Navigator

Industrial Cybersecurity Industry Analysis 2025

Fortinet 2025

navigator.westlandsadvisory.com

Introduction

In May 2025 Westlands Advisory released a paper on ‘Industrial Cybersecurity Consulting and Managed Services.’ The analysis highlighted that as connectivity increases across and between plants and enterprises, so does exposure to cyber, physical, and operational risks. Growing investment in digitalisation and tightening regulation - combined with complex operations and distributed assets and resources - all contribute to the challenge faced by Risk Leaders. WA highlighted that whilst cybersecurity maturity has improved, a lack of resources means that Risk Leaders will continue to require the support of consulting and managed security services firms to operationalise cybersecurity technology and ensure a return on investment.

This paper explores how cybersecurity technology requirements are changing due to the confluence of market forces – digitalisation, risk and regulation. In 2023 WA noted a growing convergence between two different, but entirely complimentary approaches, to risk management. The traditional Defence in Depth model, a set of layered controls to protect data, applications, endpoints and the network, and Attack Surface Management which addresses challenges related to identifying, assessing, and mitigating risks. Since then, there has been a clear acceleration of ‘platformisation’ as vendors increase the breadth and depth of capabilities through innovation, acquisition, and integrations. In part this is in response to advanced Risk Leaders achieving asset visibility and moving on to implementing network segmentation and enforcement.

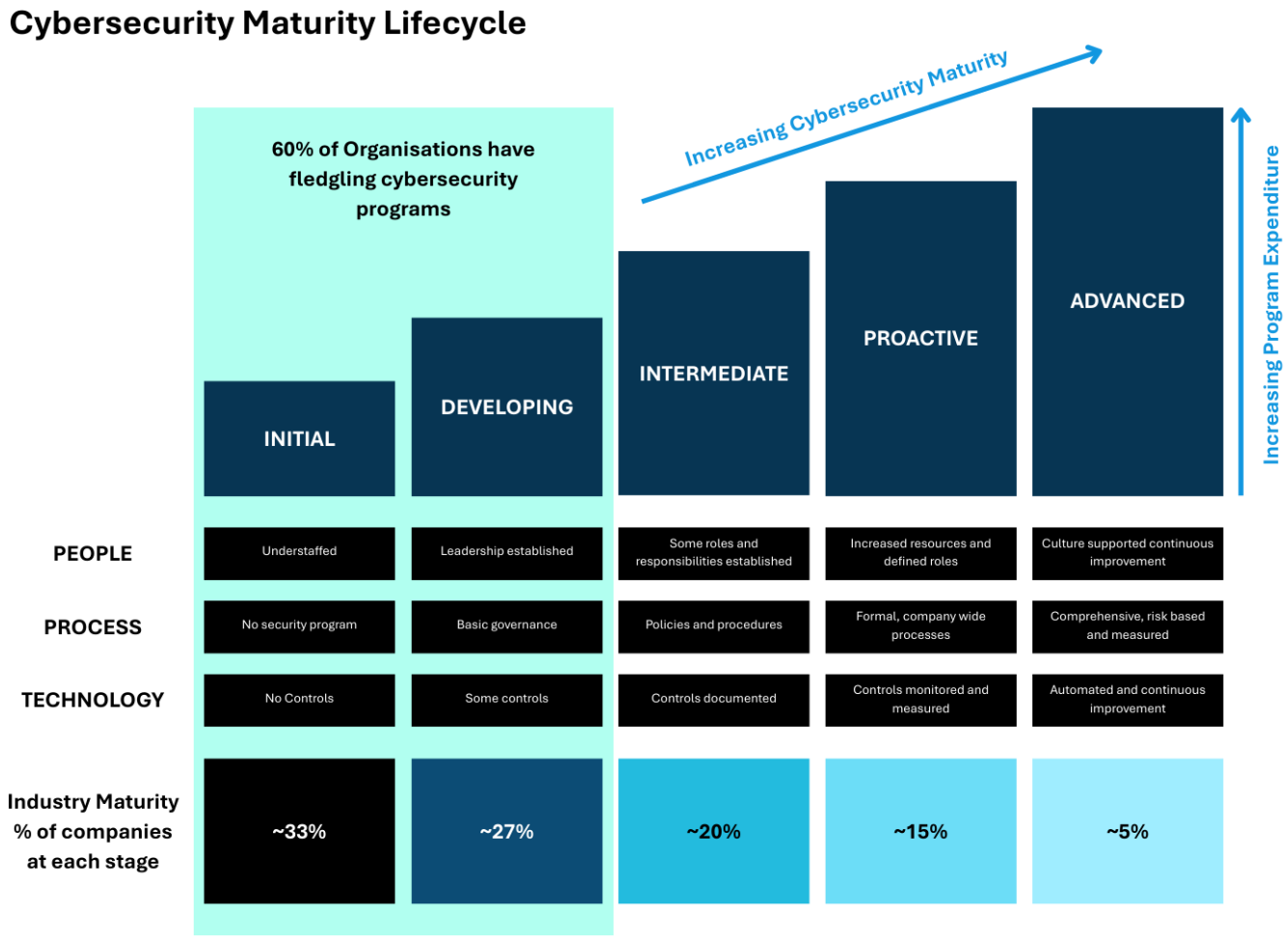
Advanced Risk Leaders are moving from defining their cybersecurity program as a set of technical controls to building a program that delivers operational resilience. This requires a framework of interoperable tools and processes across the enterprise to address the often-heterogenous nature of plants that are comprised of control systems from multiple OEMs, each specifying different cybersecurity controls or vendors. Risk Leaders should be working with vendors that provide native capabilities, integrate with a variety of 3rd party software and hardware, and can deliver a scalable and future proof solution.

