.

Positioning

- Yokogawa's focus is on delivering security throughout the lifecycle of the plant. This starts with the security assessment, design and implementation of controls, monitoring, and auditing of the controls.
- The Yokogawa OpreX™ IT/OT Security Operations Center (SOC), built of Elastic Cloud services, was designed to provide an IoT security solution for plants, providing real time monitoring of both IT and OT networks. The service originated from Yokogawa's internal SOC (Y-SOC), which monitored IT and OT, including cloud applications, across Yokogawa's 16 bases around the world. The service is built around five stages, including the implementation of reactive security controls (Security Perimeter and SIEM migration) and proactive measures Advanced Analytics, Security Automation and Predictive Analytics). Yokogawa's roadmap includes extended monitoring to 3rd party OT products and to apply MITRE ATT&CK for ICS.
- Yokogawa's security operation network consists of 6 sites in Japan, Singapore, Netherlands, India, Thailand and Romania. Global Security Competence Laboratory (SCL) in Singapore and Japan are Centres of Excellence and research centres for testing of solutions and creation of new security capabilities.

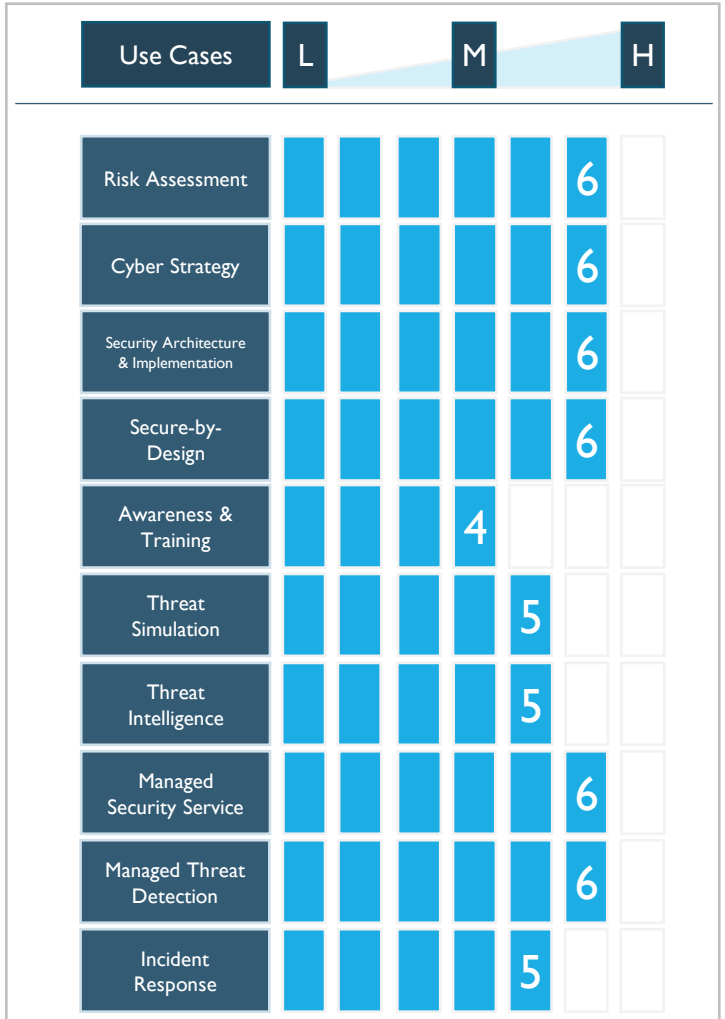
Known for

Leading industrial automation vendor

Strong customer base across Asia

OT cloud security platform

Service Capability

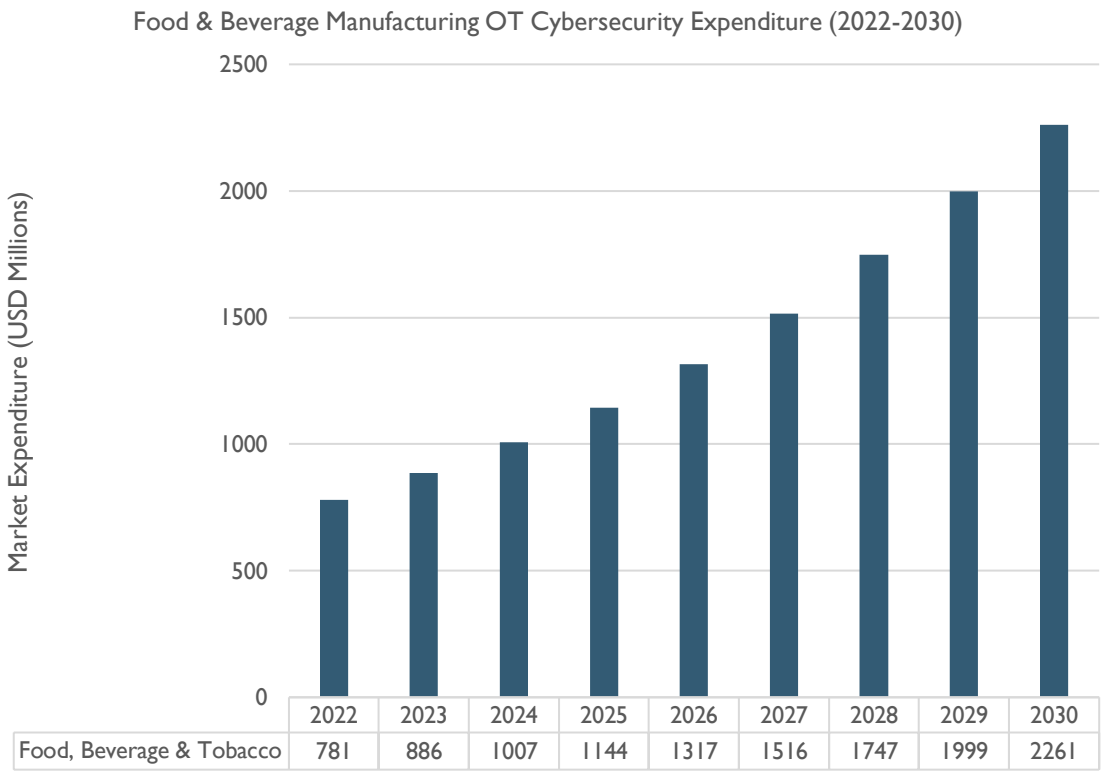


Appendix 1
Vertical Market Trends

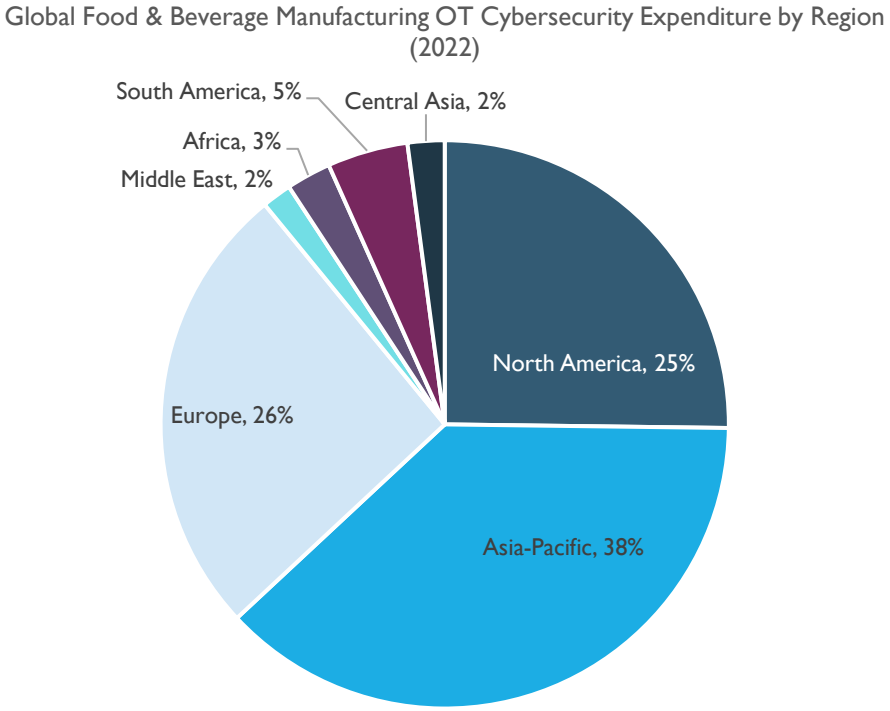
Food & Beverage price rises have resulted in high profitability for many manufacturers and increasing CAPEX

2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Food production in 2022 was characterised by shortages and rising prices due to the war in Ukraine and adverse weather in key production regions.		Food production is expected to increase over the forecast period as supply chain challenges are solved.	Awareness of the cyber threat to the Food & Beverage industry has increased following well documented ransomware attacks on several food producers. This includes JBS Foods which resulted in operational downtime, loss of revenues and payment of the ransomware demand. Interconnected, interdependent supply chains have resulted in increasing connectivity between sites and processes increasing the threat surface. At an OT level there is an increasing requirement to reassess risk as a result of changing operations and growing vulnerabilities. Key OT use-cases include network segmentation between different stages of the food or beverage process, for example treatment of water to avoid contamination, and bottling of the final product. Asset discovery, threat detection and secure remote access management for third party vendors are in high demand from customers that are starting the OT cybersecurity maturity journey. Increasing consumer demand related to traceability and sustainability, and a strengthening regulatory environment, will result in increasingly digitalised operations and connected supply chains. This is likely to result in greater connectivity and exploitation of data. Westlands Advisory predicts that there will be greater convergence between IT security operations and OT as the boundaries become increasingly blurred. There will be an increased focus on operational resilience across the business and a renewed focus on incident response to minimise the impact of any disruption. Security standards that are typically followed include ISA/IEC-62443, ISO-27001 and NIST CSF whilst IEC 61508 is followed related to safety.
A large number of food production companies reported **record profits** in 2022 with inflationary price rises being pushed to the consumer.		Profitability is likely to return to 'normal' levels once prices and the market has stabilised.	
Manufacturing investment in digitalisation is increasing, leading to higher automation and use of analytics as producers look to meet ESG goals around efficiency, sustainability, and traceability.		Broader and deeper implementation of automation and IIoT to deliver cost reduction and improved performance.	
Increasing regulation of the Food & Beverage. F&B is included in the EU's NIS2 and recent Australian regulations.		WA expects regulation to increase to improve the resilience of food supply chains whilst industry specific standards related to food safety and production are likely to evolve (e.g. TACCP, EU PAS96:2017).	
The cyber threat to Food & Beverage industry production is primarily **ransomware.**		The cyber threat is expected to remain stable throughout the forecast period.	

Food & Beverage TAM between 2023-2030 is $11.9B with a CAGR of 14%. International food brands and local production means investment will be split across regions.



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Food, Beverage & Tobacco	781	886	1007	1144	1317	1516	1747	1999	2261



Definition: Manufacture and processing of food products and beverages including fermentation and distilling processes and packaging and bottling, and manufacture of tobacco and tobacco substitute products

Automotive DX, growing regulatory requirements and a focus on supply chain resilience will continue to influence OT cybersecurity programs

WESTLANDS ADVISORY

2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Car sales in 2022 were similar to 2021 at 66 million*, still down on pre pandemic levels though recovering at the end of the year from an earlier drop in production due to semiconductor shortages.		**New car sales expected to recover** globally as economies move beyond recession and emissions regulation pushes drivers from second hand market to EV.	Automotive Cybersecurity requires protection of the vehicle (platform), the systems connecting the vehicle to diagnostics and other applications, the OEM's enterprise and operational processes, and the supply chain. At the platform level there is greater onboard protection including authentication, embedded firewalls and a focus on zero trust architectures. Vehicle design relies on data from the operational fleet, resulting in performance and usage data being consumed in cloud platforms to inform design and production. The connectivity between the consumer, OEM and supply chain requires cybersecurity controls at many levels. UNECE WP.29 forms part of a process to improve automotive resilience which requires each OEM to implement a Cybersecurity Management System to be operational by mid 2022. This will be rolled out to Tier 1,2 and 3 vendors who will need to show compliance at later dates. The result of UNECE WP.29 will be an end-to-end approach to security, ensuring that risk is understood, controls are implemented, and threats actively monitored across the automotive supply chain. Westlands Advisory expects greater use of threat detection, improved implementation of OT best practices and a greater focus on Software Bill of Materials (SBOM). ISO 21434 was released in 2021, specifying the risk management approaches required from product development to operation and maintenance of electrical and electronic systems in road vehicles and is expected to provide the guidance for embedding the appropriate GRC processes and procedures, security testing of software and embedded systems, and secure by design. Further standards include Global Auto Alliance Framework for Automotive Cyber Security Best Practices, ENISA Good Practices for Security of Smart Cars and Resilience of Smart Cars, Auto ISAC best practice document, Society of Automotive Engineers SAE J3061, US Congress SPY Car Act 2019.
Car production continues to shift East as manufacturing increases in countries with high local demand. Car production in Asia grew over 10% and accounts for 34% of global production*. The strongest y.o.y. growth was India 21.6% and Indonesia 24.3%.		A growing middle class in developing countries will result in the **continuing production growth in APAC** and is also likely to extend to Electric Vehicles. China is already the largest producer of EVs.	
The number of **connected cars is growing**. As of 2022, connected vehicles account for approximately 50% of total car sales. This percentage is expected to rise year on year, reaching 95% by 2030.		**By 2030 almost all new cars will be connected. Mass adoption of autonomous vehicles still limited** with lack of confidence regarding safety and communications infrastructure needing to improve.	
Growing focus on ESG. Sustainability is a key focus for automotive manufacturers, including the carbon footprint of their car fleet and the energy consumption and emissions related to production.		ESG focus will lead to **energy efficient manufacturing** driven by DX, and a focus on lowering the energy consumption of switches and security appliances.	
Cyber maturity and standards are slowly improving with the introduction of WP.29 CSMS regulation and ISO/SAE 21434 standard. However there is little to mandate specific levels of cyber security across the automotive ecosystem and OEMs and suppliers have taken different approaches to cyber security creating gaps and vulnerabilities.		Investment in operational resilience – driven in part by NIS2 – will result in the **growing cybersecurity maturity of the supply chain by 2030.**	

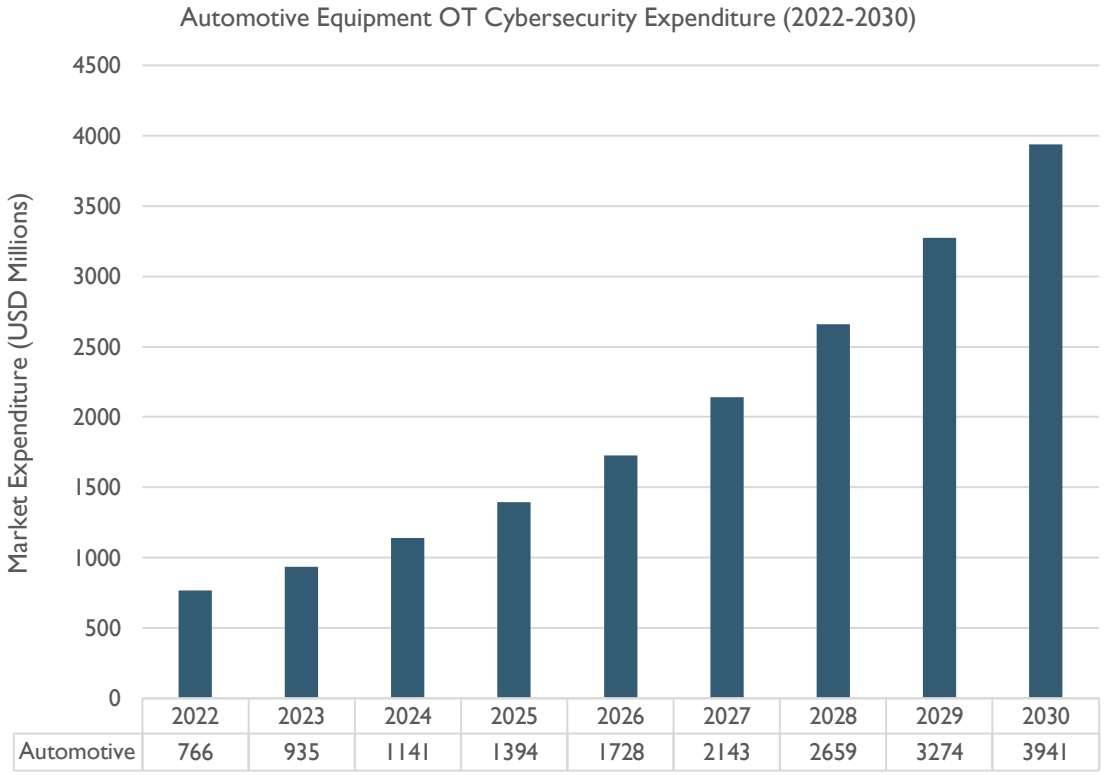
*https://www.acea.auto/files/Economic-and-Market-Report_Full-year-2022.pdf

 Weakening

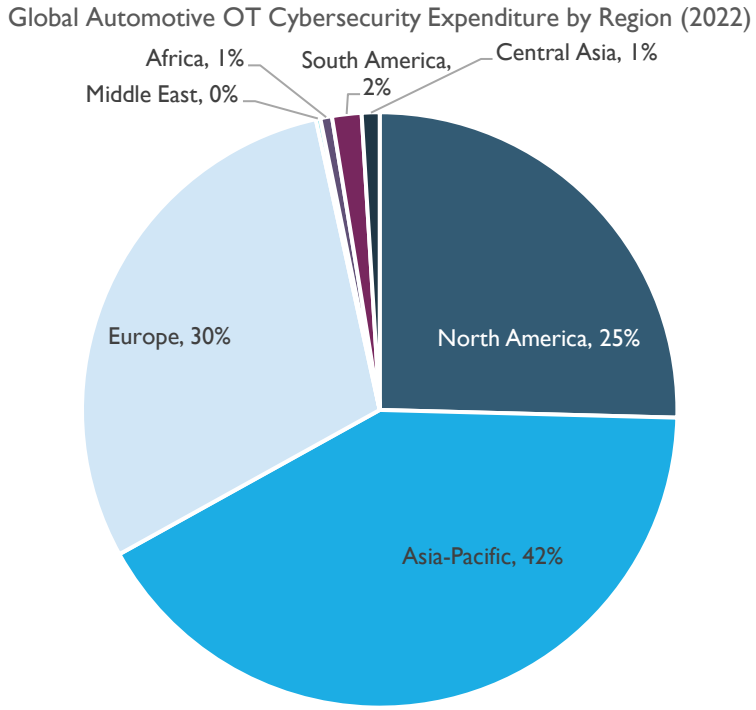
 Stable

 Strengthening

Automotive Manufacturing TAM between 2023-2030 is $17.2B with a CAGR of 23% in the main car production centres across Europe, North America and Asia Pacific.



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Automotive	766	935	1141	1394	1728	2143	2659	3274	3941



Definition: Includes motor vehicles (cars, lorries, vans, buses). Does not include electric motors (see Electrical) but does include parts and accessories including alternators, ignition wiring, power systems (windows and doors), brakes, gearboxes, exhausts, steering wheels, clutches, convertors, and accessories including belts, airbags, bumpers.

High R&D costs, supply chain pressures and growing global competition is resulting in the DX of pharmaceutical discovery and production processes and growing investment in security

2023 Trend	2030 Outlook	2030 Status
Investment in R&D is high comparative to other industries* and this is unlikely to change due to competitive forces and high demand.		Investment in US and Europe is likely to continue to maintain competitive advantage though R&D is increasing in China.
Continued investment in DX to improve discovery and enable remote monitoring in trials, connected supply chains and smart factory concepts to improve yields and improve efficiency (lower energy consumption)		Digitally enabled pharmaceutical operations leading to more efficient production of pharmaceutical products and organisational improvement related to ESG initiatives.
Pharmaceutical development, technology transfer and manufacturing are increasingly digitally linked, connecting a wide ecosystem of **partners including universities, hospitals, start-ups and clinical trial companies, contract manufacturers**		Greater collaboration and joint ventures to accelerate discovery and share risk.
Growing use of Contract Development Manufacturing Organisations (CDMO). Service providers principally provide one or all of the following services – product development, manufacturing of Active Pharmaceutical Ingredients (API) and Finished Dosage Forms (FDF).		The growth of CMDO's has resulted in a growing industrial base in APAC. This trend is expected to continue with growing globalisation of pharmaceutical production.
A high level of threat exists to pharmaceutical companies driven largely by the risk of IP theft and ransomware, resulting in **growing investment in cyber resilience** across IT and OT.		**Investment is likely to continue** to increase over the forecast period. Pharmaceuticals is likely to be one of the most resilient manufacturing sectors with a higher level of cybersecurity driven in part by an increasing focus on governance and growing regulation (e.g. NIS2).

Cyber Security Impact and Implications

Pharmaceutical manufacturing involves a set of processes to manage the Active Pharmaceutical Ingredient (API) consistently so that is can be delivered to the patient. Prior to industrial scale manufacturing, the drug development process includes discovery and development, preclinical research, clinical research and review. The manufacturing process is dependent on whether the product is a liquid, solid or drug device but typically includes dispensing, mixing/blending, filtration/compression/device filling, coating/polishing/device assembly and packaging.