Market Context

Investment in OT cybersecurity has been consistently strong over the last 5 years, with investment doubling between 2020 and 2024. Despite this investment, many asset owners remain at the initial stages of the cybersecurity lifecycle. WA estimates that 60% of organisations have no or fledging security programs with basic governance and

controls. Many of these organisations are small to medium sized business with no regulatory obligations. Without the regulatory stick, these organisations are slow to adapt.

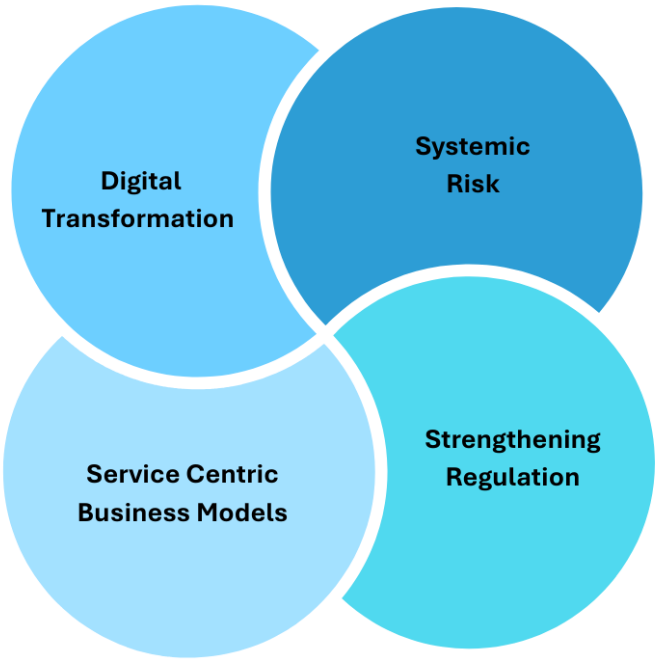
Moving along the maturity pathway organisations tend to be international with stronger cybersecurity and safety compliance requirements. Multinational Operators face complexity at scale. They often must coordinate across sites, jurisdictions, and business units, each with different infrastructure and risk profiles. Sovereign or state-regulated entities such as national grid operators, water utilities, or public transport providers often prioritise local compliance, trust, and assurance. They may face political or public accountability that global players do not. Key requirements include national data residency, sovereign service delivery and audit readiness.



The three main market forces - digitalisation, risk, and regulation - continue to shape how asset owners approach cybersecurity. In addition to these forces, Westlands Advisory has added a 4th driver of investment which is the increasing service-centric transformation of OT cybersecurity, the shift from buying cybersecurity products or point-in-time projects to consuming ongoing, integrated cybersecurity capabilities as services.

In the context of OT, it means that asset owners are increasingly turning to external partners to deliver, manage, and maintain security outcomes.

Market Forces Driving OT Cybersecurity Investment



1. Digital Transformation

OT environments are undergoing a significant shift. Once air-gapped and standalone, they now sit at the centre of complex, connected digital ecosystems. The adoption of cloud, remote operations, and edge computing is transforming how organisations design, run, and optimise industrial operations.

In this environment, traditional perimeters no longer apply. Instead, resilience depends on being able to enforce trust at the point of interaction: identity-based access, real-time monitoring, and strict segmentation across both north-south (IT to OT) and east-west (within OT) traffic flows. This includes managing distributed and connected assets, and controls that extend to endpoints, 5G infrastructure, and vendor-access portals.

2. Systemic Risk

Industrial operations face risks to their availability and safety, stemming from both intentional and unintentional actions. While sophisticated nation-state attacks are relatively rare, the more common threat comes from criminal networks targeting IT

systems or IT-connected assets within OT environments, often through ransomware. In addition, supply chain compromises and physical attacks also pose significant risks.

Industrial cybersecurity must go beyond OT network security or device hardening and extend to IT assets, ensuring that cybersecurity is not treated in silos. Platforms should support multi-layer threat modelling, coordinated response between digital and physical domains, and rapid containment strategies that prioritise operational continuity and safety.

3. Strengthening Regulation

As critical infrastructure has become a focus of national security, governments and regulators have strengthened existing regulations and introduced new ones, shifting from broad guidance to specific, enforceable obligations.

In the US TSA directions demand formal incident response planning, detection capabilities, and board-level accountability for transport operators, whilst CIRCIA mandates that critical infrastructure reports significant incidents to CISA within 72 hours.

In Europe, NIS2 expands the scope of early regulation, sets maturity baselines, and introduces penalties for non-compliance across a wide range of industry segments. The EU Cyber Resilience Act (CRA) places new requirements on manufacturers and software providers to embed security into design and lifecycle management. The UK's Cyber Security & Resilience Bill is expected to pass through Parliament in 2025, expanding the scope and regulatory powers of its predecessor.

In the Middle East, Saudi Arabia and the UAE have introduced local regulation related to critical national infrastructure protection and data sovereignty, whilst across Asia countries continue to strengthen policy, regulation and align to international standards (e.g. Australia, Japan, and Singapore).

Compliance is no longer separate from security. It must be embedded into platforms and service delivery including compliance dashboards and reporting, risk documentation, playbooks, and roadmap planning tied to regulatory timelines.