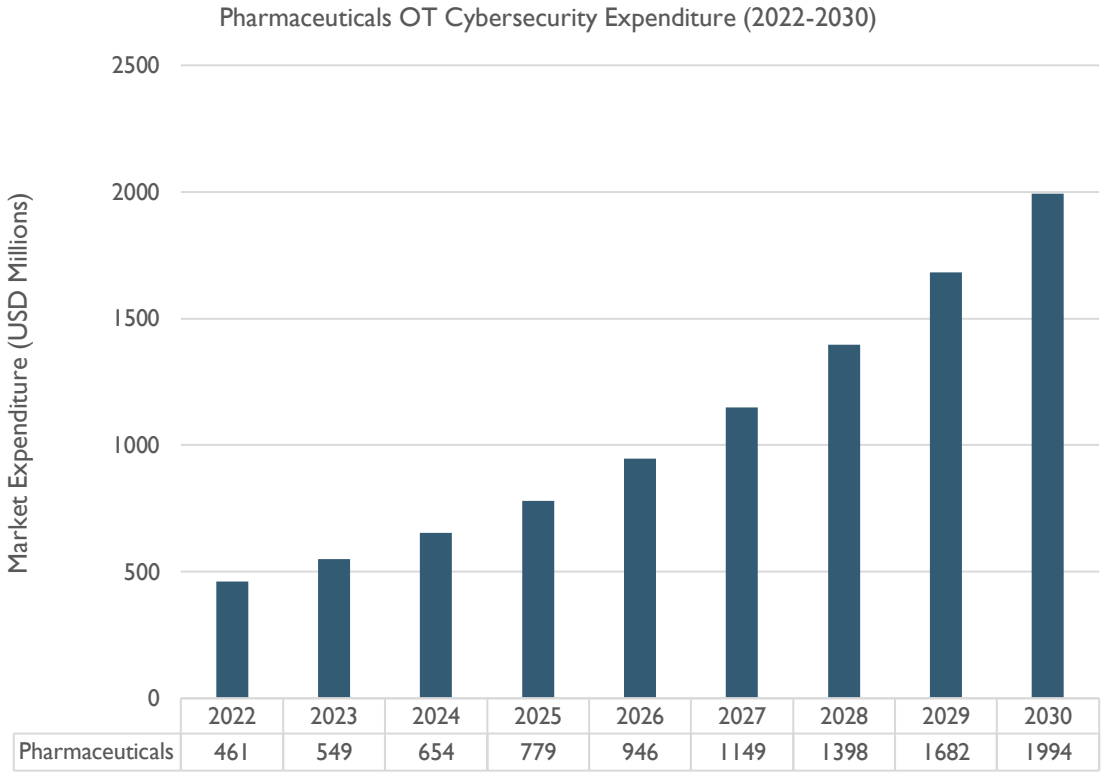
There is an ongoing cyber risk. This includes potential loss of IP and competitive advantage, leaked Personally Identifiable Information, and compromised systems availability. A report from Constella highlights the high volume of data loss in the industry including the credentials of employees. The Merck incident in 2017 – one of the many victims of NotPetya – highlights the risk to pharma manufacturing firms. The incident impacted Merck's inhouse production of API and its formulation and packaging operations resulting in an estimated > $1 billion in losses.

Pharmaceutical companies generally follow the FDA's **CGMP (Current Good Manufacturing Practice Regulations)** to ensure appropriate methods and controls are used throughout the drug development lifecycle. Additional guidance includes ICH Q8 (R2), FDA's Process Analytical Technology Guidance and ICH Q9 Quality Risk Management. Security standards that are typically followed include **ISA/IEC-62443**, ISO-27001 and NIST which is recommended in the FDA's Quality System Regulation.

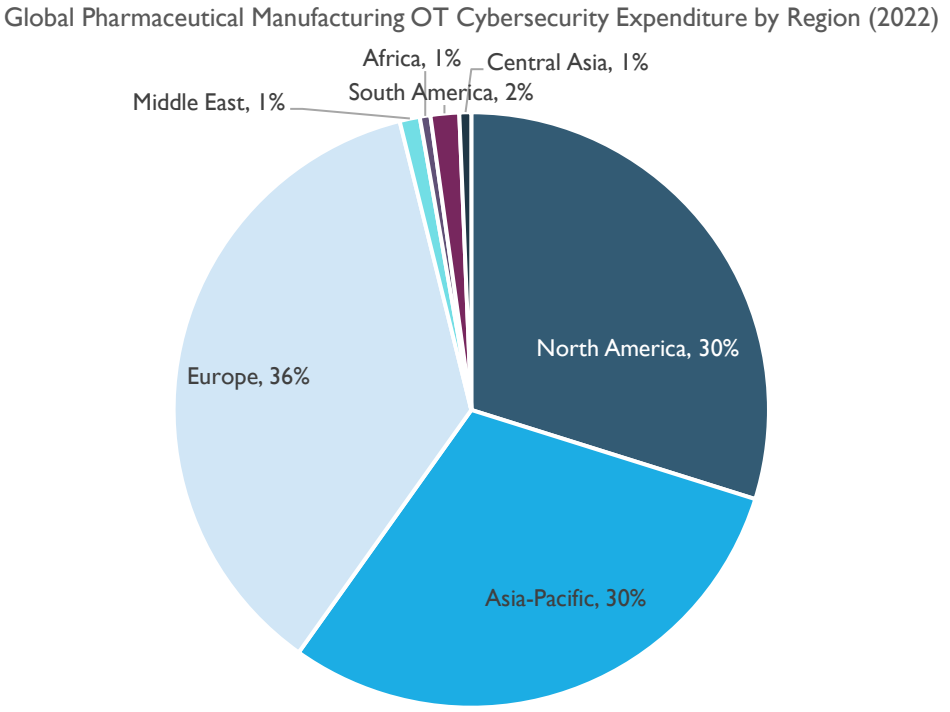
Important manufacturing use cases include OT network segmentation, asset discovery and threat detection across on-prem and cloud assets, electronic records management, third party monitoring and remote assess management.

* https://www.efpia.eu/media/637143/the-pharmaceutical-industry-in-figures-2022.pdf

Pharmaceuticals Manufacturing TAM between 2023-2030 is $9.2B with a CAGR of 20% with high investment in developed and some significant developing economies.



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Pharmaceuticals	461	549	654	779	946	1149	1398	1682	1994



Definition: Manufacture of medicinal active substances (e.g. vitamins, antibiotics) and pharmaceutical products including vaccines, diagnostic preparations (e.g. pregnancy tests), medical impregnated wadding and dressings, and botanical products.

Manufacturing production has increased steadily since 2020; however manufacturers still face economic and supply chain uncertainty and cybersecurity program maturity remains low

WESTLANDS ADVISORY

2023 Trend	2030 Outlook	2030 Status
Global manufacturing growth remains modest with the latest UNIDO analysis reporting a 3.6% y.o.y growth in production in Q3 2022 due largely to an improvement in China's performance (4.5% for the same period).		**Total global production is expected to increase steadily** to 2030 however inflation, supply chain shocks and trade restrictions are likely to restrain production in the short term.
Production growth is not equal across all industries. Production of electrical equipment and clothing has increased significantly in the last year whilst wood products, textiles and other non-metallic have fallen.		**Growing economic wealth will result in increased demand for consumables** including household appliances and fashion which will sustain growth in these industries.
New manufacturing economies are emerging as countries industrialise and global brands seek lower cost production. Production in Viet Nam and Malaysia grew at >10% y.o.y.		**Continued expansion of manufacturing in emerging economies** is expected but will also be tempered by increasing **onshoring of critical manufacturing industries** to improve supply chain resilience.
Cyber security regulation will start to push the supply chain to improve cybersecurity programs. NIS2 places more emphasis on suppliers to critical infrastructure and key industries to meet cybersecurity standards. However, it will take time to understand the impact of cybersecurity maturity.		Cybersecurity maturity is likely to **improve in higher technology industries** but currently **there is uncertainty about improvement in traditional manufacturing segments**. This will be dependent on the requirements in the regulation and the level of enforcement.
The threat to businesses from ransomware or misconfigurations that compromise availability or safety will remain the largest investment driver for most manufacturers. The SMB segment which comprises a large percentage of manufacturing are struggling to initiate cybersecurity programs**.**		The **threat to manufacturing operations is likely to remain stable to 2030** and will be addressed through solutions designed for the SMB market which will include easy to deploy and cheaper products.

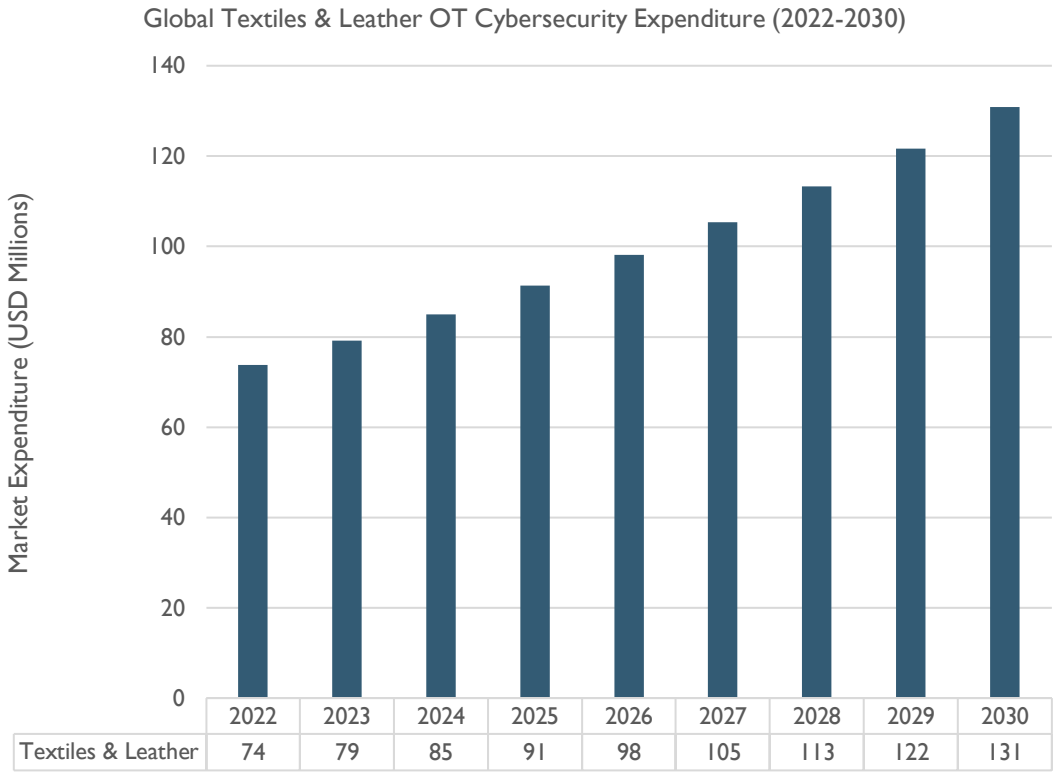
Cyber Security Impact and Implications

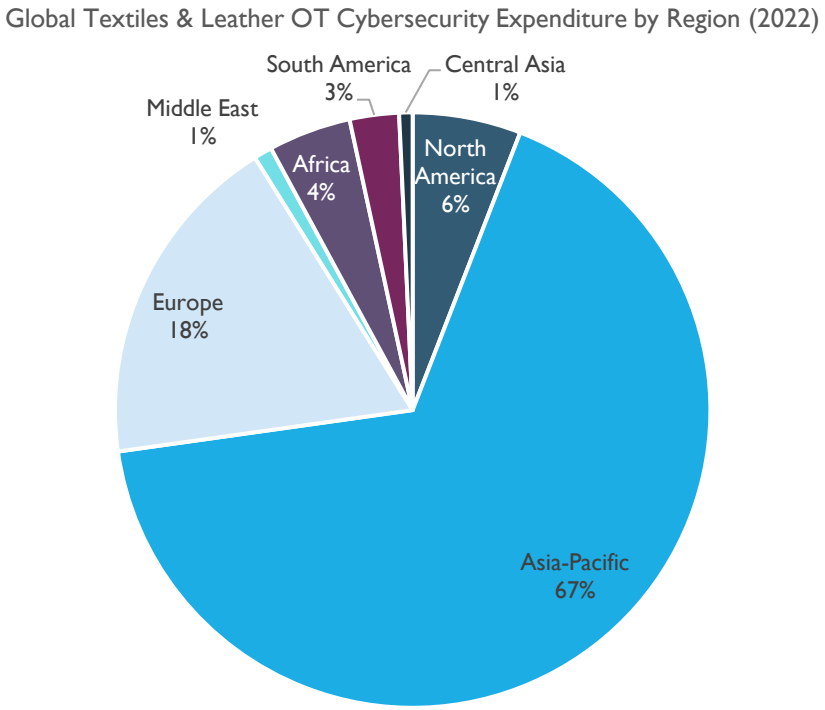
The Discrete Manufacturing segment is the largest sector due to the volume and diversity of companies included in this category. Large transformational manufacturing programs slowed in 2020/21 and this was reflected in both economic data (reduced shipments, factory closures) and financial data (significant drop in automation vendor revenues). However, the impact was not consistent around the world with Europe and North America being more heavily impacted. 2022 is expected to see a considerable bounce back in discrete manufacturing, not withstanding continuing supply chain issues, resulting in investment in plant modernisation.

Most large, international, discrete Manufacturing firms follow NIST and IEC 62443 and are more likely to invest in improving the level of plant automation and increasing connectivity between systems, sites and third party vendors. Business drivers will include a focus on efficient, agile and safe production with an increasing focus on sustainable manufacturing (lower energy consumption, reusable materials). The OT cybersecurity requirements of these firms will include professional services partners that can manage complex, international projects, with an ability to assess, tune, and implement asset discovery and threat detection tools. Network segmentation, vulnerability management and threat management are likely to be the most demanded services.

However, there is a very large SME ecosystem that will not follow standards. NISTIR 8183 was produced to provide a lighter set of standards for the SME community. SMEs are unlikely to invest in advanced technologies unless mandated to do so by supply chain partners or through regulatory authorities (if for example they are classified as Critical National Infrastructure providers). Outsourcing risk and monitoring to a localised MDR firm is the most likely customer scenario.

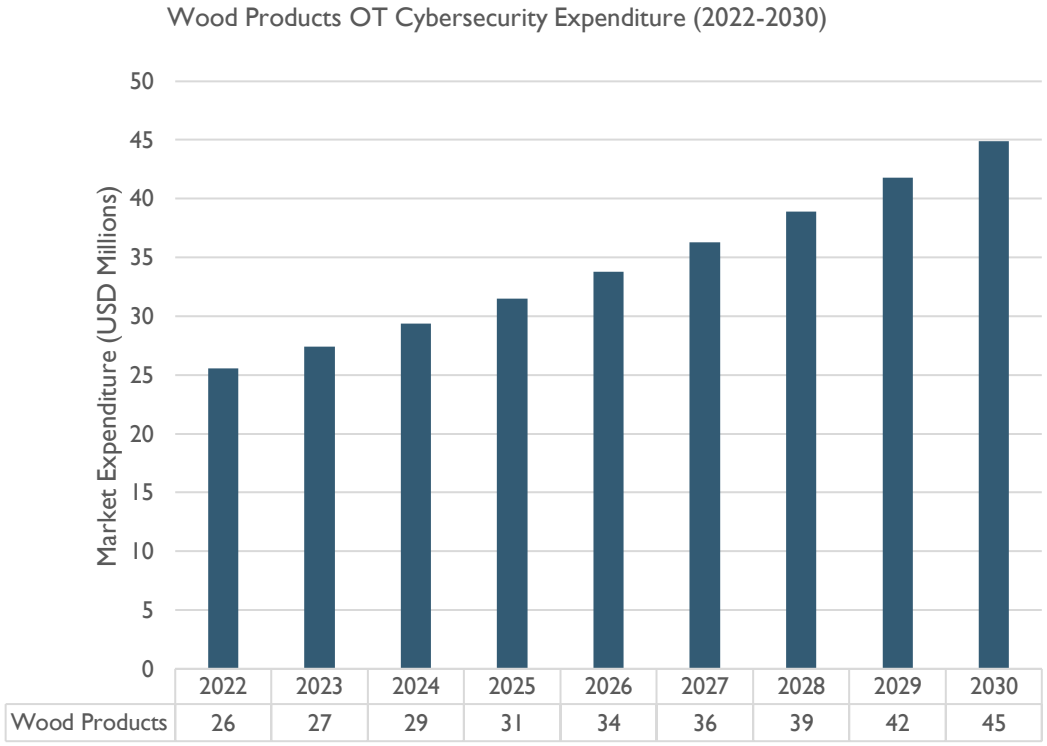
The Textile and Leather manufacturing industry is a small market with 67% of expenditure in APAC. Global CAGR from 2022-2030 is 7%

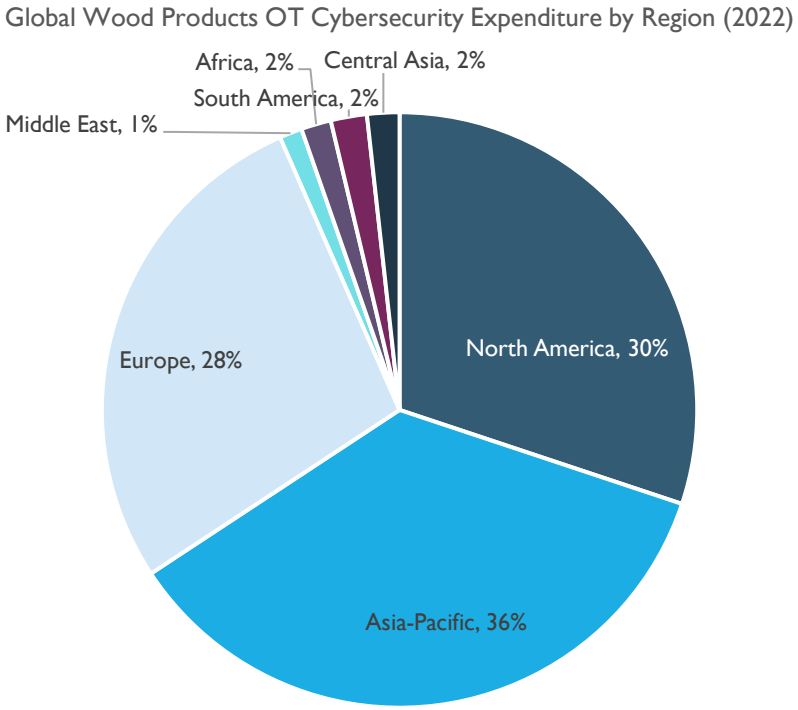




Definition: Preparation and spinning of textile fibres, weaving finishing of apparel and household products including rugs, soft furnishings and rope. Also includes the processing and preparation of leather products including bags and shoes.

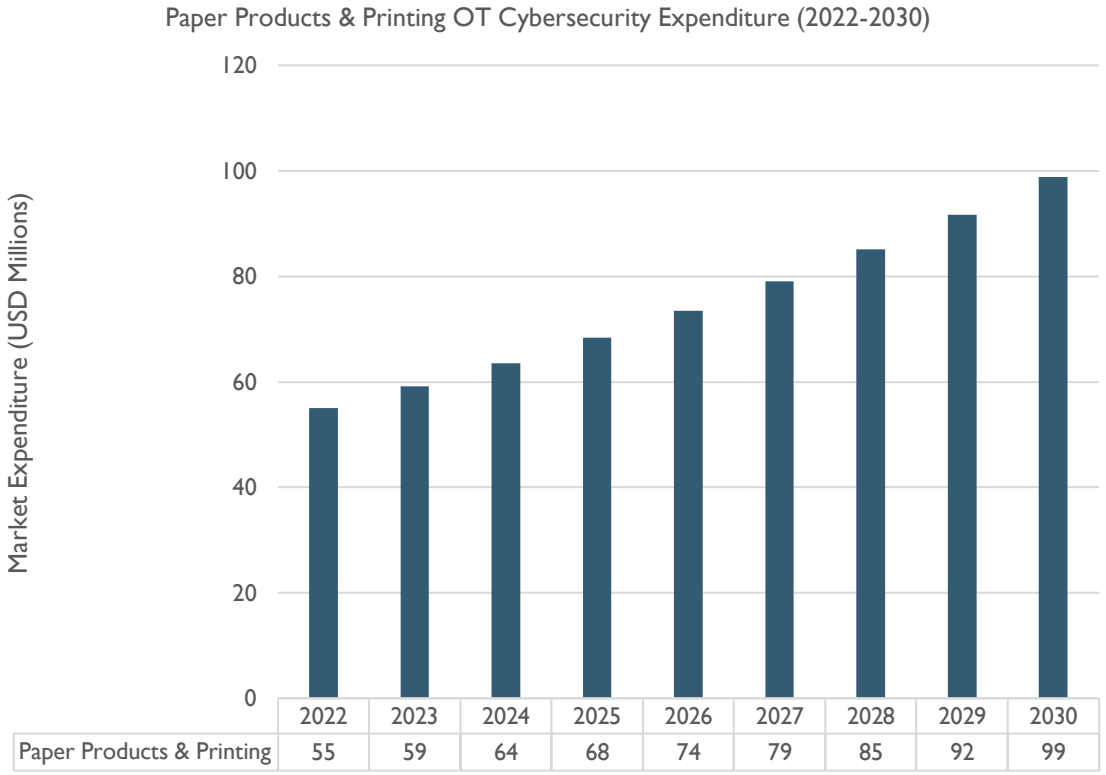
Wood Product Manufacturing TAM between 2023-2030 is $283M with a CAGR of 7%



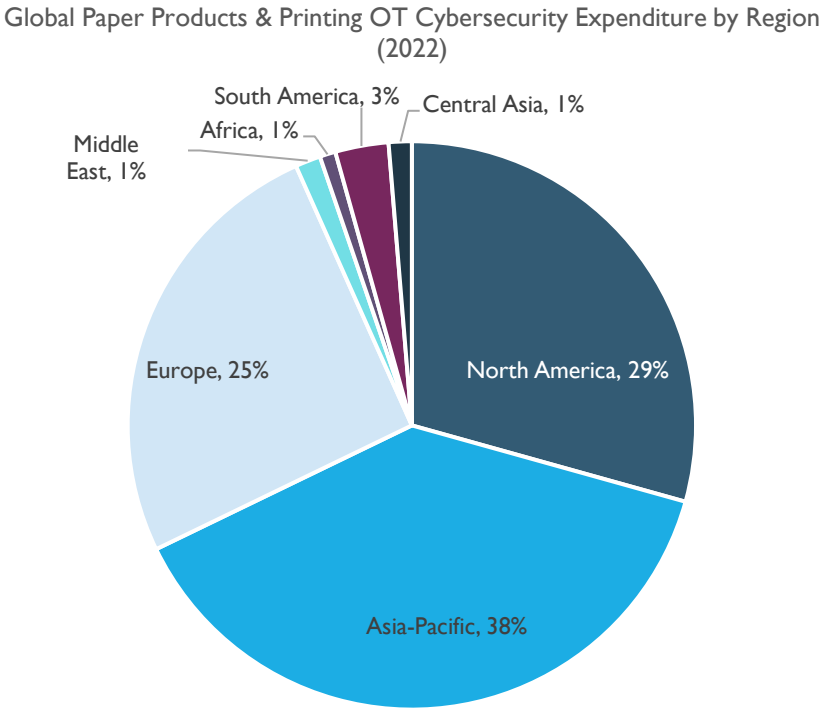


Definition: Sawing, planing, shaping and laminating of wooden products including flooring, prefabricated products such as buildings, wooden products for buildings, containers etc.

Paper Product Manufacturing TAM between 2023-2030 is $620M with a CAGR of 8%

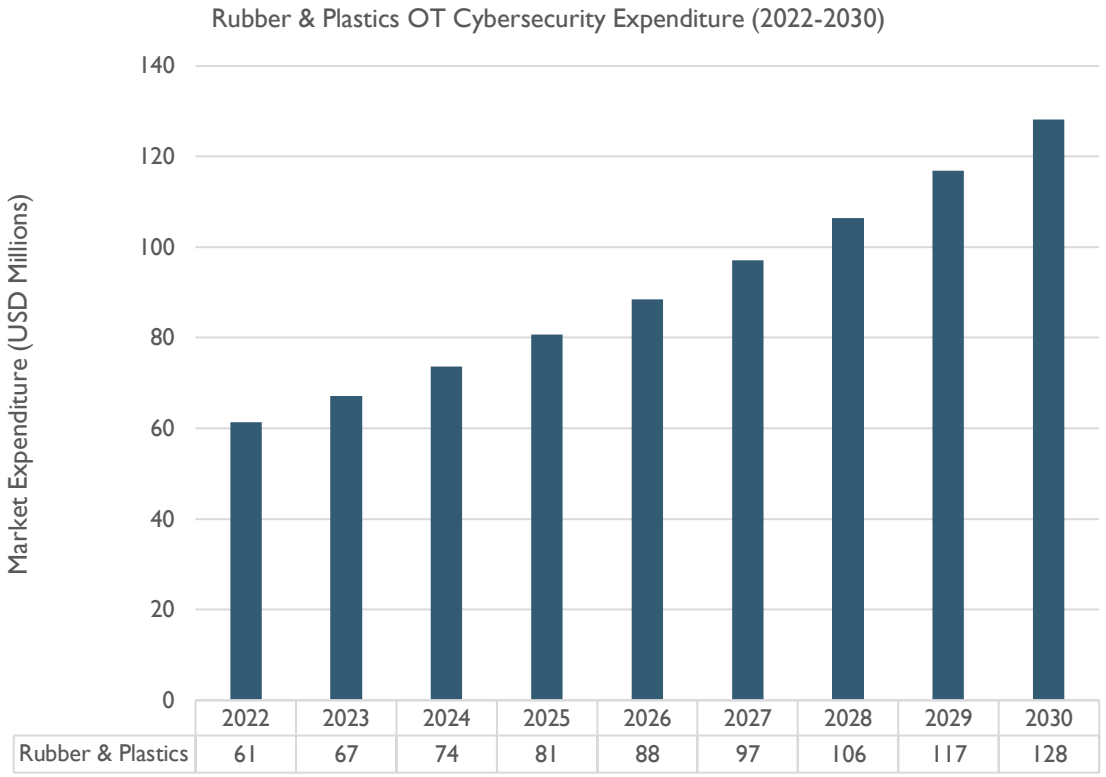


	2022	2023	2024	2025	2026	2027	2028	2029	2030
Paper Products & Printing	55	59	64	68	74	79	85	92	99

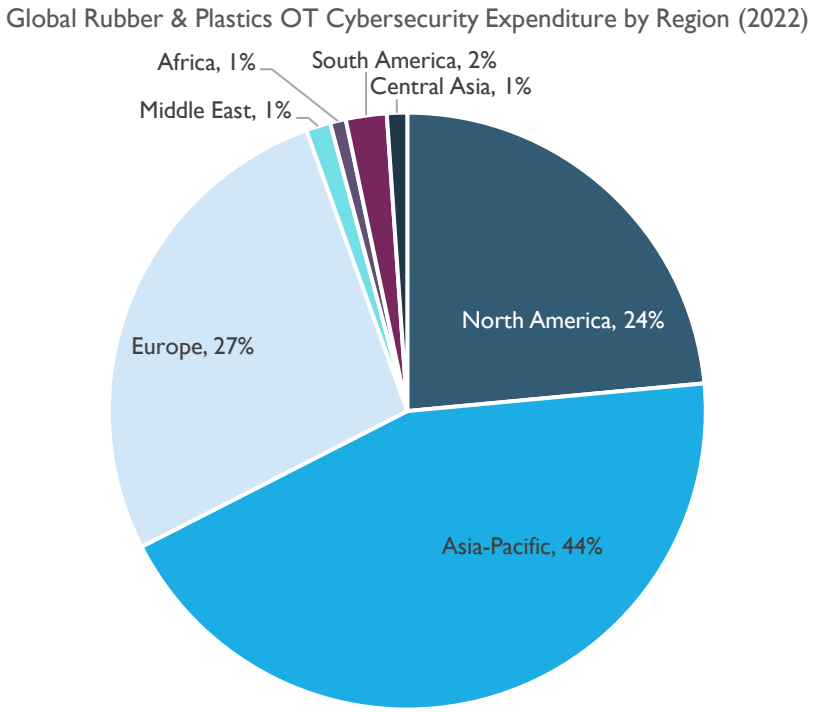


Definition: Processing of pulp and manufacture of paper and paperboard, and final product production including containers, stationary, toilet paper. Also includes printing of newspapers, books etc.

Rubber & Plastics Manufacturing TAM between 2023-2030 is $759M with a CAGR of 10%

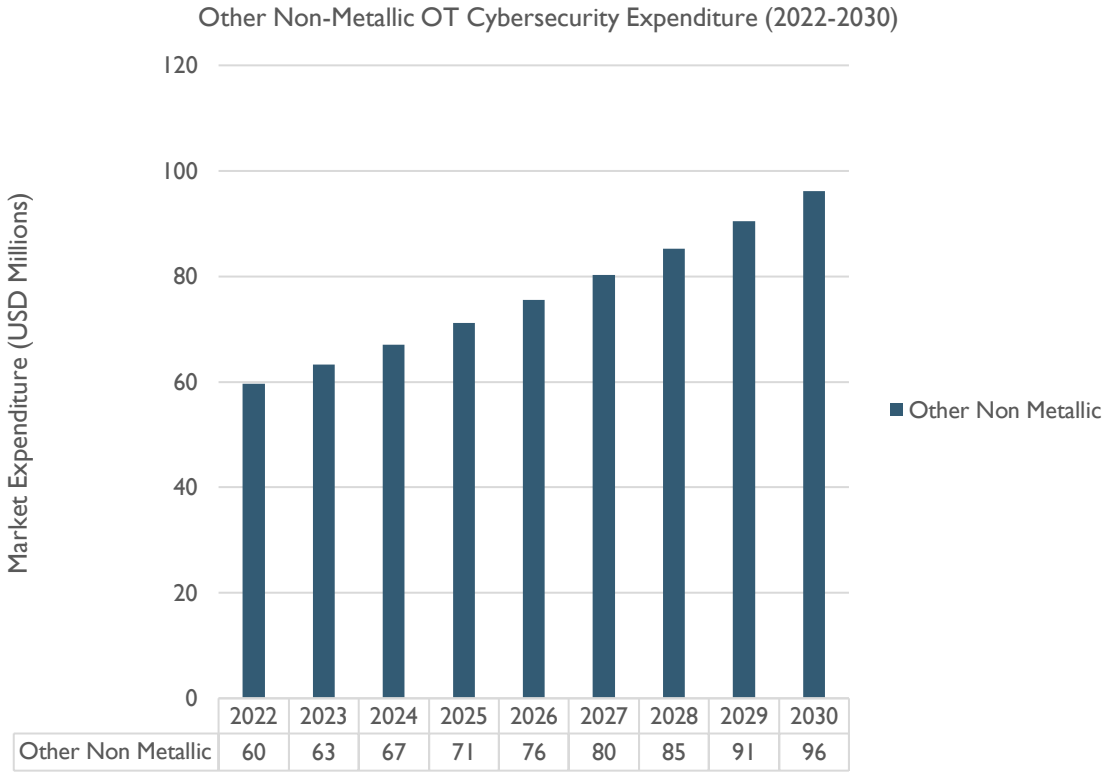


	2022	2023	2024	2025	2026	2027	2028	2029	2030
Rubber & Plastics	61	67	74	81	88	97	106	117	128

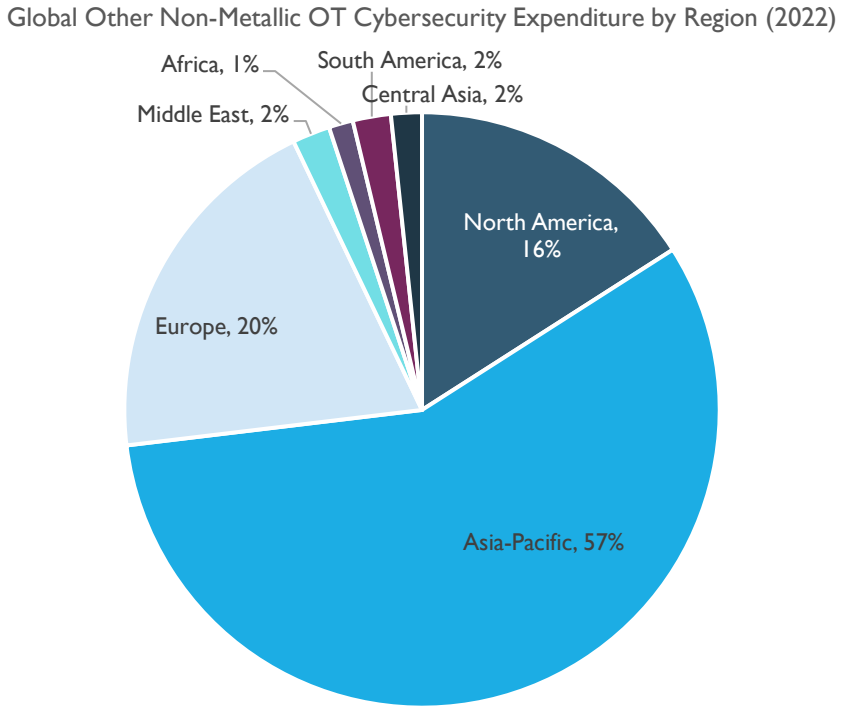


Definition: Manufacture of rubber (e.g. plastic products including automotive tyres, tubes, pipes, hoses, belts, sheets, seals etc) and plastic goods (e.g. tubes, pipes, containers, bottles, flooring, tableware etc).

Other Non-Metallic Manufacturing TAM between 2023-2030 is $629M with a CAGR of 6%

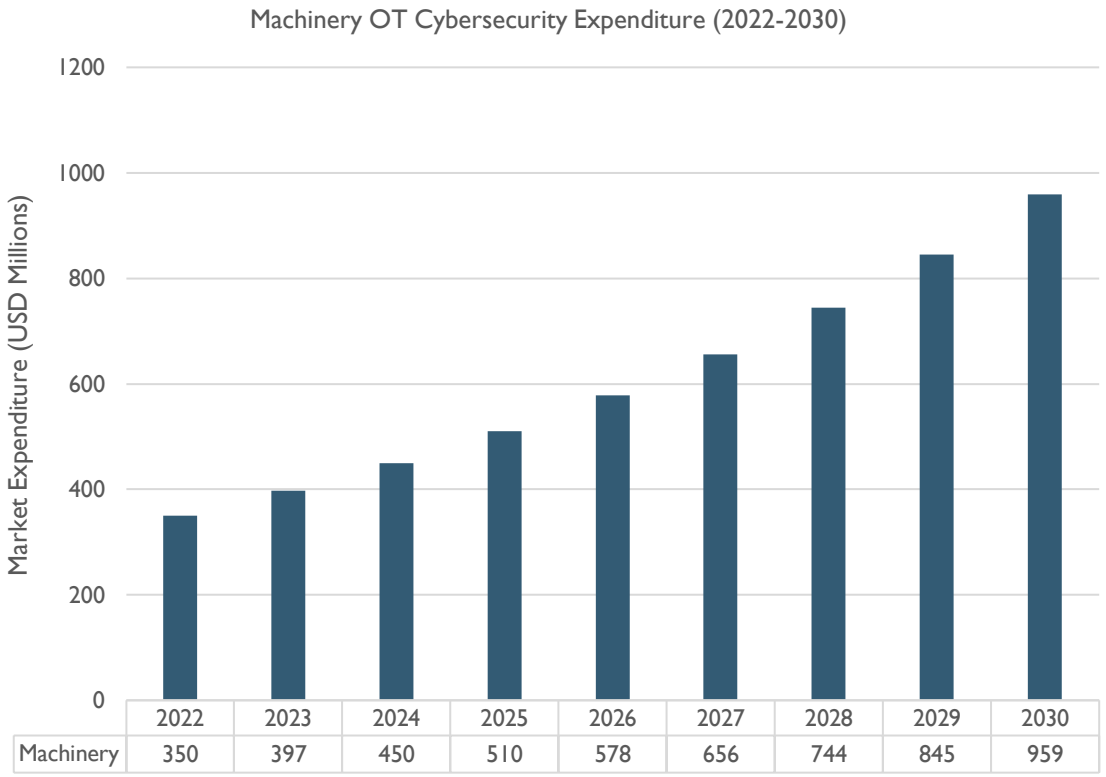


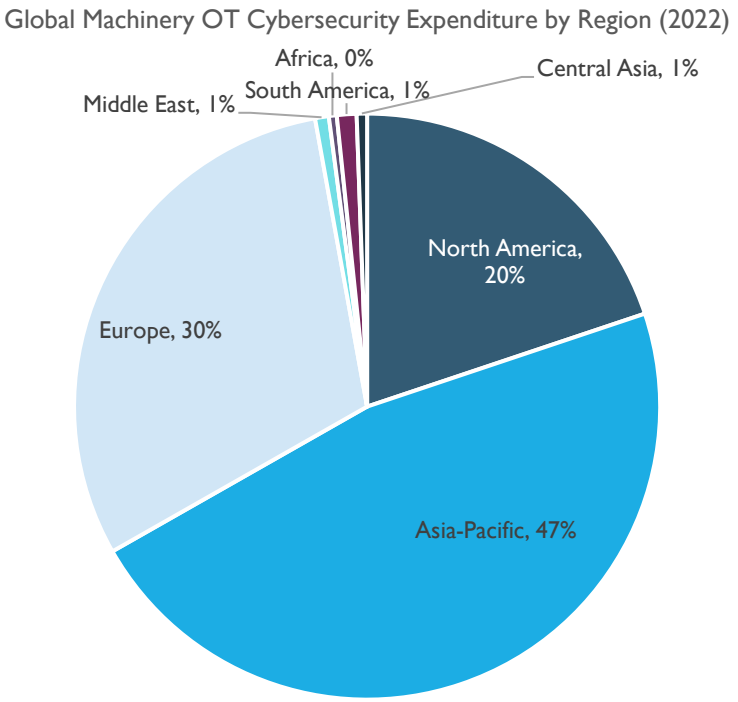
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other Non Metallic	60	63	67	71	76	80	85	91	96



Definition: Manufacturing of glass and glass products, ceramics, tiles, bricks, and cement.

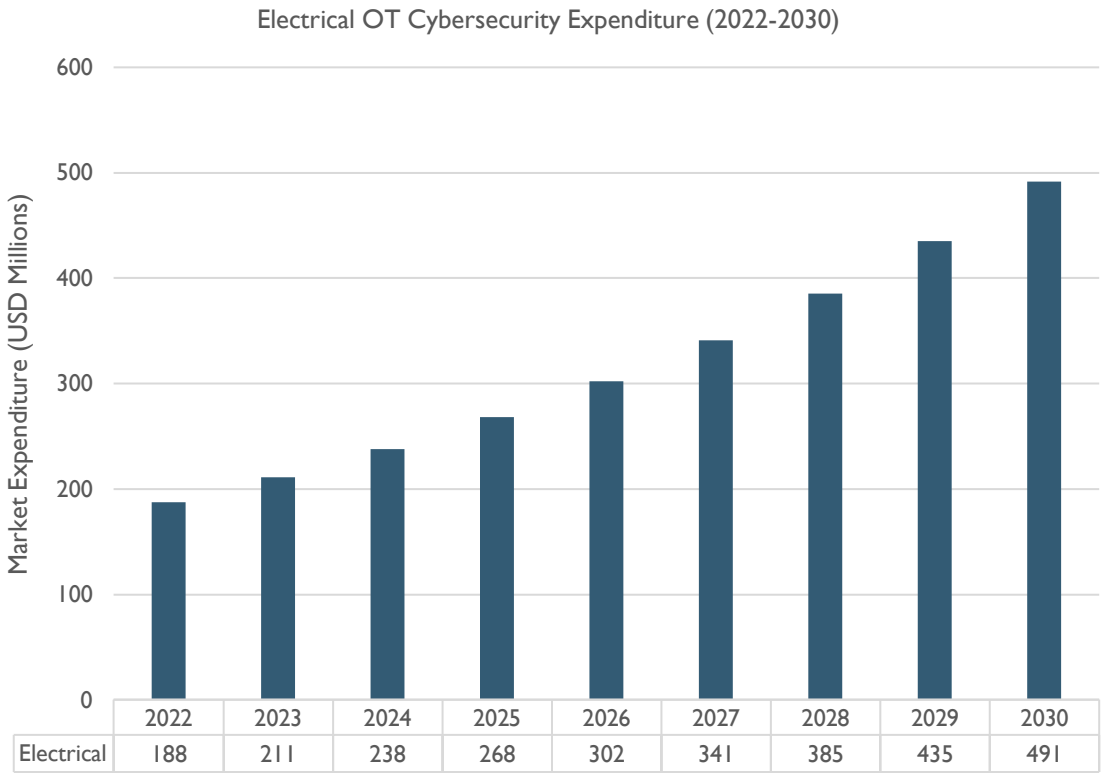
Machinery Manufacturing TAM between 2023-2030 is $5.1B with a CAGR of 13%

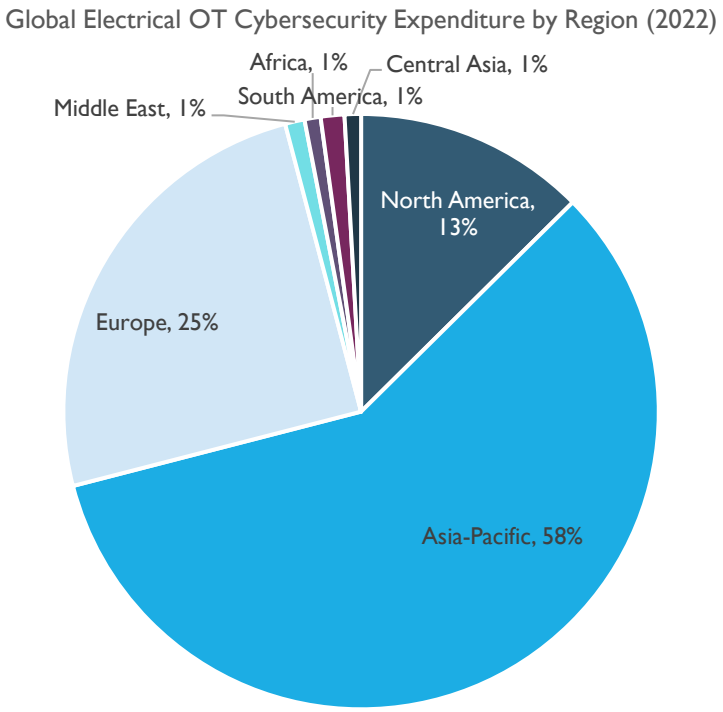




Definition: Manufacturing of machinery that acts independently on materials or performs operations (e.g. handling, spraying, weighing, welding, packaging). Includes fluid power equipment, pumps and compressors, bearings and gears, lifting and handling equipment, machine tools, machinery of mining, earthmoving, food and beverage processing etc.