4. Service Centric Business Models

One of the most significant shifts in the OT cybersecurity market is the growth of service-centric business models. Rather than purchasing standalone tools or commissioning periodic consulting engagements, asset owners are increasingly consuming cybersecurity as an ongoing service that is structured, measurable, and aligned to resilience outcomes.

In practice, this means organisations are not just outsourcing tasks like vulnerability scanning or remote access management but are engaging service providers to deliver end-to-end capabilities, including maintaining response readiness, managing third-party access across industrial estates, embedding security into engineering projects, and correlating threats across IT and OT. These services are increasingly delivered with defined service-levels and measurable outputs.

This model is being accelerated by the evolution of underlying tools and platforms. Generative AI and automation are helping providers scale expertise, supporting faster incident analysis, alert summarisation, policy creation, and executive reporting. Orchestration platforms are making it easier to consolidate fragmented telemetry into meaningful, actionable workflows.

These market forces (digital transformation, risk, regulation, and security services) have changed how Risk Leaders should approach OT cybersecurity. Organisations can no longer rely on perimeter thinking or reactive practices. Leading asset owners are focussed on resilience by design, supported by capabilities that span detection, protection, governance, and recovery.

Operational Security Challenges Faced by Asset Owners

While the case for improving OT cybersecurity is increasingly well understood, execution remains difficult. Asset owners face persistent challenges that cybersecurity platforms can help overcome. This includes helping asset owners to understand the challenge, communicate the problem, deliver the business case, and manage the security operation.

1. Measurement, Value Realisation, and Leadership Buy-in

Many organisations still struggle to define what good OT cybersecurity looks like. Resilience is often treated as an aspiration, not a measurable objective. Metrics for uptime, recovery readiness, and risk reduction are not always in place making it difficult to set priorities or secure long-term investment. Asset owners struggle to move beyond compliance checklists to performance-based metrics. Questions like “Are we resilient to ransomware?” or “How long would recovery take?” remain hard to answer. This makes it difficult to set priorities, build confidence, or justify budget.

In addition, unlike traditional IT programs, OT cybersecurity investments are often preventative, with no immediate cost savings or productivity gains. This can make it

difficult to secure funding. Business leaders may struggle to understand the risk-reduction benefits or to justify spend against other operational priorities. Linking cyber investments to resilience outcomes, such as downtime prevention or regulatory assurance, is critical but not always well articulated.

Platform metrics are expanding, providing a greater number of KPIs and visualisation to improve reporting, providing high-level dashboards with asset criticality, threat exposure, and compliance status for board-level reporting. Analytics in some platforms allow for customised assessment of the asset risk and the relative reduction from introducing a compensating control, enabling Risk Leaders to clearly communicate how investment will reduce operational risk and the associated financial cost to the business.

2. Strategic Alignment & Governance

Asset owners are accelerating digital transformation and connectivity between IT and OT systems. This brings opportunities for efficiency, data-driven optimisation, and remote operations but it also introduces significant security and scalability concerns. As more enterprise applications and analytics platforms connect to OT data sources, organisations must manage increasing IT connectivity within traditionally isolated environments.

OT cybersecurity cuts across multiple departments from engineering and operations to IT, procurement, legal, and executive leadership. Without clear ownership and structured collaboration, initiatives stall or become fragmented. Internal misalignment on roles, funding, and priorities often creates confusion and inaction.

In addition to strategic alignment, compliance obligations are increasing across sectors and jurisdictions, from NIS2 to NERC CIP and TSA directives. For many organisations, staying ahead of shifting regulatory demands while maintaining operational performance is a significant burden.

Security teams must work closely with business units and engineering teams to align priorities, avoid disrupting core processes, and ensure that cybersecurity does not become a barrier to innovation. This requires scalable architectures, consistent governance, and services that balance control with operational agility. OT cybersecurity platforms solve this, providing shared context between IT, OT, and business teams, accelerating IT/OT convergence whilst providing value to different users. In addition, they provide support for standards like IEC 62443, NIS2, NERC CIP and offer compliance dashboards and evidence generation.

3. Foundational Visibility & Vulnerability Management

Establishing accurate and continuous visibility into OT environments remains the most fundamental yet persistent challenge for industrial cybersecurity. Many organisations still

struggle to answer basic but critical questions: What assets do we have? Where are they located? What software and firmware are they running? Are they vulnerable?

OT cybersecurity platforms address this by providing passive, non-intrusive asset discovery that is tailored for industrial protocols and control system behaviours. These platforms map the network in real time, identify device model and firmware version, and build dynamic inventories without disrupting operations. This visibility extends across legacy systems, proprietary devices, and remote field assets, giving security teams, engineers, and operators a shared view of the environment.

Beyond simple inventory, visibility must now include vulnerability context. Platforms correlate asset configurations with threat intelligence, CVE databases, and vendor advisories to highlight which systems are exposed and which matter most based on criticality and network location. This risk-based approach allows organisations to move beyond static compliance checklists toward prioritised vulnerability management, guiding remediation and segmentation efforts where they will have the greatest impact.

4. Detection, Segmentation, and Threat Response

OT cybersecurity has become synonymous with detection and while this remains an important requirement, there is a growing need to refocus on enforcement and incident response to address a shift towards resilient operations.