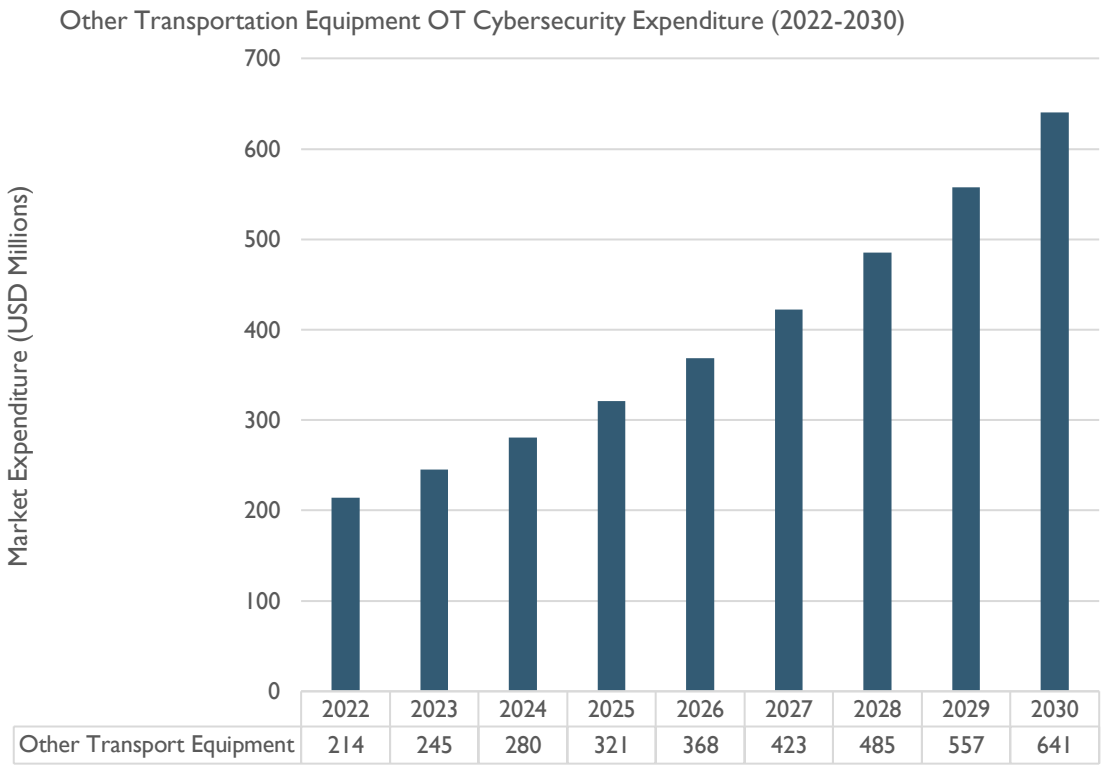
Electrical Manufacturing TAM between 2023-2030 is $2.7B with a CAGR of 13%



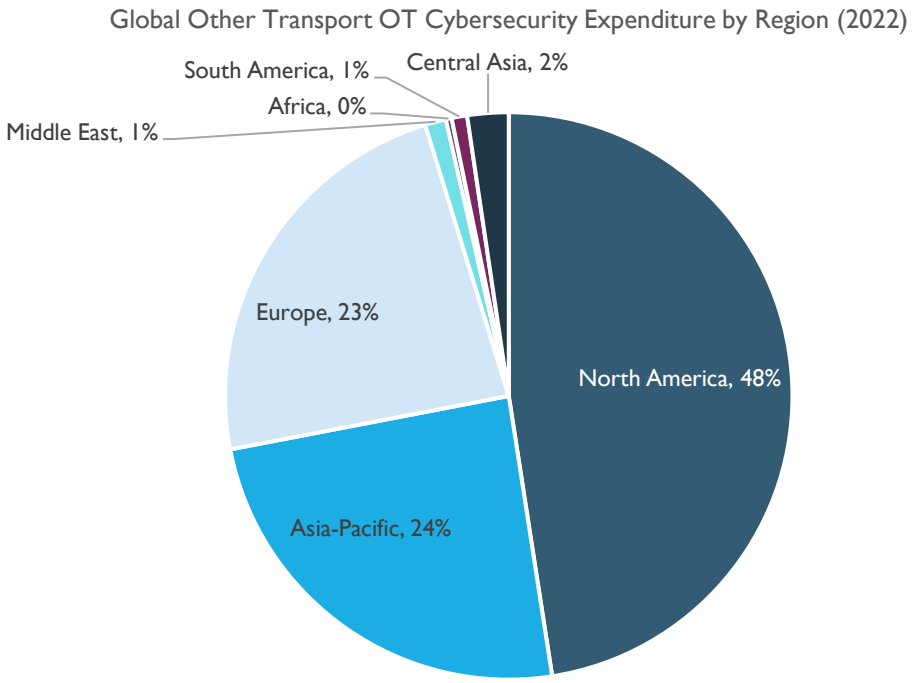


Definition: Products that generate, distribute and use electrical power including motors and generators, electricity distribution and control equipment (e.g. relays, fuses, switching equipment), electric lighting equipment, and consumer appliances.

Other Transport Manufacturing TAM between 2023-2030 is $3.3B with a CAGR of 15%

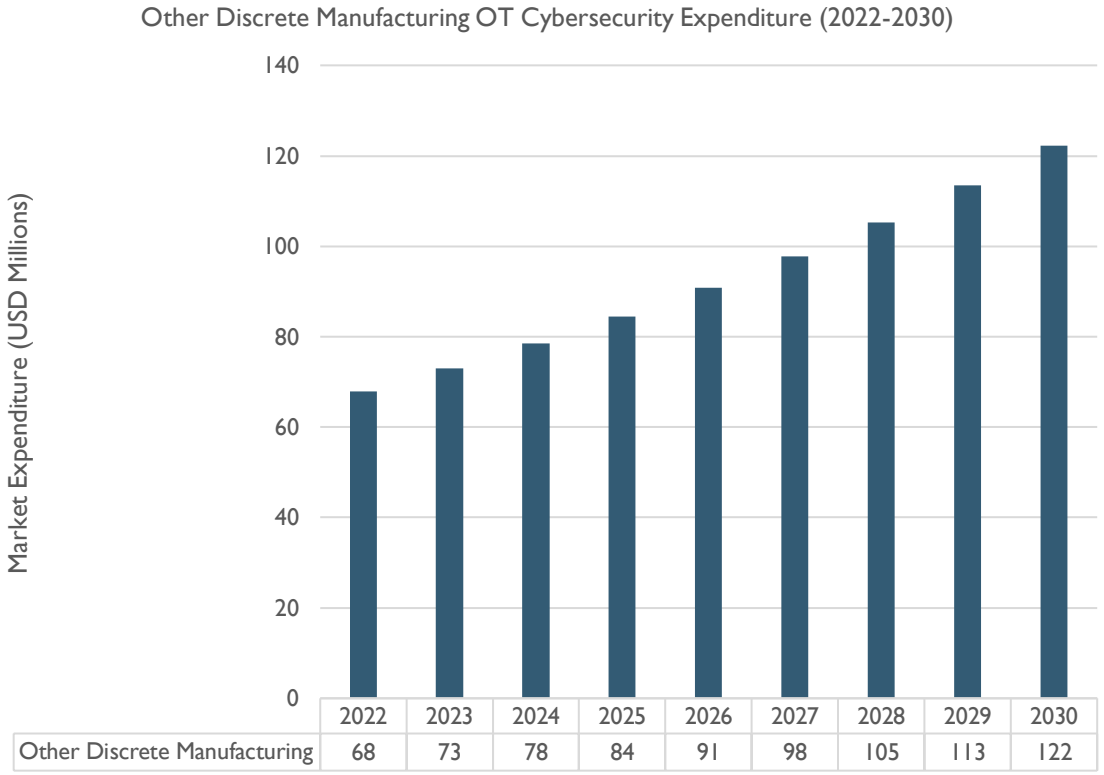


	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other Transport Equipment	214	245	280	321	368	423	485	557	641

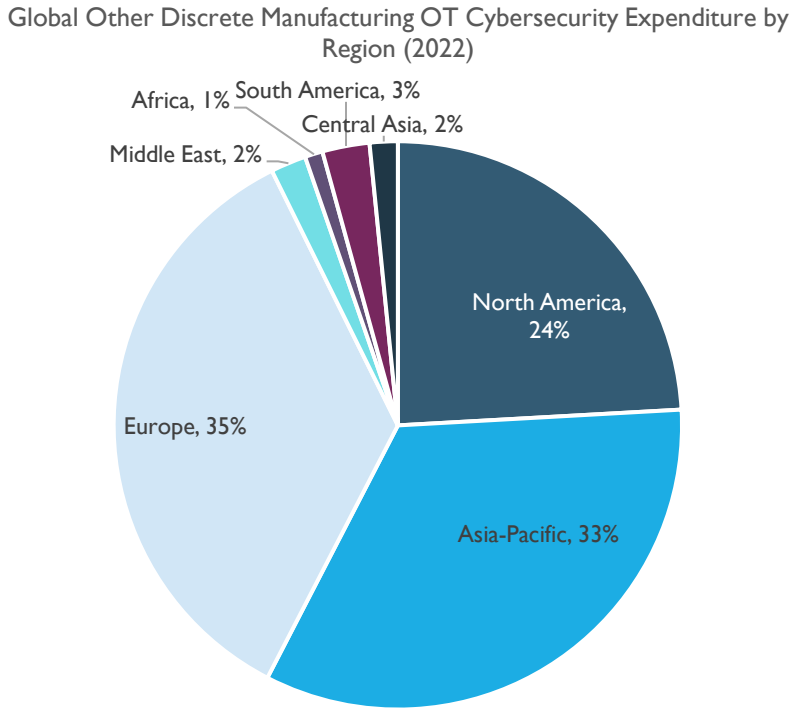


Definition: Manufacturing of ships, aircraft and railway engines, motorcycles and military vehicles.

Other Discrete Manufacturing TAM between 2023-2030 is $766M with a CAGR of 8%



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Other Discrete Manufacturing	68	73	78	84	91	98	105	113	122



Definition: A range of products not covered by other categories including furniture, jewellery, games, toys, sports equipment and musical instruments.

Computing & Electronics production capacity is expected to expand significantly to 2030 through investment in new sites, increasing levels of automation and growing use of AI

2023 Trend	2030 Outlook	2030 Status
Demand is currently high due to a post COVID-19 rebound from various industries including automotive and consumer. UNIDO & OECD reported annual production growth of >5% (2021-2022).		Production is likely to grow faster than many other manufacturing sectors due to the criticality of computing and semiconductors to AI, IoT and 5G.
Semiconductor growth is expected to improve in 2023 following the supply chain issues in 2022 with Taiwan, South Korea leading production. The industry is expected to double in size between 2021 and 2030.*		New investment is likely to shift production away from current production centres, with the US onshoring production (CHIPS for America Act), Chinese investment in growing national capacity and a focus on production in emerging APAC economies.
B2B2C business models means that computing and electronics firms need to **manage the full product lifecycle** from sourcing, to design, production, logistics and Point of Sale, increasing the connectivity through a company wide ERP.		Increasingly integrated supply chains and strategic partnerships including Electronic Contract Manufacturers (ECMs) with pressure to automate and deliver additional value to their customers.
Investment in DX to improve automation and predictability in fab plants, including reduction in scrap, resolving bottlenecks and improving supply chain performance.		Automated, data driven fabrication plants incorporating higher levels of analytics and AI driven largely by new greenfield facilities.
Cybersecurity resilience in the sector is relatively high compared to other manufacturing sectors though their remains a large variance between the largest manufacturers with new plants, and the SME community comprising smaller ECMs and specialist manufacturers.		Cybersecurity maturity in the sector is expected to improve significantly to 2030 due to investment in new plants and a focus on operational resilience. The investment in cybersecurity will be driven in part by growing national regulation and industry specific standards.

Cyber Security Impact and Implications

Cyber risk is high in computing and electronics, especially for those companies with leading IP or supplying advanced electronics to government and militaries. The current supply challenges in the industry means that **availability and reliability of production is a priority** and will result in growing investment in real-time monitoring and predictive maintenance. Ransomware is of high concern as it may result in operational downtime, customer penalties and lost contracts. Loss of confidential data is a further risk and a concern in an industry reliant on contract manufacturing.

Secure by design is an important consideration during the manufacturing process to ensure a root of trust is established for semiconductors and that vulnerabilities are detected at the design stage to prevent incidents in downstream industries.

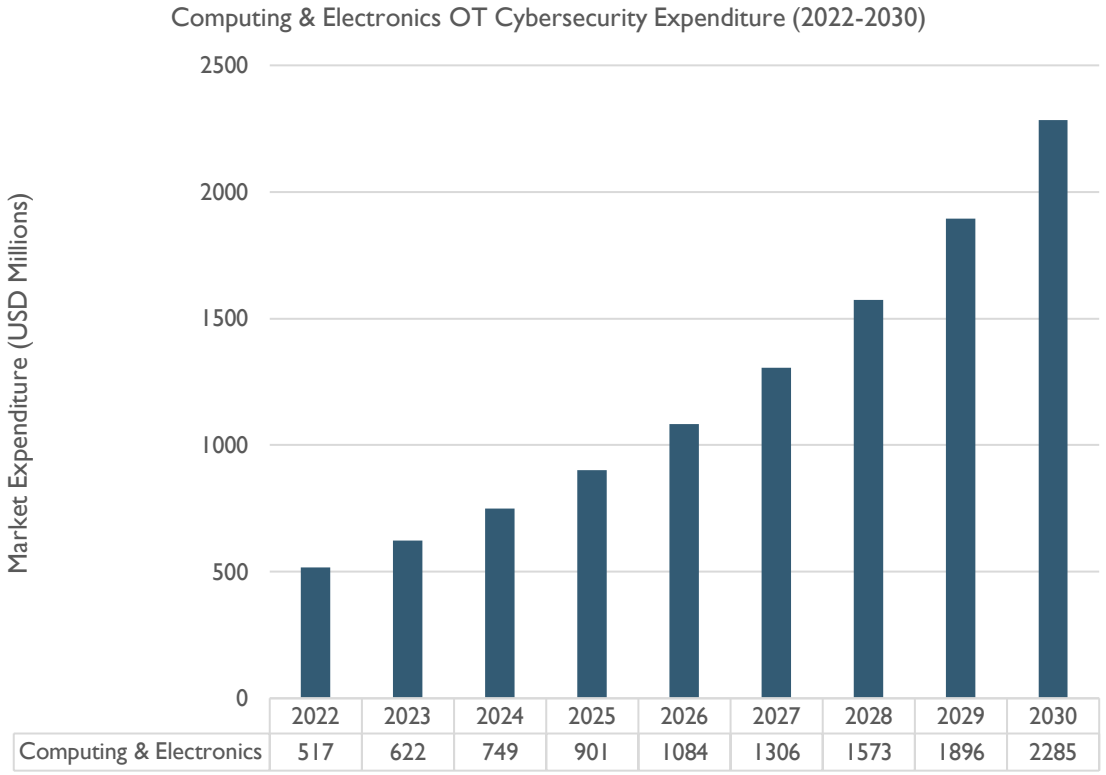
There are a range of standards depending on the product. The IPC standard and its various components is generally used by electronics manufacturers to ensure product quality for PCBs. Computing and Electronics manufacturers will be subject to a range of security standards and regulations depending on their customer mix. For example, Defense related electronics firms in the U.S. are subject to DoD requirements including CMMC and ITAR.

Cybersecurity maturity in the semiconductor manufacturing industry is relatively advanced though there are ongoing challenges related to protection of manufacturing processes. In January **2022 SEMI E187-Specifications for Cybersecurity of Fab Equipment** was launched as a standard for semiconductor operations with a focus on managing end of life OSs, ensuring secure networking, endpoint protection and effective log management and monitoring.

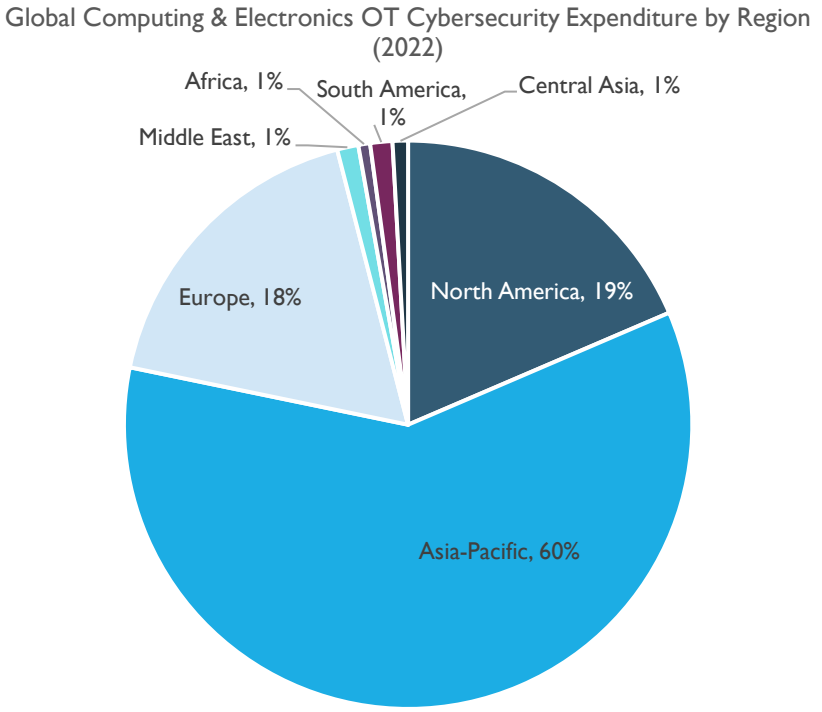
Other regulation and standards related to semiconductors are primarily focussed on ensuring secure-by-design and resilience in the supply chain. Manufacturing security strategy is informed by NIST, **IEC 62443** and **ISO 27000.**

https://www.mckinsey.com/industries/semiconductors/our-insights/the-semiconductor-decade-a-trillion-dollar-industry

Computing & Electronics Manufacturing TAM between 2023-2030 is $10.4B with a CAGR of 20%

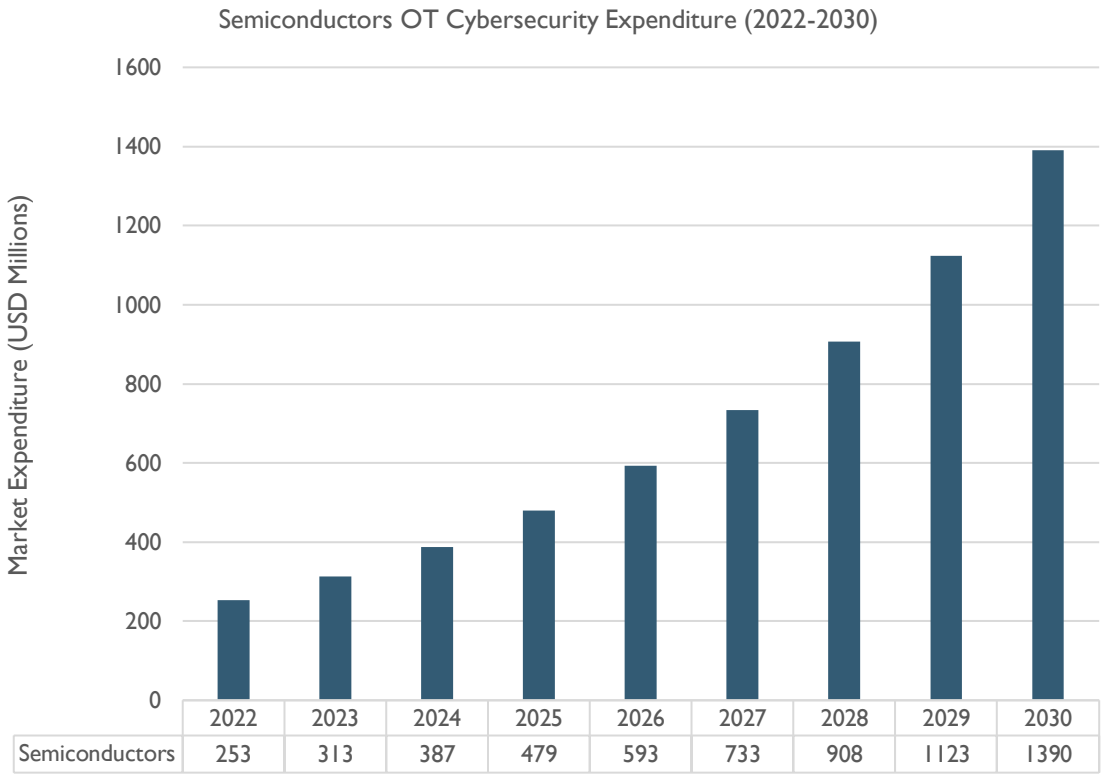


	2022	2023	2024	2025	2026	2027	2028	2029	2030
Computing & Electronics	517	622	749	901	1084	1306	1573	1896	2285

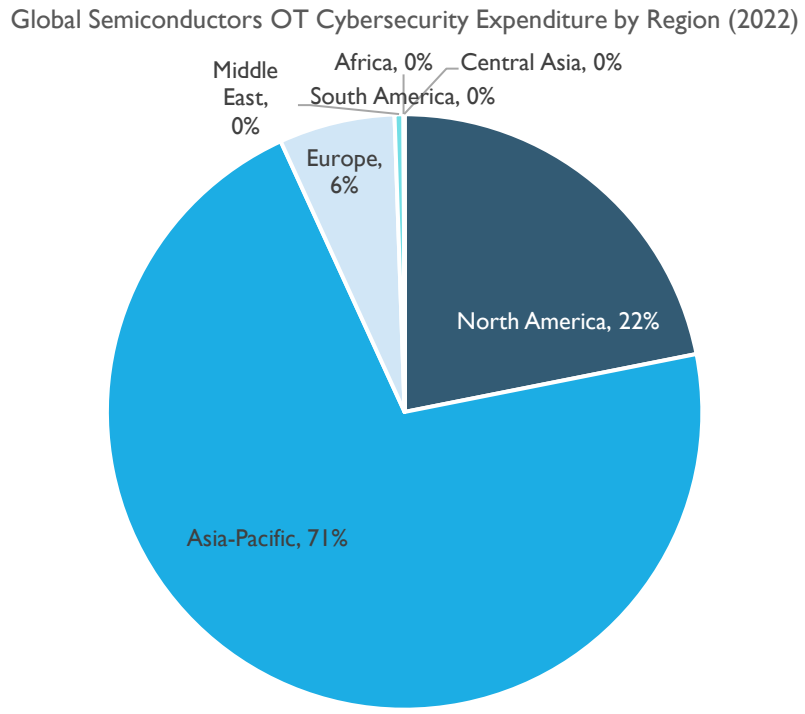


Definition: Manufacture of computers, communications equipment, and optics. Production processes are characterised by the design and use of integrated circuits. Includes electronic components and boards (semiconductors, capacitors, diodes etc), computers and peripheral equipment (e.g. monitors, keyboards, printers etc), communication equipment (e.g. telephones, mobiles, modems, antenna, consumer electronics (e.g. televisions, radios), electronic instrumentation for healthcare (e.g. CT scanners, pacemakers etc), instruments for measuring, testing and navigation.