OT cybersecurity platforms address this by combining anomaly detection, industrial threat intelligence, and protocol-aware analytics to monitor for both known and unknown threats. They can interpret industrial protocols such as Modbus, DNP3, or PROFINET, enabling accurate identification of anomalous activity. Leading OT platforms support the shift to resilience by enabling integration between detection with firewalls, NAC systems, and segmentation gateways to enforce policies in real time, therefore isolating compromised assets, blocking unsafe commands, or restricting network access based on risk posture. This enforcement must be done carefully to avoid unintended operational impacts, which is why process-aware enforcement is gaining traction.

Effective segmentation is central to this approach. OT platforms assist in designing and validating zoning architectures, inspecting east-west and north-south traffic to detect policy violations, and supporting dynamic micro-segmentation. These capabilities help prevent lateral movement and contain threats before they can impact critical systems.

In addition, industrial systems often rely on external vendors and OEMs for maintenance. Remote access solutions are essential but also bring risk. Without strong control over who has access, when, and how, organisations expose themselves to unmanaged entry points and monitoring blind spots.

At the same time, operational realities can limit the speed or scope of enforcement. Operations teams are rightly focused on uptime and safety and changes that introduce latency, risk downtime, or interfere with automation are often resisted. Non-invasive monitoring and context-aware alerting remain important, but they must now be paired with enforcement mechanisms that are precise, predictable, and fail-safe. Achieving this balance requires strong cross-functional governance to ensure that security measures enhance resilience without compromising core processes.

5. Integration & Interoperability

A persistent challenge for many industrial organisations is the lack of integration between IT and OT security. Historically treated as separate domains this divide has led to silos that hinder coordinated detection and response. As cyber threats increasingly cross IT/OT boundaries, attackers exploit weakly monitored interfaces such as shared services, VPNs, or remote maintenance channels. To address this, modern OT cybersecurity platforms are designed to integrate bi-directionally with IT tools such as SIEM, EDR, SOAR, and IAM systems. This enables unified visibility, alert correlation, and coordinated response workflows across both domains, providing a more holistic view of enterprise risk.

Integration is not only a matter of IT/OT convergence but is also critical in managing the tool sprawl and vendor fragmentation that characterise many industrial environments. Over time, asset owners often accumulate a patchwork of security solutions often comprised of multiple firewall vendors and detection tools, managed by different service providers. This heterogeneity results in duplicated data, disjointed workflows, and critical blind spots. OT cybersecurity platforms are evolving to serve as integration hubs, offering open APIs, connector libraries, and data normalisation capabilities. These allow organisations to unify monitoring across diverse protocols and vendor systems, reducing noise and improving operational efficiency.

Risk Leaders should shift from loosely connected point solutions to integrated, platform-based ecosystems. This not only improves detection and response capabilities but also streamlines compliance, reporting, and long-term lifecycle management. For OT risk leaders, investing in integration is now a foundational step in building operational resilience.

6. People, Process & Talent

There is a shortage of professionals with both cybersecurity expertise and operational experience. Asset owners often rely on small internal teams who cannot keep pace with the growing scope of threats, regulatory requirements, and technical complexity. User-friendly interfaces, automated baselining, and AI-assisted threat triage reduce demand on skilled analysts. Some vendors offer managed detection and response (MDR) for OT.

Aiming for business resilience

As industrial systems become more connected, more complex, and more critical to business continuity, the concept of resilience has become central to cybersecurity strategy.

Resilience in this context is not about preventing every incident. It is about being able to anticipate, absorb, and recover from disruption without losing control of operations, compromising safety, or undermining customer and stakeholder trust.

The World Economic Forum's Unpacking Cyber Resilience report (November 2024) frames this well:

"Cyber resilience is an organization's ability to minimize the impact of significant cyber incidents on its primary goals and objectives."

For OT environments, these goals are uniquely operational. The priority is not just protecting data or devices, but maintaining safe, stable, and available physical processes whether that is running a turbine, managing a power grid, or keeping a production line online. Whilst traditional cybersecurity programs often focus on preventing incidents and meeting compliance requirements, resilience asks more strategic questions.

- Can we detect disruption early enough to take action?
- Can we contain an incident before it becomes a systemic failure?
- Can we recover operations quickly, safely, and in a coordinated way?

In this sense, resilience is not just a technical goal but a business capability. It requires risk-aligned governance, cross-functional ownership, contingency planning, and operational ability to respond under pressure.

It also recognises that threats do not respect organisational boundaries. A cyber incident in IT can cascade into OT. A compromise at a supplier or contractor can create ripple effects across the supply chain. A power outage, network failure, or system misconfiguration can be just as disruptive as a malware infection.

Resilience reframes cybersecurity as a continuous business risk management process that is comprised of six core capabilities. Cybersecurity platforms contribute to how Risk Leaders will deliver against these priorities.

Achieving Cybersecurity Resilience

- Visibility and prioritisation: Clear understanding of assets, dependencies, and risks - especially for the most critical systems.
- Layered protection: Segmentation, remote access controls, endpoint hardening, and perimeter enforcement to limit exposure and contain spread.
- Integrated governance and decision-making: Defined roles, shared policies, and cross-functional coordination and collaboration between engineering, security, operations, and executive leadership.
- (Managed) Security Operations: Monitoring, orchestration, automation and reporting of operations and incidents.
- Incident response and recovery readiness: Playbooks, tested procedures, offline backups, and clear escalation pathways that reflect the realities of industrial operations.
- Sustained maturity through lifecycle integration: Security embedded into procurement, engineering design, transformation initiatives, and ongoing risk management.