Semiconductor Manufacturing TAM between 2023-2030 is $5.9B with a CAGR of 24%



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Semiconductors	253	313	387	479	593	733	908	1123	1390

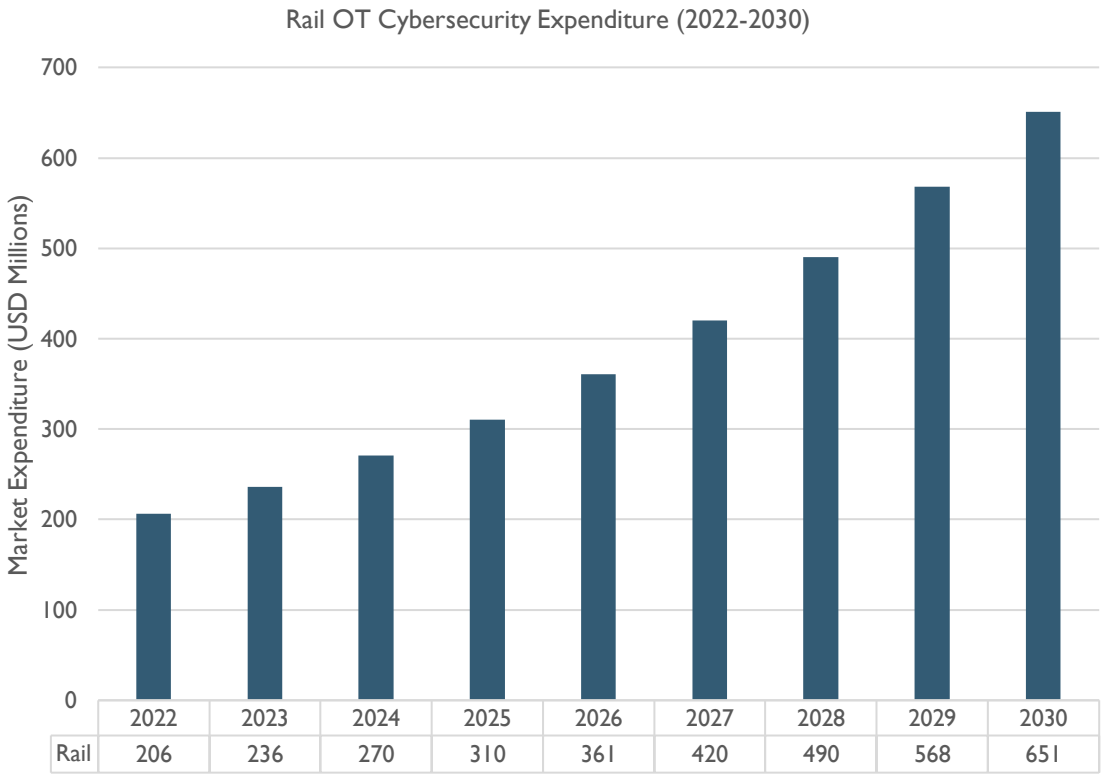


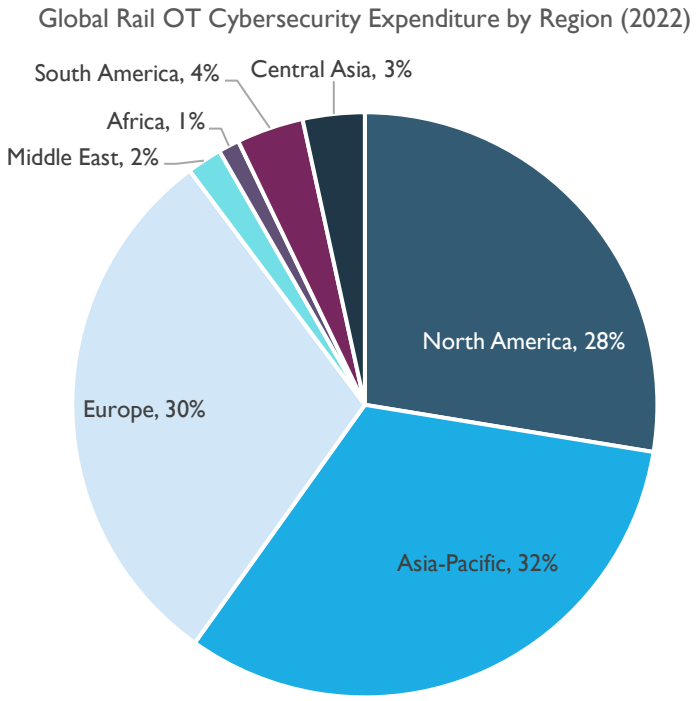
Definition: Manufacture of semiconductors and peripheral equipment.

Rail cybersecurity is heavily based on IEC 62443 standards and will continue to mature to 2030

2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Passenger demand for rail services is stable post pandemic as passengers continue to work from home or have chosen different transport options to travel.		Whilst 2020 led to a decrease in investment and post 2020 rail usage has been lower, most projections point to increasing investment in rail infrastructure and rolling stock as part of national decarbonisation strategies.	New infrastructure will focus on improving on-time performance and passenger services, requiring secure communication systems for V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communication and passenger connectivity. Most investment will be in Asia and Europe. New digital infrastructure will be built with a Defence in Depth mindset whilst "brownfield" installations will require improved perimeter protection leading to different levels of cyber maturity. Increasing reliance on digital infrastructure for trains and networks will lead to increasing NOC/ SOC integration. Maintaining safety performance is paramount to rail operators. Safety can't be compromised through improvements to security and therefore requires a joint approach to safety and security. In-depth knowledge of RAMS (Reliability, Availability, Maintainability and Safety) in rail operations with an understanding of the relationship with security is an important go to market consideration. The cyber security risk needs to be communicated as part of the safety story. A growing Defence in Depth mindset is based on IEC 62443, Security Level 3, including data (rail signals, rail commands, keys and secure communications), applications (authentication, secure software methodology) platforms (host firewall, access control, patch management and monitoring) internal network (security zones, firewall, internal DMZ, AAA) perimeter security (DMZ, firewalls, ACL, VPN, IPS/IDS, AAA) physical security (guards, locks, cabinets, access control), and procedures. Other standards include ISO 27001,27002 and 27005 and in Europe CLC/TS 50701 which applies 62443 to the railway sector.
Public and Private ownership models operate differently across countries. Most networks across Europe and Asia are controlled or heavily regulated by Government bodies.		No expected changes to the status quo.	
Increasing digitalisation of rail networks through ERTMS (EU Rail Train Management System), ATO (Automatic Train Operation), Traffic Management, Intelligent Infrastructure and RCM (Remote Condition Monitoring).		Widespread use of cloud analytics to improve real time operations, 5G network deployments, and introduction of driverless train systems.	
Rail networks are complex and mainly siloed - threats to OT include signalling systems (remote monitoring, juridical recorder, interlocking and automatic train protection), command & control (automatic train control, energy traction, docking) and other onboard systems.		Growing interconnectivity between systems and rail networks will expand the attack surface. There will continue to be a high level of risk as the sector goes through a cycle of modernisation. However, an increasing percentage of the signalling systems and rolling stock will be secure-by-design.	
Cyber security maturity is low though awareness is increasing as digital investment increases. Implementation of the NIS directive is patchy across European countries and availability of skills is a key issue. R-C2M2 model is used to assess levels of maturity across the industry.		NIS2 in Europe will strengthen regulation of rail networks and with plans for a single European railway area (SERA), there will be increasingly interoperability of the rail network and standardisation of cybersecurity. Regulation is expected to strengthen globally.	

Rail TAM between 2023-2030 is $3.3B with a CAGR of 15%





Definition: Operational Technology, for example signalling systems, level crossings, and Train Control & Management Systems, used to transport passengers via rail including freight transportation. Includes suburban passenger transportation including metros and tramway.

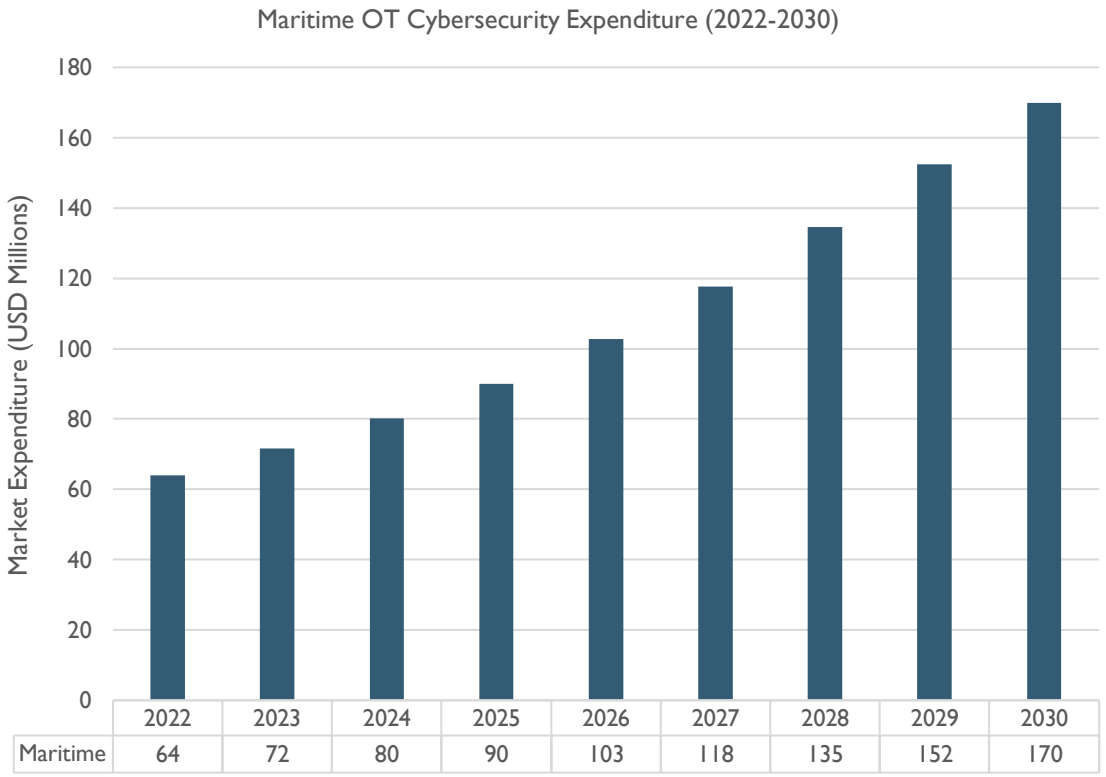
Ports & Maritime cybersecurity maturity will continue to improve as shipping and port operators focus on resilience and shipyards implement secure-by-design

WESTLANDS ADVISORY

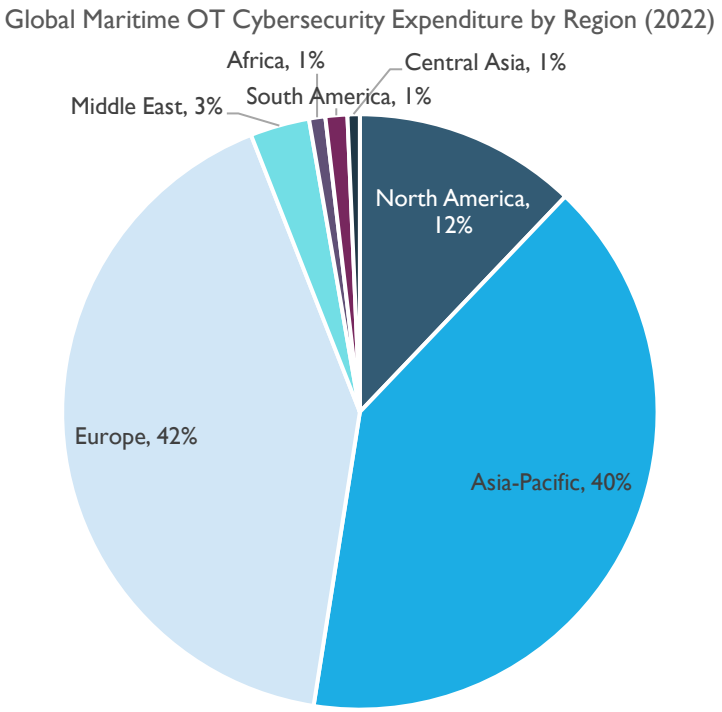
2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Maritime trade volumes have been erratic between 2020 and 2022 due to COVID-19, inflation and supply chain issues. **Annual growth is expected to stabilise in 2023 at 2% p.a.** to 2025.*		Currently **APAC is the largest trade region** and will remain so, accounting for 42% of goods loaded and 64% of goods unloaded in 2021, and is likely to grow its market share further.	Maritime is slowly digitalising as legacy systems reach end of life and are replaced. The business driver is efficiency and lower cost and this has led to increasing automation to decrease crew sizes and the cost of logistics processes. Digitalisation of processes from ship to shore, via SATCOM and broadband satellite communications, has increased connectivity across the shipping supply chain. Innovation and Centres of Excellence tend to be located in Asia. Singapore is often viewed as the innovation driver and has invested significantly in cybersecurity projects including testbeds to evaluate vulnerabilities and risk management. Key research programs include Sustainable Maritime Environment and Energy, Next Generation Ports, Maritime Safety & Security, Smart Fleet Operations and Maritime Traffic Management. All of these themes are linked through a greater need for digitalisation and secure connectivity. Cybersecurity is a thread that runs through these initiatives and is one of eight key areas of development to enable transformation. OT system security can be complex due to the number of different OT systems onboard, and varying configurations and architectures. Depending on the vessel this can include power generation systems, water treatment, HVAC, automated safety controls and cargo management systems. At Ports, OT cybersecurity includes cargo handling systems and warehouse automation. IMO recommendations are aligned to NIST and specify that relevant onboard systems should be considered. Protection and detection tasks includes network monitoring, network intrusion detection, network segmentation, vulnerability management and a defence in depth approach to cybersecurity. Apart from IMO guidance on best practices, maritime organisations also consult with Navigation and Vessel Inspection Circular 05-17, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA), which is based on NIS, and Regulation 19 of SOLAS regarding AIS and GMDSS.
Digitalisation of maritime operations is growing including the use of data analytics and automation. Trends related to improved situational awareness, just in time delivery, improved efficiency and predictive maintenance have driven investment.		Increased use of **broadband communications, data analytics and IoT**. A trend towards detection, identification, classification and tracking of maritime assets helping to streamline cross border processes.	
Emissions remains a significant maritime challenge, currently generating 2.5% of the global greenhouse emissions and predicted to increase further due to ageing fleets.*		The IMO has set a target **to cut emissions by 50% by 2050**. Plans to reach this goal include the adoption of 'Fastrigs', meteorological & satellite systems as well as AI in ship systems. EU has adopted proposals to cut emissions by 55% by 2030.	
Maritime consolidation has resulted in a lower number of shipping operators with the top 20 operators now controlling over 90% of the market. This has been acknowledged as one of the factors behind **high freight costs in 2022 and record profits**.		Higher profitability may lead **to increased investment in infrastructure**. UNCTAD notes the need to improve port infrastructure and to upgrade fleets to reduce carbon emissions. WA expects modernisation to be slow.	
Cyber Security Regulation is evolving. IMO guidance on cyber risk comes into effect on Jan 2021 (Resolution MSC.428(98). The ICS produces a guide to cyber security onboard ships** NIST and ISO 27001 are cited as reference documents.		**Further regulation is expected**. IASC Unified Requirements (UR) E26 and E2, based on IEC 62443, requires shipyards to adopt secure-by-design principles. Adoption is mandatory from January 2024.	

*UNCTAD

Ports & Maritime TAM between 2023-2030 is $919M with a CAGR of 13%



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Maritime	64	72	80	90	103	118	135	152	170



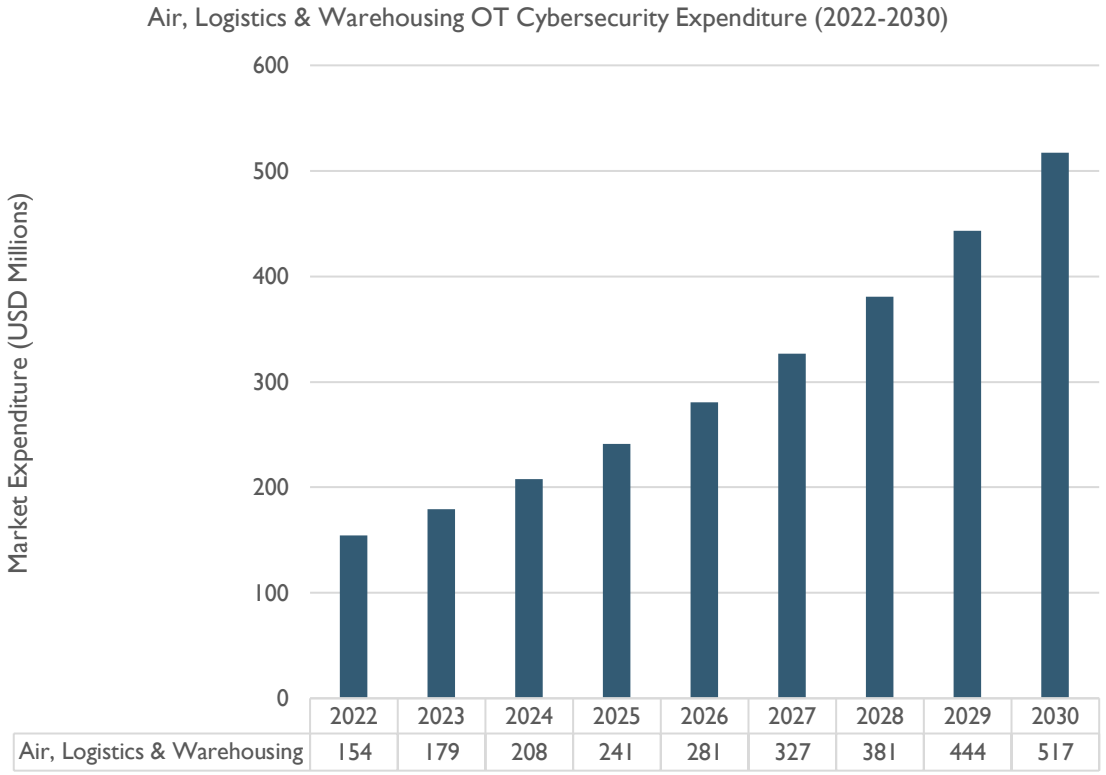
Definition: Operational Technology, for example propulsion systems and material handling, used in maritime operations including transportation of passengers and freight, and port operations.

Air Transportation & Logistics industries will grow steadily to 2030; cybersecurity maturity is expected to improve but will be inconsistently applied across complex distribution networks

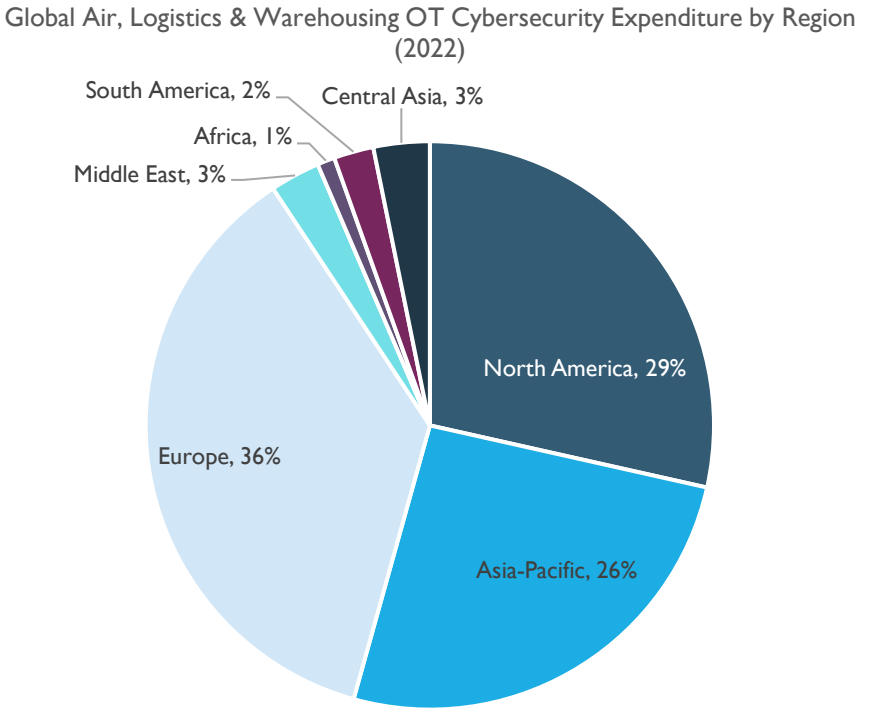
2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Air traffic has recovered and both cargo and passenger flights are likely to be higher than pre-pandemic levels by the end of the year.*		**Passenger flights will grow at 3.6% p.a.** to 2041 whilst freight delivered by air will also increase by 3.2% p.a.** Growth is expected between all regions with highest CAGR domestic flights in India and Emerging Asia and all regions to and from China.	The growth in consumerism, online shopping services, new business models based around Just in Time (JIT) delivery and Last mile delivery, has led to the growth of Distribution Cities. These cities compete for customers on location (proximity to customers), infrastructure (ports, roads), space for warehousing and taxes and incentives. The decentralized distribution model has resulted in cities across Asia developing logistics clusters with a network of closely located warehouses and cold stores to ship goods nationally. The transportation and logistics industry consists of a network of connected and distributed companies, systems and processes. The OT security challenge encompasses transportation systems (rail signalling, port operations, marine systems), and warehousing that includes material handling solutions, robotics, micro-fulfilment, and automated guided vehicles. The business objective of transportation and logistics operators are similar irrespective of the role of the company in the network – getting a person or object from point A to B on time and profitability. An interruption to operations from an cyber incident may lead to delays, customer dissatisfaction and possible financial penalties. It may also compromise passenger and staff safety. The threat is principally from ransomware and cybersecurity best practices include clear segmentation between IT and OT networks, asset visibility across distributed networks, and the adoption of zero trust principles including remote access to OT systems.
Airport investment is set to increase in 2023 to meet future demand requirements. This includes both DX of existing operations and CAPEX to support new terminals and infrastructure.		ACI estimates **$2.4 trillion will be needed to address long term passenger and cargo demand to 2041**** and over half will be in APAC. This will include integrated transportation systems, terminal buildings and other facilities.	
Growing use of 3PL providers requires warehouse infrastructure from airports and other major distribution centres and at strategic points, including cold stores and warehousing.		**Larger and more integrated networks of warehousing** to facilitate higher demand for just in time delivery.	
Growing digitalisation across air transportation and logistics. Airport DX investment was growing pre-pandemic with a focus on passenger automation and IoT concepts.		**Increasing levels of automation** including the use of robots and pick to light systems to improve warehouse automation and efficiency. At airports increasing integration of passenger systems (including bagging handling) and aircraft operations which includes a range of systems dependent on OT.	
Cybersecurity maturity is improving. However, the fragmented nature of the logistics industry, which includes multiple asset owners, means that gaps exist across the logistics chain.		**Regulation is expected to lead to improved** cybersecurity as airports and vital parts of 3PL – including maritime and rail – will be covered by regulation focussed on the protection of critical assets.	