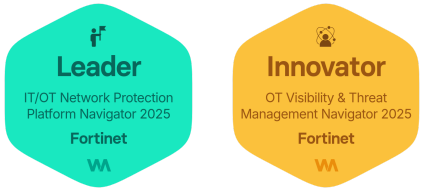
Concluding

In 2024 Westlands Advisory assessed the relative strength of trends impacting cyber risk. While cybersecurity expenditure has followed a linear growth curve over the last decade, and regulation has in most cases lacked teeth, digitalisation, automation, and cybersecurity incidents have been closer to an exponential growth curve. Westlands Advisory forecasts that cybersecurity expenditure will continue to grow strongly to address legacy systems, strengthening regulation, and continuing digitalisation.

WA's Navigator series provides a benchmark of leading OT cybersecurity platform vendors. This includes the OT Visibility & Threat Management Navigator 2025 and the IT/OT Network Protection Navigator 2025. The summary of both is represented in the IT/OT Cybersecurity Platforms Navigator 2025. The majority of Risk Leaders will be reliant on tools from a range of cybersecurity vendors and therefore should select partners whose technologies integrate seamlessly.

Risk Leaders should consider cybersecurity platforms that enable the organisation to transition towards resilient operations whilst addressing the needs and requirements of engineers and cybersecurity teams. Cybersecurity platform providers should be proven partners in OT, deliver native cybersecurity capabilities, but also integrate widely to provide protection and visibility across OT, and interoperability with modern IT cybersecurity tools.

Profile: Fortinet 2025



Introduction

Fortinet is a leading cybersecurity organisation with global revenues of $6B. OT cybersecurity has been a key strategic pillar of the organisation for the last 20 years, with extensive improvements over the last 5 years resulting in significant innovation, product expansion, growing alliances and increasing market share.

The Fortinet vision is to deliver broad, integrated, high-performance security products and services across IT and OT infrastructure. Fortinet continues to develop an integrated cybersecurity solutions portfolio – the Security Fabric platform is based on single OS, FortiOS – which is extended to the OT cybersecurity market. The OT Security Platform consists of over 20 products in 3 solution pillars: secure networking, zero trust/SASE, and security operations secured with AI-powered OT security services. In addition, the technology integration offered through the OT Security Platform extends beyond Fortinet solutions to third-party technologies, delivering a comprehensive and centralised OT service.

Positioning & Strategy

Globally, the Fortinet OT business is highly integrated and collaborative, consisting of a leadership team with numerous GIAC and ISA/IEC accreditations with significant industrial and engineering experience, and a pool of Subject Matter Experts that consult with partners and customers. The company has significant presence at industry events, consults on standards and regulations, and delivers frequent industry thought leadership.

Fortinet continuously invests in new technology to improve OT security for organisations. The company invests heavily in innovation, using Gen AI and Agentic AI to solve OT security operational challenges and in designing vertical specific solutions. The Fortinet OT Security platform delivers comprehensive security across multiple locations and sites, integrating networking and security to enable deep automation and real-time protection across industrial assets, networks, and appliances. It also makes extensive use of gen-AI and ML to accelerate decision-making and enhance operational efficiency, enabling

security teams to gain real-time insights and benefit from AI-driven automated incident detection and response.

Fortinet also has a strong reach through a globally distributed set of offices, engineering centres, and data centres providing customers with local support (25 global support centres) backed by sector and global expertise (FortiGuard Labs). Their OT cybersecurity business continues to grow at above market rate with high customer retention rates and CSAT scores reflecting strong satisfaction with its products and support services. Fortinet holds a particularly strong position in Europe and the Middle East, alongside significant customer relationships in the US and APAC. In terms of partnerships, Fortinet work with a wide range of partners through its Fabric-Ready Technology Alliance Partner Program and maintains strong relationships with channel partners and global SIs. The company has also forged a strong collaborative relationship with industrial automation and control system vendors such as Schneider Electric, Rockwell Automation, Siemens, and Honeywell to name a few.

Capabilities

For over two decades, Fortinet has protected OT environments through proactive and transformative OT security products.

Asset Discovery and Management for organisations are delivered through FortiGate (FortiOS) and FortiAnalyzer, which provide a unified network-wide device visibility and inventory, and integration with the FortiGuard Security Services, to continuously discover OT/IoT assets and vulnerabilities for the Fortinet OT Security Platform.

Fortinet’s FortiGate Rugged NGFWs and FortiSwitch Rugged devices, as well as indoor models, enforce industrial-grade network protection and policy-based segmentation (zone/VLAN/port isolation), using FortiGuard’s OT Security Service to block malicious lateral movement, ensuring strong Network Protection and Segmentation. While solutions for Endpoint Protection include FortiEDR and FortiClient, providing endpoint security for OT/IT hosts, and FortiEDR has been optimised for OT environments (deployable in hybrid OT/IT and on-prem settings) with legacy OS support. Remote Access Management is supported by FortiGate (with VPN/NGFW) and FortiAuthenticator secure remote connectivity to OT sites, and Fortinet’s FortiSRA solution adds OT-specific secure remote-access controls (e.g. managed credentials), including logging, monitoring, and recording of remote sessions.

For Risk and Vulnerability Management, FortiGuard OT Security Service supplies thousands of OT-specific IPS rules for OT-specific applications, protocols, and

vulnerabilities, and validated integrations provide continuous OT vulnerability assessment and risk scoring, all managed through FortiManager / FortiSIEM. The company also provides passive (FortiGate) and active Threat Detection (FortiNAC / FortiClient) with FortiSandbox for investigation. FortiNDR and FortiDeceptor can also be used, and all integrate seamlessly with FortiSIEM for comprehensive threat management.

FortiSIEM/FortiAnalyzer are used for Security Operations, centralising IT/OT event management and alerting for SOC operations, while OT-focused tools like FortiDeceptor (deception) and FortiNDR (network detection) provide additional OT threat hunting and compliance support. While Fortinet do not have a dedicated OT Back-Up and Disaster Recovery solution, Fortinet's FortiSOAR, brings OT specific security automation and response capabilities and can be integrated across the OT Security Platform and third-party solutions.

Market Perception

Fortinet is widely recognised by industrial enterprises, critical infrastructure operators, and OT cybersecurity stakeholders as a leading OT security platform provider. Notable strengths include the depth of integration across the Fortinet OT Security Platform, custom-built ASICS technology, and continued innovation in securing complex environments. Fortinet's ability to deliver high-performance, low-latency security tailored to industrial needs, and at scale, makes it a trusted partner for safeguarding mission-critical OT systems.

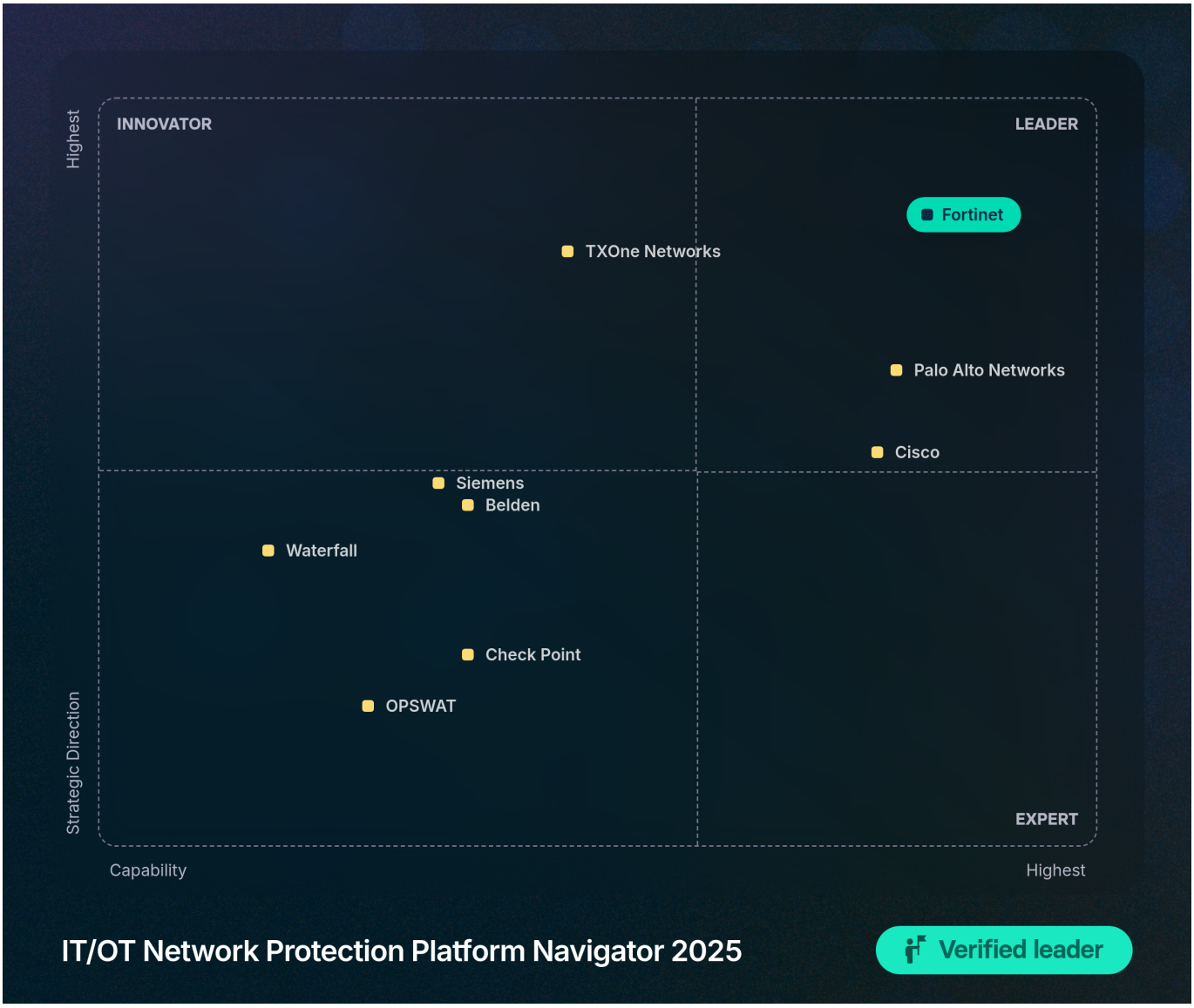
The Fortinet OT Security Platform: The single FortiOS operating system delivers a suite of security capabilities with indoor and ruggedised appliances, virtual machines, cloud, and containers making FortiOS easy to deploy regardless of site or location. Customer benefits includes a flexible, scalable, and holistic security solution that protects, detects, and responds to security and operational incidents.