*ICAO
**Airbus
***ACI

Air Transportation & Logistics TAM between 2023-2030 is $2.6B with a CAGR of 16%



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Air, Logistics & Warehousing	154	179	208	241	281	327	381	444	517



Definition: Operational Technology to facilitate the transportation of passengers and freight by air (e.g. baggage handling systems) and warehousing and storage of goods (e.g. warehouse automation, cold stores etc.)

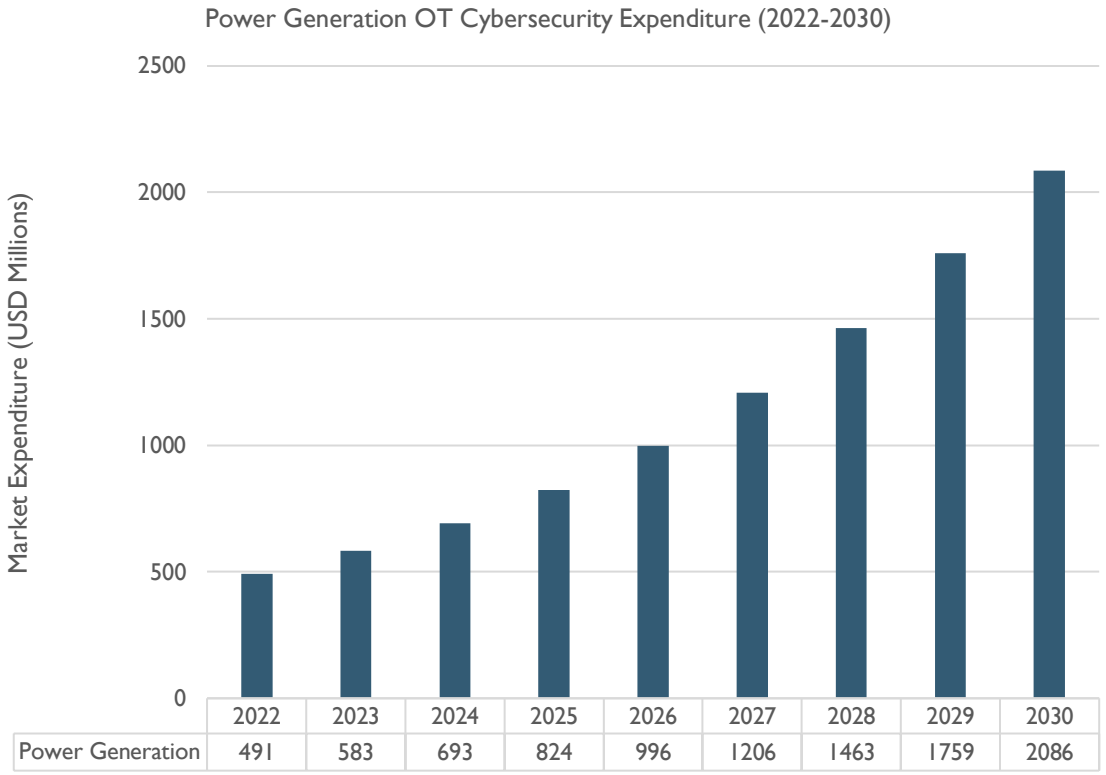
Power Generation & Energy Transmission and Distribution infrastructure continue to shift to using renewable energy sources and smart grids to deliver lower carbon emissions

WESTLANDS ADVISORY

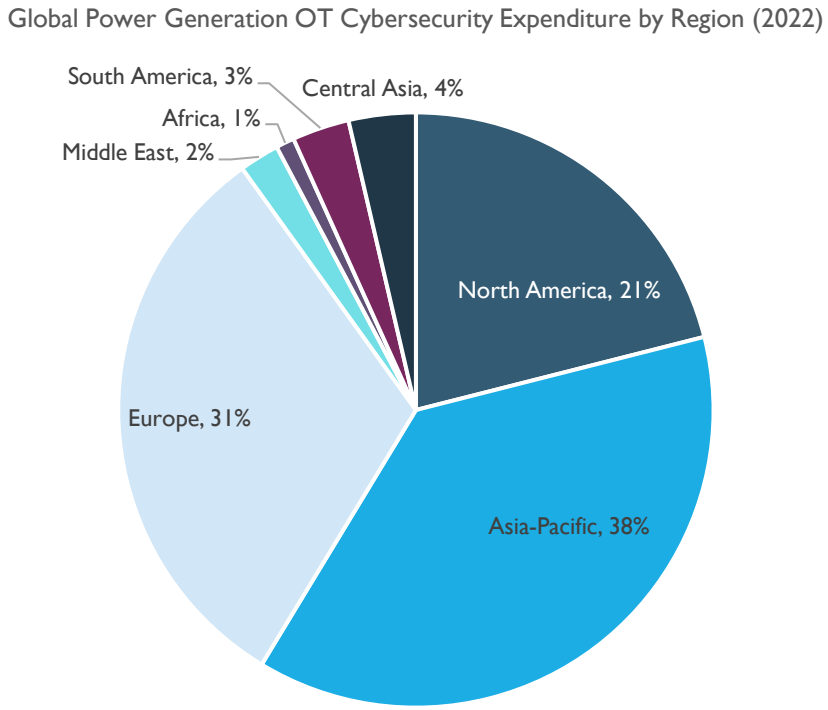
2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Energy generation will increase in 2023 and has grown since the COVID-19 lockdowns in 2020. China is the largest producer of power followed by the US and India.		**Future energy demand will be mostly met by electrification** (e.g. wind) rather than fossil fuelled power generation which will remain largely stable to 2035** before reducing.	The increasing digitalisation of energy networks makes them more vulnerable to cyber attacks. This has resulted in standards and regulation to ensure safety and reliability. The primary guiding policy in Europe is the Network and Information System (NIS) directive whilst in the US NERC is widely adopted and followed. However, compliance is patchy across the EU with enforcement dependent on each national regulator. NIS2 will have a greater impact in the EU. Localised policy is also relevant, especially related to national sovereignty (for example in Sweden data must reside within country) whilst the German security act requires energy producers, and suppliers of critical hardware, to implement threat detection in IT and OT environments. The increasing regulatory focus on Energy in Europe provides a guide for the general direction of travel across all advanced and high growth economies. The growth of the smart grid and interconnection between energy and transportation networks (electric charging, smart homes) creates still as yet unknown security challenges and vulnerabilities that are likely to increase risks across the transmission and distribution networks. This has resulted in significant investment in test beds to understand the causal effects between infrastructure. However, at a practical level, Westlands Advisory expects tightening regulation, growing digitalisation and use of the cloud, to result in a renewed focus on cybersecurity maturity related to Operational Technology. NERC CIP is the gold standard in the US and is widely followed outside of the region. Compliance with NERC, which sets out the required security controls, is widely tracked by utilities. Westlands Advisory expects organisations to invest in tools that provides greater visibility of assets and threats across the DMZ including EDR, NDR, and greater use of threat intelligence and hunting. NIS2 will have a greater impact on cybersecurity maturity in the European Union.
Fossil fuels accounts for the majority of the energy mix **though renewables now make up 13% of total power generation**.***		Various scenarios exist for the energy mix by 2030 but all point to a **greater proportion of power generation being delivered by renewables**, principally Wind and Solar with significant programs in both the US and China.	
Digitalisation of plants to continue to improve operational performance, safety, maintainability and energy efficiency.		New plants and renewables will be added by 2030, but the current installed base will be responsible for the majority of the capacity. These **plants will be refurbished and modernised** over their lifetime with a focus on efficiency, availability and safety.	
Smart grid investment continues to grow in NA, Europe and China but dropped in 2021 in emerging markets. According to the IEA the level of digital investment in grid infrastructure increased from 12% in 2015 to 19% in 2021.		Investment is expected to continue to grow as the US modernises its network, Europe connects renewables and China installs HV networks and digitalises the grid. **Smart Meters and Automation & Management Systems are the largest expenditure categories.**	
Electrification of transportation requires a large ecosystem of automotive vendors, logistics companies, cities and utilities to collaborate, plan and manage transportation infrastructure and business models.		By 2030 the use of electric cars will have increased considerably. Fleets and drones will become increasingly important as autonomous, electric delivery models emerge with 5G infrastructure. **EV infrastructure will be the fastest growing smart grid investment category to 2030.**	

*IEA data
**McKinsey
***BP Energy Outlook

Power Generation TAM between 2023-2030 is $9.6B with a CAGR of 20%

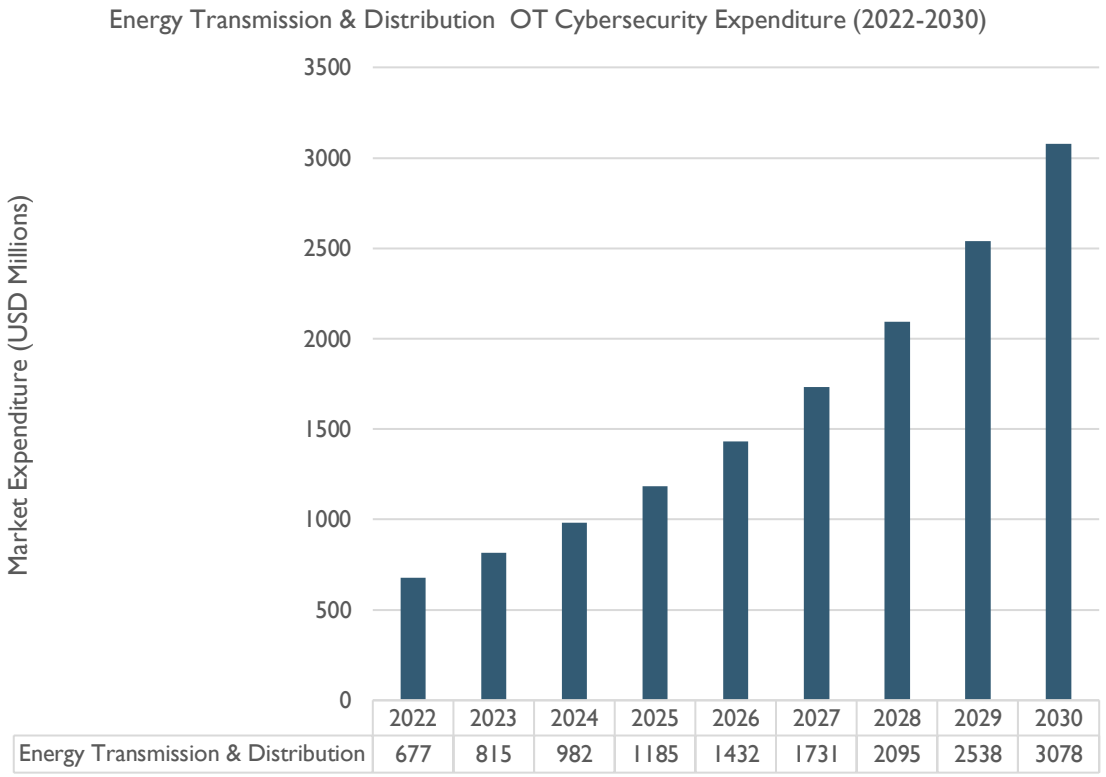


	2022	2023	2024	2025	2026	2027	2028	2029	2030
Power Generation	491	583	693	824	996	1206	1463	1759	2086

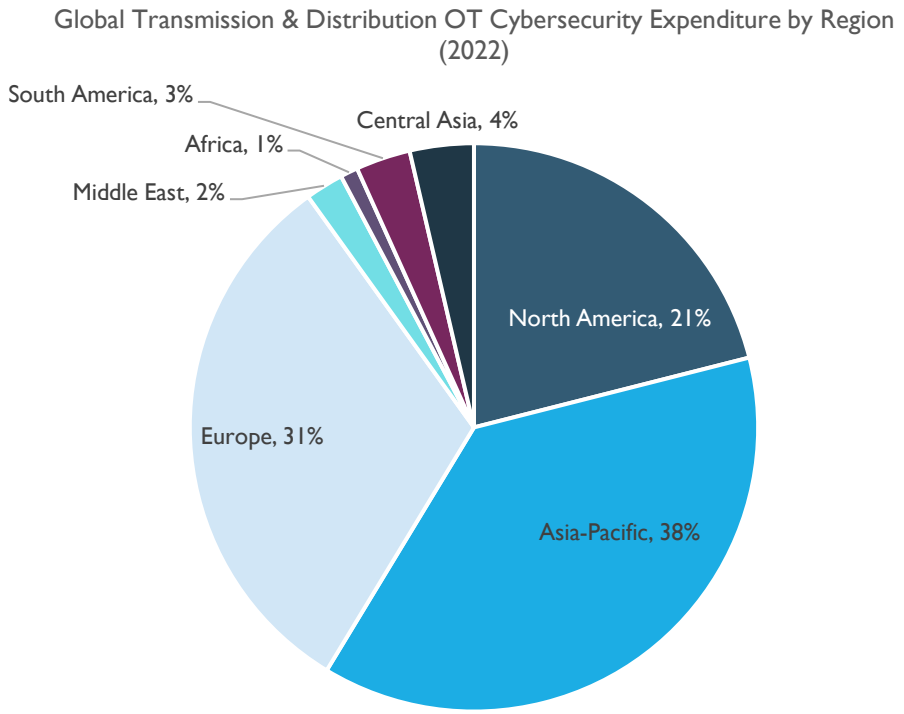


Definition: Production of energy including nuclear, coal, gas and renewable plants.

Energy Transmission & Distribution TAM between 2023-2030 is $13.9B with a CAGR of 21%



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Energy Transmission & Distribution	677	815	982	1185	1432	1731	2095	2538	3078



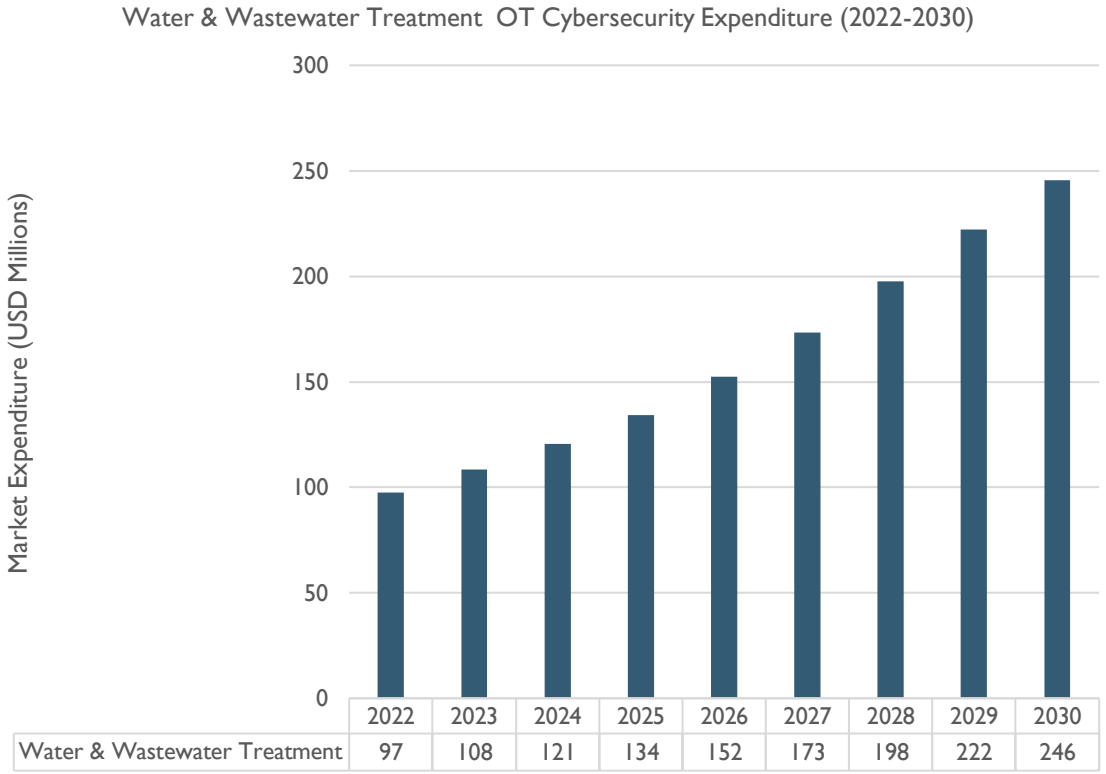
Definition: Transmission and Distribution of electrical energy through the grid and mains gas supply.

Water & Wastewater infrastructure investment remains low but increasing digital investment and regulation will result in improving cybersecurity maturity

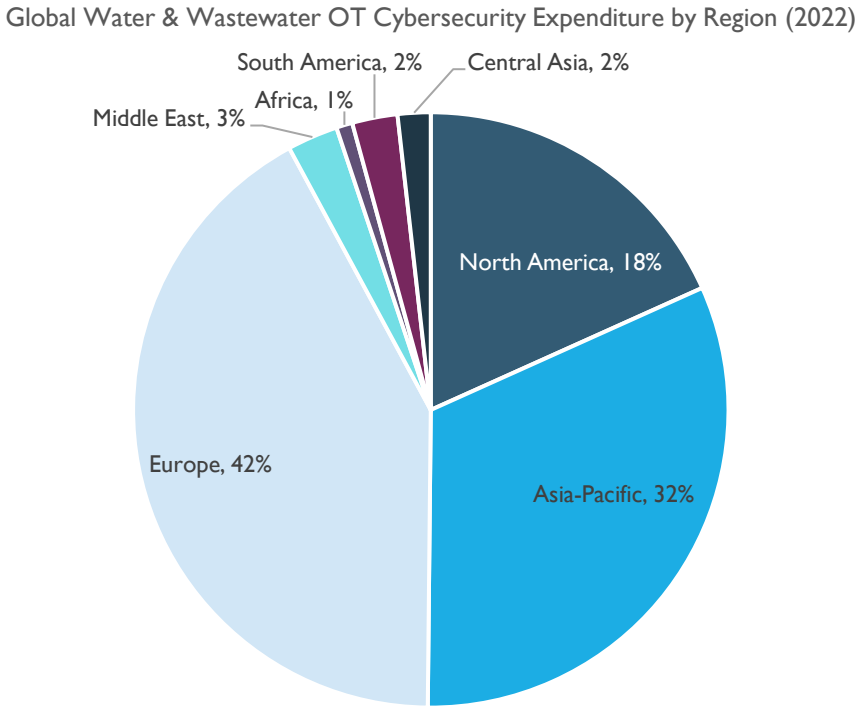
2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Water Demand has been growing at 1% per year for the last 40 years.		Population growth and other socio-economic factors will result in a 1% annual increase in water consumption to 2050 according to UNESCO.	Although investment in water and wastewater infrastructure is significant, the distributed nature of water plants and limited budgets has resulted in low levels of investment. This does change by region. Privatisation in Europe has led to large water groups with more resource and centralised procurement programs. However, in the US for example, there is a high level of fragmentation with over 50,000 water utilities with limited resource and skill sets. Water infrastructure is critical national infrastructure. The attackers incentive is unlikely to be financial and ransomware has become more prevalent. The combination of low resource, limited cybersecurity skills, and highly distributed and increasingly connected infrastructure contributes to a high level of risk. The US WSCC and WaterISAC highlighted the risk in a report in 2021 which surveyed 600 US water utilities. In the survey only 30% had identified their OT networked assets, 57% had a cyber risk management plan and nearly 40% spent under 1% of their budget on security. There was a strong correlation between utility size and OT Cyber maturity– the larger the utility, the more likely they were to spend on cyber, conduct risk assessments and know their assets. The scenario in the US contrasts strongly with some European case studies where there is more consolidation and managed security services include threat intelligence, hunting and incident response. Extending these services to OT is a growing theme as water networks become more reliant on data analytics and automation. Cybersecurity standards and best practices are generally issued by national regulatory bodies and includes alerts from industry ISAC's on existing and new vulnerabilities. NIST SP 800-82 is widely quoted. In Europe NIS2 regulation will apply.
Infrastructure in need of investment to meet future requirements. 26% of the world's population do not have access to safe managed drinking water whilst 40% of water bodies do not provide 'safe' water.		Progress against the UN's SDG 6 targets – safe drinking water for all – has been slow. Whilst global water efficiency is increasing (particularly in the industrial sector), the rate of progress on IWRM is lagging.	
Levels of digitalisation are steadily increasing globally through the use of IoT, analytics and digital twins for predictive maintenance and water efficiency.		Higher levels of connectivity using sensors and AI to predict water demand and automate management of the water network in developed economies.	
Development of digital water standards and legislation. European commission identified the water industry as having low-level cyber maturity. The main action globally will be to introduce standards towards large-scale pilots and to expand the market uptake of technologies.		EU commission recognised this digital shift in the industry and the lack of specific regulatory standards. Current action plan to develop upon ICT4Water standards in place towards 2030.	
Cyber Risk. The Oldsmar, Florida water treatment plant cybersecurity incident highlighted the vulnerabilities and consequences of a cyber security incident on water treatment facilities. Whether user error or an attack, the example highlights the importance of monitoring and control at plants.		Regulation is likely to result in improved cybersecurity maturity. NIS2 covers the water and wastewater treatment sector in the EU, the US EPA released a new memorandum in March 2023 to enforce inspection of PWS (Public Water Systems), and the Australia SLACIP act are examples.	

IWRM – Integrated Water Resources Management

Water Utilities TAM between 2023-2030 is $1.4B with a CAGR of 12%



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Water & Wastewater Treatment	97	108	121	134	152	173	198	222	246



Definition: Water collection, treatment and supply including sewerage treatment.