ASICs Technology: Fortinet designs and manufactures its own custom ASICs with the latest iteration being FortiSP5. This proprietary approach enables Fortinet to deliver high performance, energy efficient, and cost-effective solutions compared to general-purpose CPUs. By integrating these customs ASICs with its FortiOS operating system, Fortinet provides a unified and high-performance security solution that addresses the demands of modern network environments.

OT Innovation: Fortinet offers the broadest range of industrial-grade security hardware solutions, including FortiGate Rugged firewalls and FortiSwitch Rugged switches. This includes current and forthcoming versions that are compliant with industry specific

standards (e.g. railway, maritime, Oil & Gas, and other industries). Fortinet's product roadmap is highly responsive to customer requirements and industry standards and has resulted in a number of industry awards including the 2024 Red Dot Product Design Award (FortiGate Rugged 70G-5G-DUAL) and ControlEngineering 2024 Silver Product of the Year Award for FortiGate Rugged 70F and 2025 Gold Product of the Year Award for FortiGate Rugged 70G-5G-DUAL. Innovation extends to AI and ML where the focus has been on detections, understanding risk and improving security operations.

IT/OT Network Protection Platform Navigator 2025



Introduction

OT Network Protection is integral to a Defence-in-Depth approach, providing protection at the network boundary (North to South) through network monitoring and enforcement of policies and segmentation of East to West traffic.

Definition

Network Protection platforms have several native capabilities, including firewalls and access control. Use-cases may include network visibility, segmentation, Zero Trust policy enforcement, and incident response. Most network protection platforms also include other native technical controls (e.g. endpoint protection) or integrate with third party tools. The Platform orchestrates and provides centralised visibility and control of OT cybersecurity operations.

Further insight on the market and industry trends is available in the related WA Insight report, “Industrial Cybersecurity Industry Analysis”.

Evaluation

The following capabilities are included in the evaluation:

- Network Protection including Firewalls, IPS, unidirectional gateways and data didoes.
- Network Segmentation including Firewalls, VLAN’s, Access Control Lists (ACL), SDN and agentless Micro Segmentation through identification and logical grouping of assets and devices.
- Endpoint Protection including malware scanning, application whitelisting and patch management, and USB protection.
- Secure Access including PAM, VPN and ZTNA.
- Security Operations & Incident Response including SIEM, SOAR, XDR and EDR plus playbooks.

Qualification

Vendors must meet the following criteria to qualify for consideration in the IT/OT Network Protection Platform Navigator:

- Company must provide some native solutions for OT network protection including firewalls, IPS and Data Diode.

- 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 SOC solutions.
- The company has strong coverage in more than one geographical region with OT cybersecurity revenues > $20M

Methodology

Further information on WA's methodology can be found on the website at https://navigator.westlandsadvisory.com

OT Visibility & Threat Management Navigator 2025

Introduction

Visibility & Threat Management platforms include asset and network discovery, contextualisation, vulnerability management and threat detection. The platform will typically integrate with other security platforms or with the SIEM.

Definition

The market consists of a range of vendors using different approaches. This includes pureplay visibility and asset management competitors using agent-based discovery, threat detection companies using passive scanning among other techniques, and network vendors delivering visibility and threat detection through firewalls or embedded in

switches. Further insight on the market and industry trends is available in the related WA Insight report, “Industrial Cybersecurity Industry Analysis”.

Evaluation

The following technologies are included:

- Asset Visibility including active scanning and agent-based discovery.
- Vulnerability Management.
- Risk Management including quantification, configuration management and compliance management.
- Threat Detection including Machine Learning, User & Entity Behavioural Analytics (UEBA) and Signatures.