Oil & Gas industry profitability is currently high though large CAPEX is not expected in 2023 but is likely to increase to 2030 to facilitate demand for LNG and energy security

2023 Trend	2030 Outlook	2030 Status
Oil & Gas production increased slightly in 2022 and will be followed by a further moderate increase in 2023. However, high crude oil prices for Brent, OPEC Basket and WTI, resulted in in **record oil company profits in 2022/3.**		Oil & Gas prices have dropped in Q1 2023 but remain relatively high at $80 per barrel. Longer term forecasts suggest that average prices will be between **$70-$80 per barrel to 2027 which will sustain high profit levels.**
No significant changes to Oil & Gas CAPEX in 2023/4. Higher profits may not necessarily lead to new exploration or production in the short term as NOC's and IOC's focus on short term shareholder value.		**Investment is likely to increase over the period to 2030** in areas such as certified natural gas and carbon neutral LNG as countries look to balance the energy trilemma of security, affordability and sustainability.
"Digital oil fields" and pipelines to improve operational efficiency. Digital investment to reduce cost through automation, integrated asset management and real-time surveillance of production and supply. Reducing inefficiencies and costs.		Increasing digitalisation characterised by remote monitoring and asset management, predictive maintenance through low cost sensors, IoT devices, M2M, cloud deployment and data analytics.
Net refinery capacity will increase significantly in 2023 mainly East of Suez due to new plants in Middle East, China and India. Capacity in the Atlantic Basin has declined since 2021 though there is net expansion in Africa.*		Refining capacity is expected to continue to increase East of Suez whilst the trend in NA and Europe has been to **convert refineries to biofuels production**. Demand for future refinery capacity will be linked to the rate of EV adoption.
Cyber maturity is improving especially amongst the large IOC's as cyber is now acknowledged as a significant risk. However, this does not necessarily filter down to the operational level or across the supply chain. Improvement needed as digitisation expands and cyber threat increases.		Cyber information sharing through ISACs, security by design for new systems and increasing compliance with regulation is likely to improve cyber maturity. However, change will be evolutionary rather than revolutionary. Standards include ONG-C2M2, ISO 27001, IEC 62443, API Standard 1164 and NIST.

Cyber Security Impact and Implications

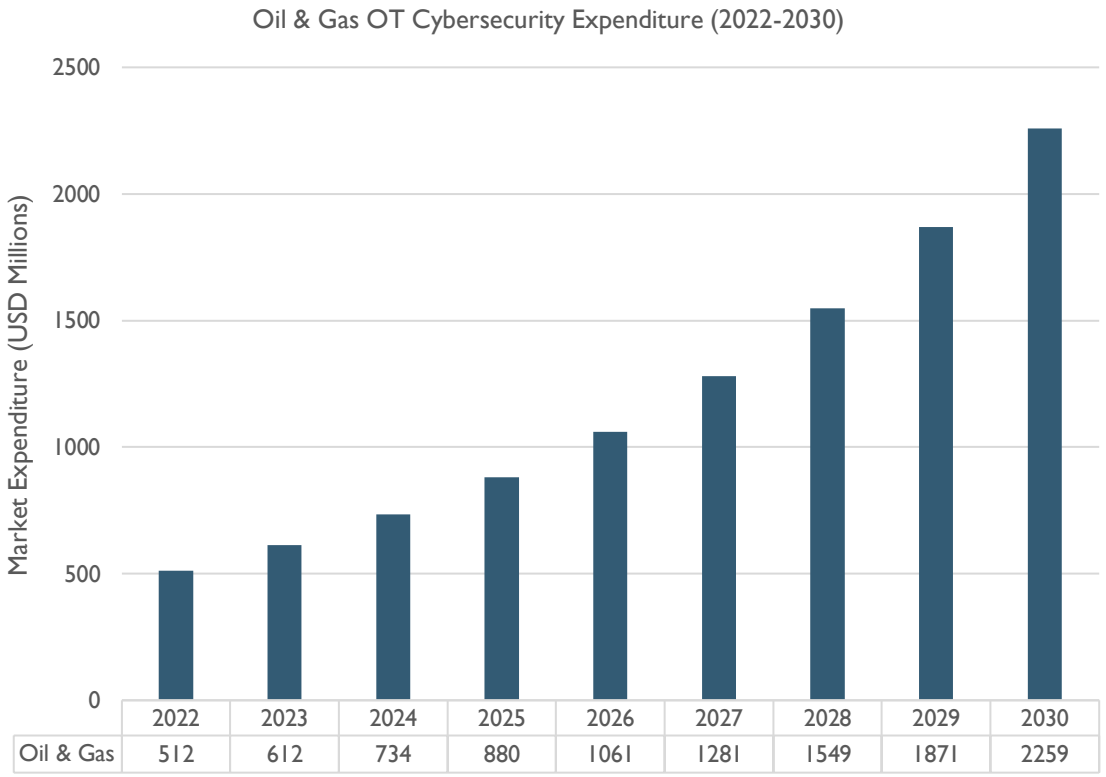
Oil & Gas upstream and midstream operations differ significantly in terms of processes, business models and technologies. However both operations are often seen as national critical infrastructure and highly targeted. The Colonial Pipeline attack in May 2021 is an example of both the vulnerabilities that exist and the impact of an attack. The ransomware attack was executed through accessing the network through using compromised credentials linked to a VPN account, providing remote access to the network. The attackers exfiltrated around 100 gigabytes of data and encrypted the payment systems, impacting business operations. This was not an attack on OT, but resulted in operations being shutdown to prevent further damage. It provided an insight into the scale of a successful attack on OT, resulting in pipeline operations ceasing for 6 days and dramatic scenes of fuel shortages on the US East Coast.

The case of Colonial accelerated regulatory oversight in the US, moving from voluntary measures in the Pipeline Cybersecurity Initiative in 2018 to a series of directives. Westlands Advisory expects the Oil & Gas industry globally to re-evaluate its cyber security strategy to ensure it is fit for purpose. This includes performing regular risk assessments, implementing and maintaining appropriate governance structures, policies and procedures, and incident response plans. The focus is on developing resilience – improving an organisations ability to recover quickly from an event.

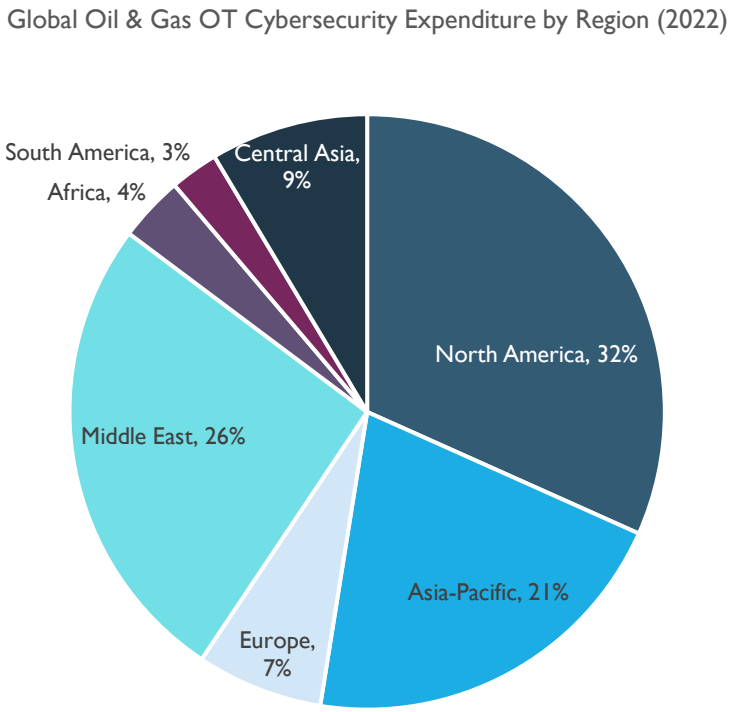
Technology requirements map to NIST and includes asset discovery, network segmentation, compliance monitoring, threat monitoring and the development of playbooks and business continuity planning. Oil & Gas has a higher requirement for mobile threat defence and secure remote access management due to reliance on mobile devices for remote diagnostics and monitoring. Other cyber challenges to O&G includes the use and reliance on standard IT products with known vulnerabilities, data networks between on-shore and offshore facilities, and legacy control systems (DNV research).

*IEA data
IOC (International Oil Company)
NOC (National Oil Company)

Oil & Gas TAM between 2023-2030 is $10.2B with a CAGR of 20%

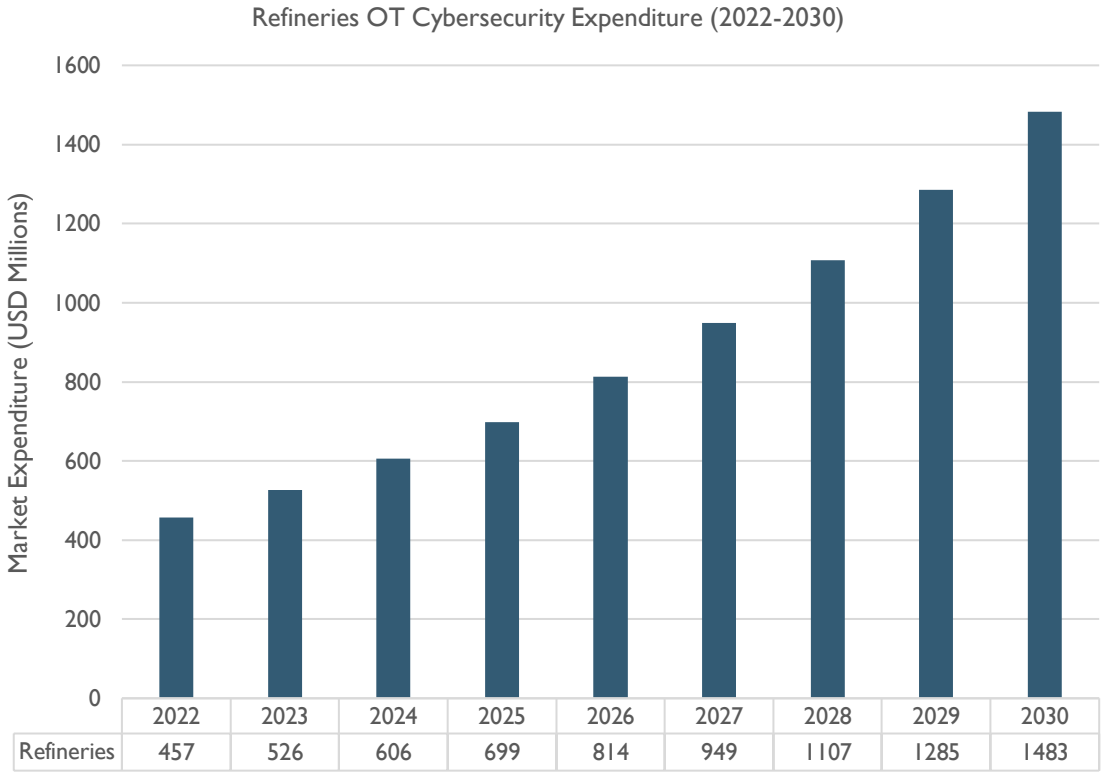


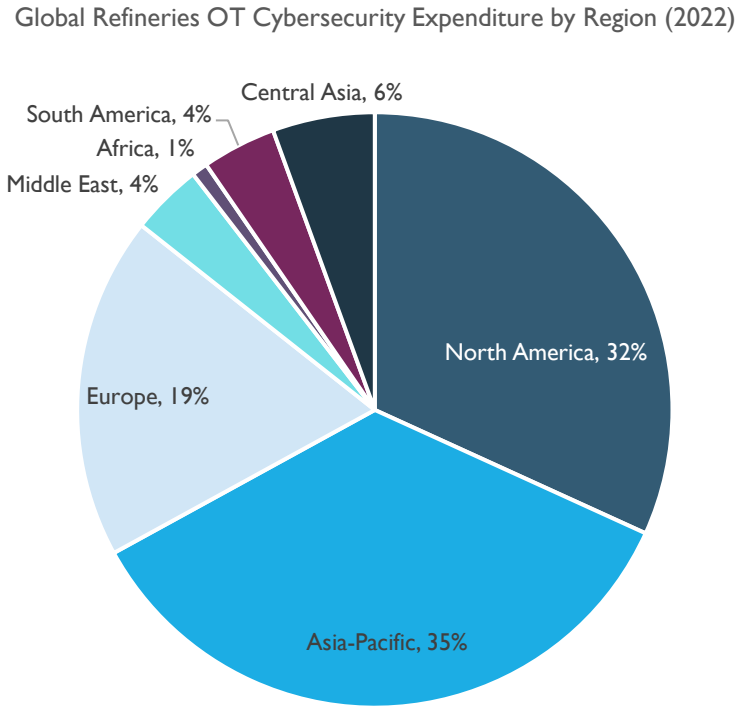
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Oil & Gas	512	612	734	880	1061	1281	1549	1871	2259



Definition: Upstream exploration and production of crude petroleum and gas.

Refineries TAM between 2023-2030 is $7.5B with a CAGR of 16%





Definition: Petroleum refining which involves the separation of crude petroleum into component products through cracking and distillation. This also includes the production of related gases including ethane, propane and butane but not industrial gases etc.

Chemical industry production capacity to be met by new plants and more efficient operations whilst cybersecurity maturity will increase due to regulations.

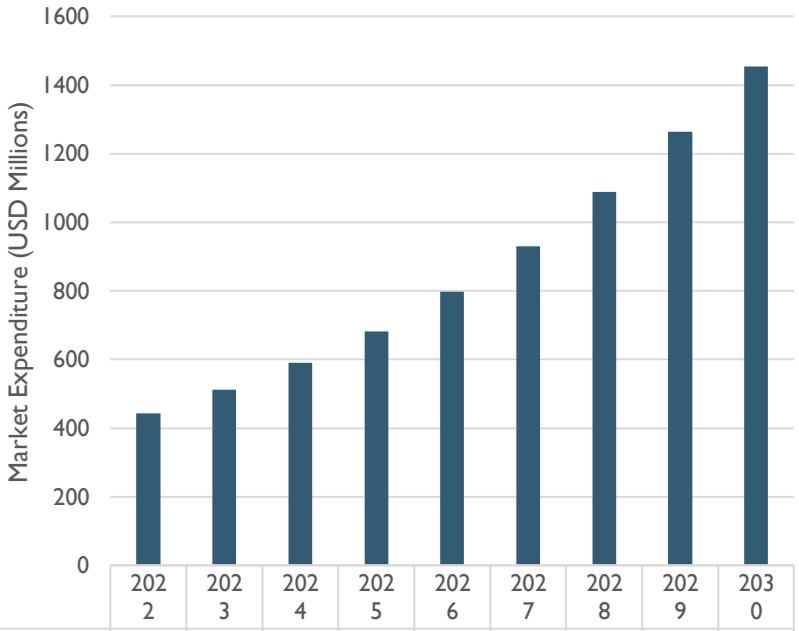
WESTLANDS ADVISORY

2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
Moderate growth is expected in 2023 following a slow 2022. The American Chemical Council estimates production grew 2% in 2022 and will reach 2.9% in 2023. BASF has a more conservative outlook for 2023 of 2%		**Global growth to 2030 is estimated at around 2%** p.a., lower than global GDP growth. This will differ by region, with some countries, notably India, expected to outperform the global average.	The digital maturity of the Chemical industry is lower compared to other industrial sectors and OT security is an area that requires investment. Customer challenges include gaining a view of networks across distributed sites and a mix of DCS architectures and configurations. The endpoint for large Chemical producers should be an end-to-end security architecture. However, transformation for many organisations is likely to be slow due to the complexity and safety aspects related to chemical processing. The customer priority will be safety, reliability and availability and therefore Westlands Advisory expects improvements to cyber resilience to be a lengthy process. Threats listed by CISA includes Buffer Overflows, Hard-Coded credentials compromise allowing control of HMIs or PLCs, and cross-site scripting to gain credentials as the prelude to an attack. These are common to all OT systems but highlight the importance of managing assets, securing access and protecting internet facing assets as part of an OT strategy. Obsolescence management is a key challenge for many Chemical (and Oil & Gas) facilities. This requires organisations to manage lifecycle data and maintain a SBOM to manage the risk posed by obsolescence (IEC 62402). Asset visibility and detection tools, and network segmentation, remain important security controls. The level of maturity increases according to company size and distribution, profitability (McKinsey Research) and ownership, with a wide variation in security practices across chemicals. Westlands Advisory does expect cybersecurity to mature across the industry due to digital transformation and increasing regulatory requirements.
Inflation has increased input costs considerably, pushing chemical companies to maintain profits through **increasing yields and throughput.**		**Plant expansion** in China and India are expected but high borrowing costs around the world is also likely to benefit **investment in DX** (rather than significant plant CAPEX) which can deliver process improvements at lower costs.	
Global rates of digital maturity in the chemical industry now exceeds 42%* indicating most chemical producers are in the process of actualising digital solutions.		Greenfield plants in emerging markets and modernised plants will increase digital maturity, with chemical companies becoming both **more operationally efficient and resilient.**	
High carbon contribution. Petrochemicals account for 14% of global oil and 8% of global gas demand whilst chemical industry ranks 3rd in industrial CO2 emissions.**		Chemical sector oil demand continue to increase by 33% up to 2030 and almost 50% by 2050. Investment in DX is one element of a larger ESG focus that includes **lower energy consumption** and a shift to **renewable power sources.**	
Low cybersecurity maturity. GAO have identified a lack of preparedness in US chemical plants, CFATS needs to continue to adapt to IIoT and digitalization within the industry. ISA 62443 is not tailored to chemical industry meaning specific standards are required to maintain safety.		Cybersecurity maturity will mature to 2030 as a result of DX and also **increasing regulatory requirements**. The EU's NIS2 will include chemical production and distribution including a focus on ensuring supply chain resilience.	

*Accenture data
**IEA data

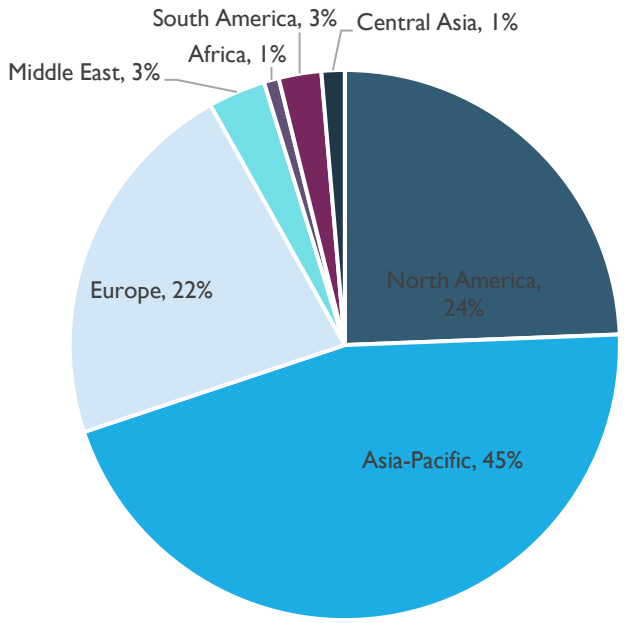
Chemicals and Chemical Product TAM between 2023-2030 is $7.3B with a CAGR of 16%

Chemicals & Chemical Products OT Cybersecurity Expenditure (2022-2030)



	2022	2023	2024	2025	2026	2027	2028	2029	2030
Chemicals & Chemical Products	443	512	591	683	797	931	1088	1264	1454

Global Chemicals & Chemical Products OT Cybersecurity Expenditure by Region (2022)



Definition: Transformation of organic and inorganic raw materials through a chemical process to produce chemical products. This includes industrial gases (refrigerants, carbon dioxide etc), dyes and pigments, inorganic chemicals (e.g. nitric acids), organic chemicals (e.g. acylic and cylic hydrocarbons), fertilisers, primary plastics (e.g. polymers and silicones), synthetic rubber, agrochemicals, paints, soaps and detergents, cleaning agents, glues, essential oils, etc.

Other Process Industries, including Mining and Steel, are focussed on improving productivity at existing sites and plants requiring with CAPEX forecast to be historically low to 2030

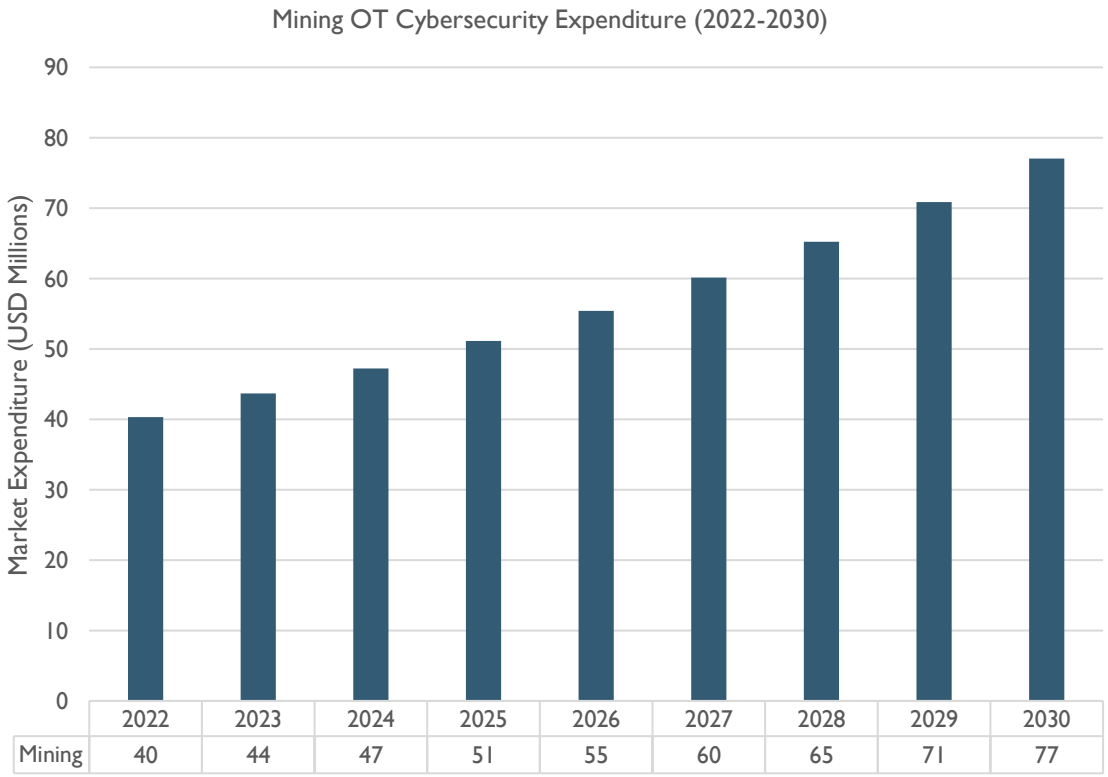
2023 Trend	2030 Outlook	2030 Status	Cyber Security Impact and Implications
CAPEX in the mining industry will be lower in 2023 than previous years as new mines become operational.		**Iron Ore and other minerals CAPEX is expected to further decrease to 2030** with most investment in sustaining existing mines rather than developing new sites. Coal production is expected to remain largely flat to 2030.	Other Process Industries includes **Mining and primary metal manufacturing** which includes iron and steel mills, foundries, aluminium production and copper. There is a significant process industry in Asia which includes coal mining (China, India, Indonesia and Australia are among the 5 largest producing countries in the World) whilst Australia is a leading supplier of certain minerals. China, India and South Korea are among the largest steel producers in the world. China is a leader in cement production whilst India, Indonesia and Vietnam are also in the top 10 globally. New infrastructure CAPEX is forecast to be relatively low to 2030 as focus switches to increasing productivity from existing mines and steel and metal producing plants. Therefore most cybersecurity expenditure will be on securing existing brownfield sites. Standards recommended by industry groups includes NIST and IEC 62443.
Steel production is forecast to increase slightly in 2023 following a >2% decline in 2022. Steel making capacity rose 1% in 2022. Production is expected to be close to 80% of capacity in 2023 – relatively high compared to the previous 20 years.		**Steel production to be reaching peak by 2030s** as materials science and recycling leads to alternatives.	
ESG factors are an increasingly important for process industries due to high energy costs and sustainability requirements.		Process industries will transition towards more sustainable practices with a focus **on using greener energy sources** and better resource management.	
Process industries are slowly digitalising with investment increasing to improve yields, energy consumption, throughput, scrap optimization, and quality.		**More mature digital operations** in some instances, including private 5G networks and increasing use of data and analytics. However, progress will be comparatively slow.	
Metals, mining and other process industries are generally at **an early stage of the cybersecurity lifecycle** due in part to a lack of cybersecurity regulation. This is changing due to heightened risk requiring firms to adopt a defence in depth approach to security.		**Cybersecurity programs are likely to improve** as a partial consequence of a growing ESG focus and the geopolitical importance of minerals. The criticality of some minerals in global supply chains may lead to stronger regulation which will further drive investment.	

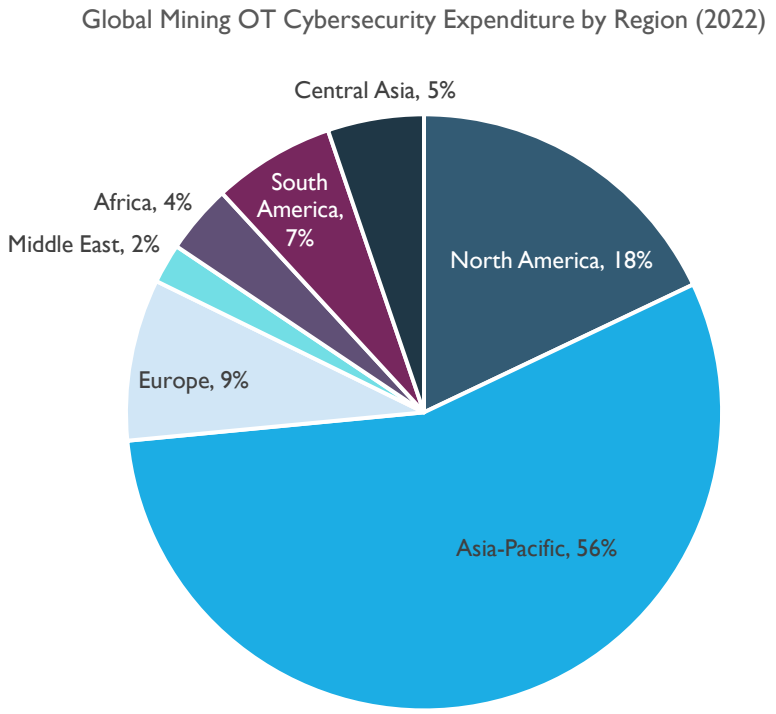
 Weakening

 Stable

 Strengthening

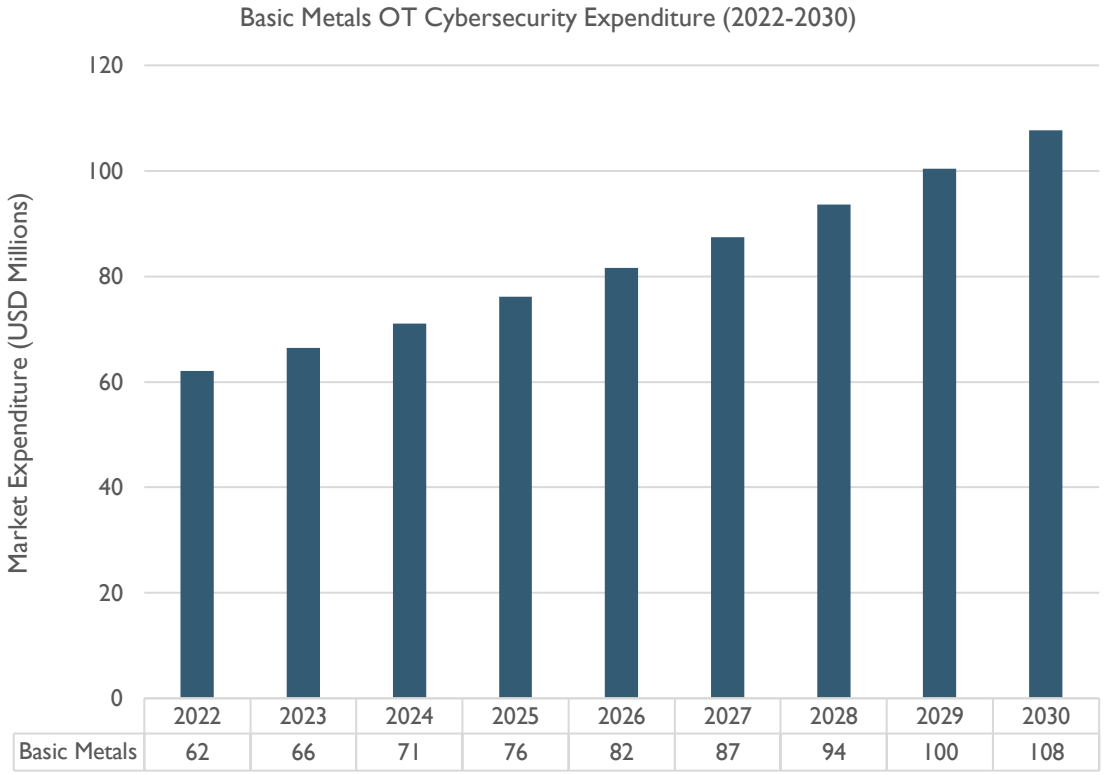
Mining TAM between 2023-2030 is $471M with a CAGR of 8%



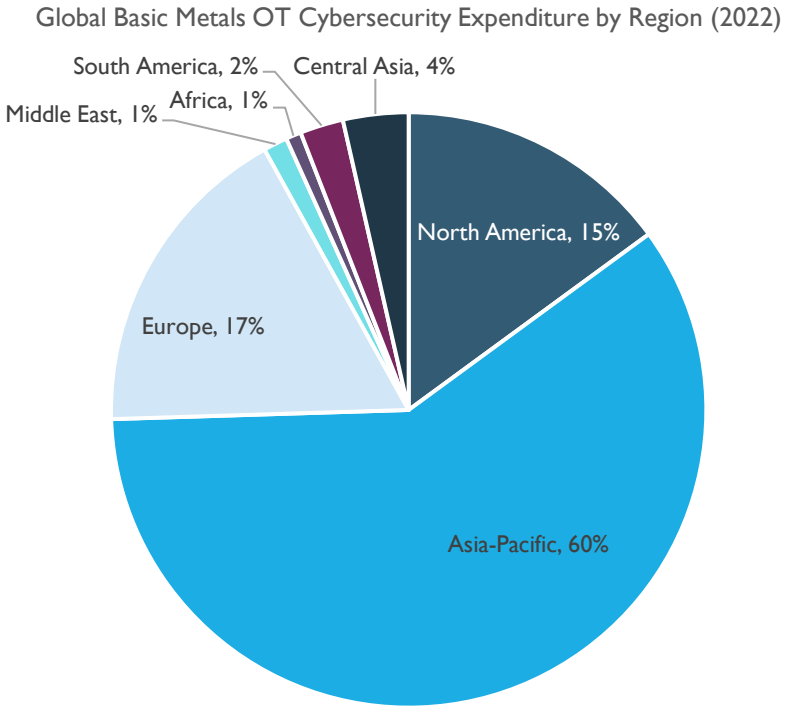


Definition: Mining of iron ores, non-ferrous metal ores, and uranium and thorium ores, and quarrying of stone, sand and chemical and fertiliser minerals.

Basic Metals Production TAM between 2023-2030 is $685M with a CAGR of 7%

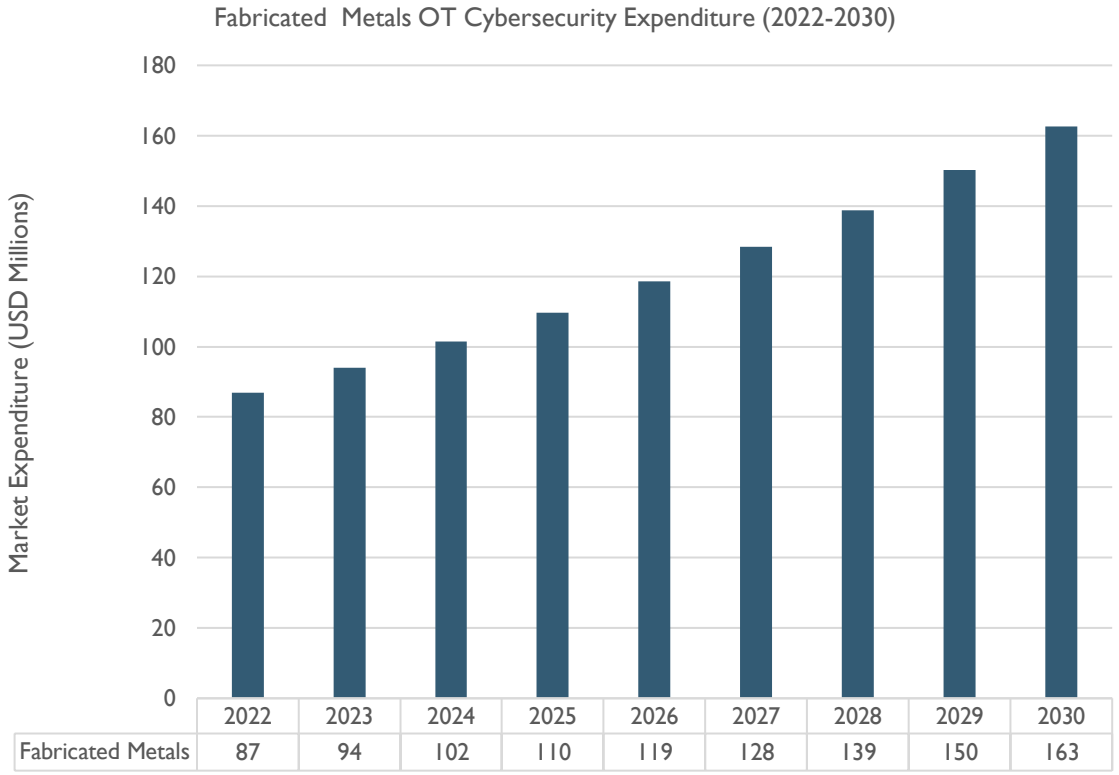


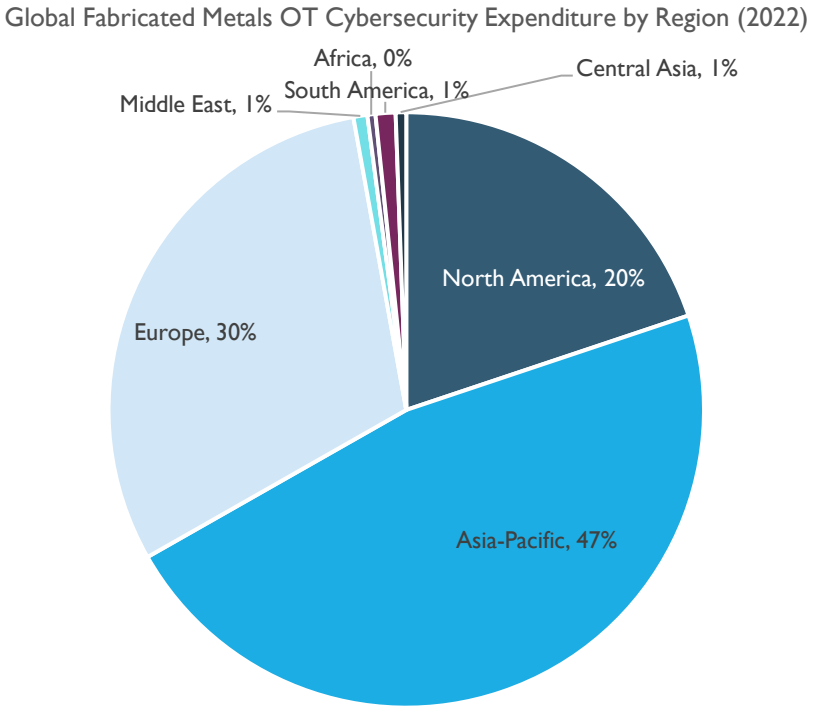
	2022	2023	2024	2025	2026	2027	2028	2029	2030
Basic Metals	62	66	71	76	82	87	94	100	108



Definition: Smelting and refining of ferrous and non-ferrous metals from ore, pig or scrap using metallurgic techniques. Also included is the manufacture of metals alloys and super-alloys. The output of smelting is usually in the form of an ingot which is then rolled to create plates, sheets bars and rods which are then used for castings and other basic metal products.

Fabricated Metals Production TAM between 2023-2030 is $1B with a CAGR of 8%

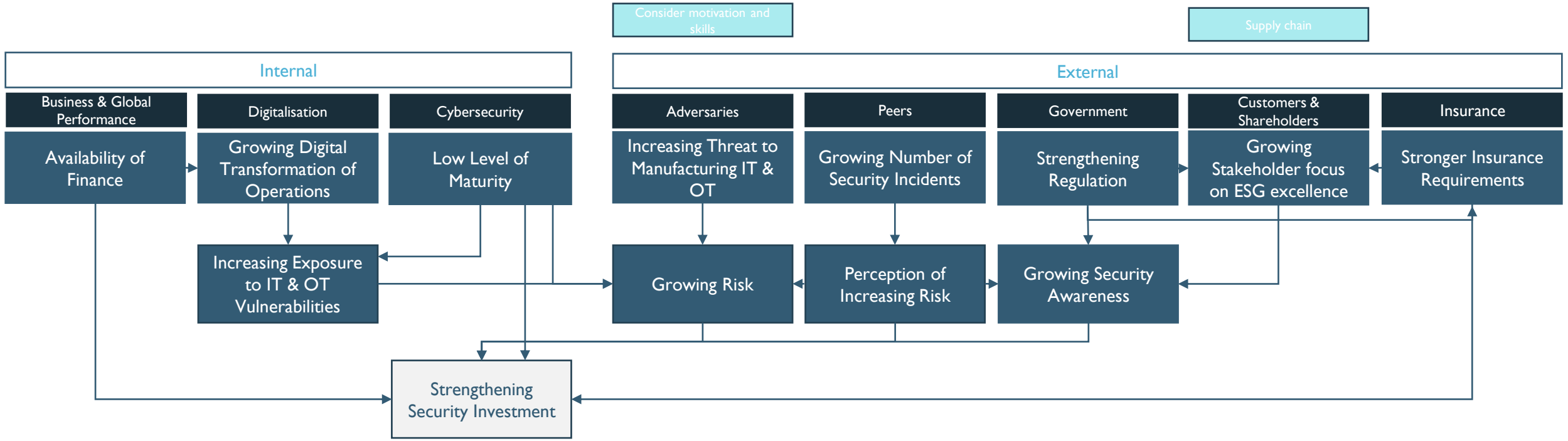




Definition: Manufacturing of pure metal products including structural metal products (e.g. prefabricated huts and sheds), frameworks for industrial equipment (e.g. blast furnaces, lifting equipment), doors, radiators, ammunition, and the forging, pressing, stamping and roll-forming of metal, cutlery, tools, toys and other metal components.

Appendix 2
Methodology

Forecast Methodology

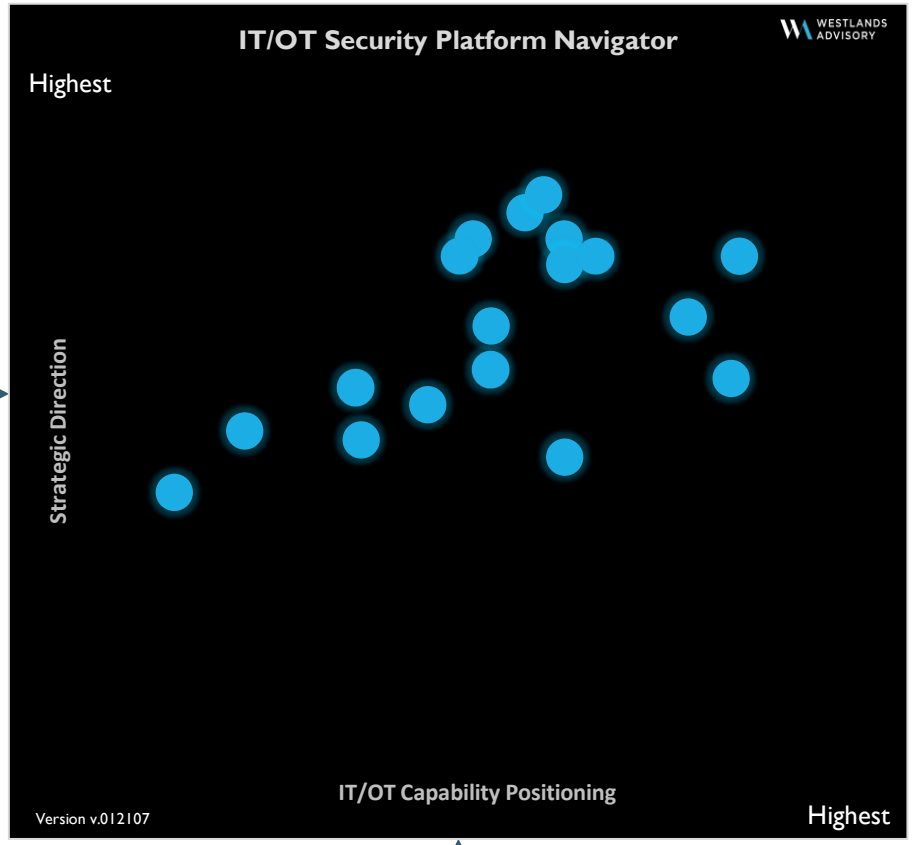


Navigator Methodology

The Navigator provides an evaluation of a Vendor's current position (Capability Positioning) versus its strategic intent (Strategic Direction).

Evaluation	Summary	% of Score	Positioning
Strategy & Investment Evaluation	Assessment of company strategy related to investment in people, technology and processes to improve its delivery of solutions to customers. This includes initiatives related to disruptive trends including new technology (e.g. 5G & IIoT) industry convergence, regulation and risk.	100%	Strategic Direction
OT Cybersecurity Capability Maturity Evaluation	An evaluation of services and/or technologies against categories outlined in the NIST cybersecurity framework. The evaluation includes whether the company has native capability in each category, and whether the technology has been widely deployed and tested in OT environments. (https://www.nist.gov/cyberframework/framework)	50%	Capability Positioning
Competitive Strength Evaluation	Evaluation of services and/or technologies in relation to competitor capabilities and customer requirements.	50%	Capability Positioning

Navigator



Navigator Evaluation Criteria

WESTLANDS ADVISORY

Capability Positioning

- Vision
- Operational Performance
- Technical Solution
- Ecosystem
- Financial & Governance
- People & Skills
- Innovation
- Infrastructure
- Reputation & Brand

Strategic Direction

- Vision
- Operational Strategy
- Product Roadmap
- Ecosystem Strategy
- Business Strategy
- People & Skills
- R&D Strategy
- Infrastructure Plans
- Brand Direction

IT/OT Cybersecurity Platform Navigator Qualification

WESTLANDS ADVISORY

- Company must provide native solutions in 4 of the following categories including a strong customer base.
    - Asset Visibility
    - Network Protection
    - Network Segmentation
    - Vulnerability Management
    - Risk Management
    - Endpoint Protection
    - Secure Access
    - Threat Detection
    - Security Ops & IR
    - Back-up & Recovery
- The relevant products integrate into a centralised platform
- The platform ingests information from other platforms or sources to enrich the data
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations.
- The platform has SIEM capabilities or integrates with SOAR platforms.
- The company has strong coverage in more than one geographical region.

Visibility & Threat Management Platform Navigator Qualification

WESTLANDS ADVISORY

- Company must provide native solutions for asset visibility and threat detection
- The relevant products integrate into a centralised platform
- The platform ingests information from other platforms or sources to enrich the data and provide context
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations.
- The platform has SIEM capabilities or integrates with SOAR platforms.
- The company has strong coverage in more than one geographical region

IT/OT Network Protection Platform Navigator Qualification

- Company must provide native solutions for OT network protection including all or one of NGFW, IPS and Data Diode.
- The relevant products integrate into a centralised platform with other network protection products including access management.
- The platform ingests information from other platforms or sources to enrich the data and provide context
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations, providing network and device visibility and management
- The platform has SIEM capabilities or integrates with SOAR platforms.
- The company has strong coverage in more than one geographical region