Qualification

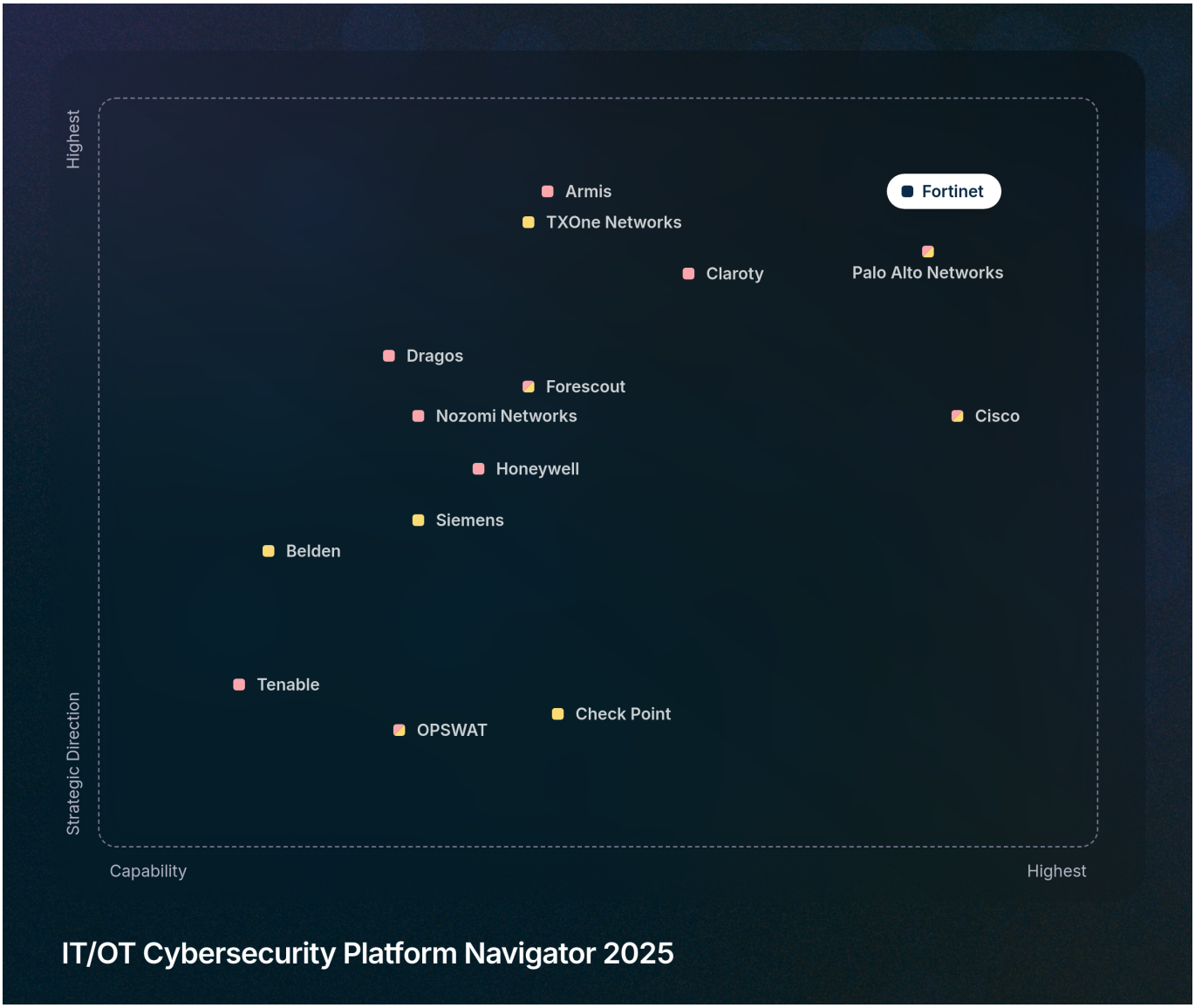
Competitors must meet the following criteria to qualify for consideration in the IT/OT Visibility & Threat Management Navigator:

- The Company must provide native solutions for asset visibility and threat detection.
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations.
- The platform integrates into SIEM and SOC solutions
- The company has strong coverage in more than one geographical region with OT cybersecurity revenues > $5M

Methodology

Further information on WA’s methodology can be found on the website at https://navigator.westlandsadvisory.com

IT/OT Cybersecurity Platform Navigator 2025



Introduction

IT/OT Cybersecurity Platforms include several native products and integrate with other products or platforms to provide the customer with a single, unified view of operations.

Definition

The market consists of two types of vendors, those providing Visibility & Threat Management and those that have a strong Network Protection product portfolio. Security Leaders will usually rely on at least one vendor from each category. However, competitors are expanding capabilities and it is increasingly common for vendors to provide both Visibility & Threat Management and Network Protection solutions.

Further insight on the market and industry trends is available in the related WA Insight report, “Industrial Cybersecurity Industry Analysis”.

Evaluation

The following technologies are included in the evaluation:

- Asset Visibility
- Network Protection
- Network Segmentation
- Vulnerability Management
- Risk Management
- Endpoint Protection
- Secure Access
- Threat Detection
- Security Ops & IR
- Back-up & Recovery

Qualification

- Company must qualify for either the OT Visibility & Threat Management Navigator or IT/OT Network Protection Platform Navigator.
- In addition, the platform must have native solutions or be able to integrate with products from both categories.
- The company must have OT cybersecurity revenues > $30M

Methodology

Further information on WA’s methodology can be found on the website at https://navigator.westlandsadvisory.com

Appendix

Vendors are assessed according to Capabilities and Strategic Direction.

This includes an evaluation of current products and services, contributing 50% of the total capabilities score, and an evaluation of nine further categories that completes the scoring. The remaining score is against 9 core competencies including Leadership & Staff, Internal Operations, Security Processes, Technology Implementation, Market Access, Execution, Partners, Customers, and Business Performance.

Strategic Direction is an assessment of the company plans and strategy related to Vision, Investment, Leadership & Staff, Internal Operations, Product & Services Roadmap, Technology Implementation, Market Access, Partners, and Customers.

The following information and insight contributes towards the Navigator research and conclusions. Westlands Advisory directly interviewed over 70 organisations - a mix of Service Vendors, Platform Vendors, CISOs, and Engineering Leaders.

- Open Source: Collection of all relevant open-source information on vendors including company documentation and information, reviews and 3rd party websites.
- Questionnaire: The Industry OT Cybersecurity Navigator 2025 vendor questionnaire is an important source of information. The survey is issued at the start of the process and is confidential, only being used for evaluating vendor performance.
- Vendor Briefings: Vendor briefings offer industry the opportunity to provide Westlands Advisory with insights into current capabilities, strengths and strategic direction. The purpose of the Vendor Briefing is to ensure that Westlands Advisory has the facts and insight required to evaluate the companies' Capability Positioning and Strategic Direction.
- CISO and Engineering Leaders: Interviews with CISOs and Engineering Leaders to gain further insight into Service Vendor performance, strengths and weaknesses and views on the wider ecosystem.
- Community Briefings: Westlands Advisory gains insights from Platform Vendors and other channel partners into the relative strengths and weaknesses of different Service Vendors. Westlands Advisory also consults with industry experts on the market and services and has an independent consultation process to ensure that the process is fair and representative.