Magic Quadrant for CPS Protection Platforms

12 February 2025 - ID G00808225 - 47 min read

By Katell Thielemann, Wam Voster, and 1 more

Cyber-physical systems protection platforms that discover and protect assets in production or mission-critical environments are emerging as a leading market category. This research will help cybersecurity leaders find the right vendor to facilitate protection of CPS using CPS protection platforms.

Strategic Planning Assumptions

By 2027, 75% of CPS-intensive organizations will obtain cybersecurity capabilities from a cyber-physical systems protection platform (CPS PP), accelerating the shift from point solutions.

By 2027, 45% of organizations will prioritize remediation capabilities as a selection criterion for CPS PPs, prioritizing “doing” over “knowing.”

Market Definition/Description

Gartner defines the cyber-physical systems (CPS) protection platforms market as products that use knowledge of industrial protocols, operational/production network packets or traffic metadata, and physical process asset behavior to discover, categorize, map and protect CPS in production or mission-critical environments outside of enterprise IT environments. CPS protection platforms can be delivered from the cloud, on-premises or in hybrid form. Gartner defines CPS as engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). When secure, they enable safe, real-time, reliable, resilient and adaptable performance.

Whether in critical infrastructure, manufacturing, warehousing, transportation, utilities, building management or healthcare, every asset-intensive organization has CPS. They can be interchangeably called operational technology (OT), Internet of Things (IoT), Industrial IoT (IIoT), Internet of Medical Things (IoMT), smart building solutions, or Industrie 4.0. Whatever term organizations choose to adopt, these systems have one thing in common — they are managed digitally but interact with the real, physical world.

Security for these connected assets used to be "out of sight, out of mind," or covered under a generic OT security umbrella dominated by network-centric tools. An asset-centric security discipline has emerged, however, as organizations aiming to reduce cyber risks started asking questions such as:

- "What CPS do I have?"
- "How do they connect?"
- "What is their risk profile and how can I improve my security controls as a result?"

The CPS protection platforms market exists because:

- **The attack surface is growing:** CPS are usually core value creation assets and, if they go down, they halt production or derail missions. The more connected they become, the more they expand the attack surface. This increasingly makes them attractive targets for ransomware, industrial espionage or geopolitically motivated attacks. From operational disruptions of pipeline operators to halted machinery at shipbuilders, the number of disclosed attacks continue to rise.
- **Threats are on the rise:** malware purposely built for industrial environments such as INDUSTROYER.V2 and Pipedream are emerging.
- **More vulnerabilities are surfacing:** yet remain difficult to manage as CPS cannot be patched at will.
- **More regulations, directives and frameworks are emerging:** due to increased threats to critical infrastructure-related organizations, governments are recognizing that the ubiquitous CPS technology landscape supporting them is key to national security and economic prosperity.
- **Manual asset inventories are time inefficient and costly:** and IT security tools are inappropriate for many CPS environments.

Mandatory Features

The mandatory features for this market include:

- Vendor-native asset discovery, visibility and categorization
- Support for both modern and unique industrial protocols while not interfering with the operation of any device
- Detailed network topology and data flow diagrams
- Detailed pedigree of assets, including nested devices
- Vulnerability information and recommended actions
- Threat intelligence information and recommended actions
- Integration with IT security tools
- Risk scoring and recommended actions

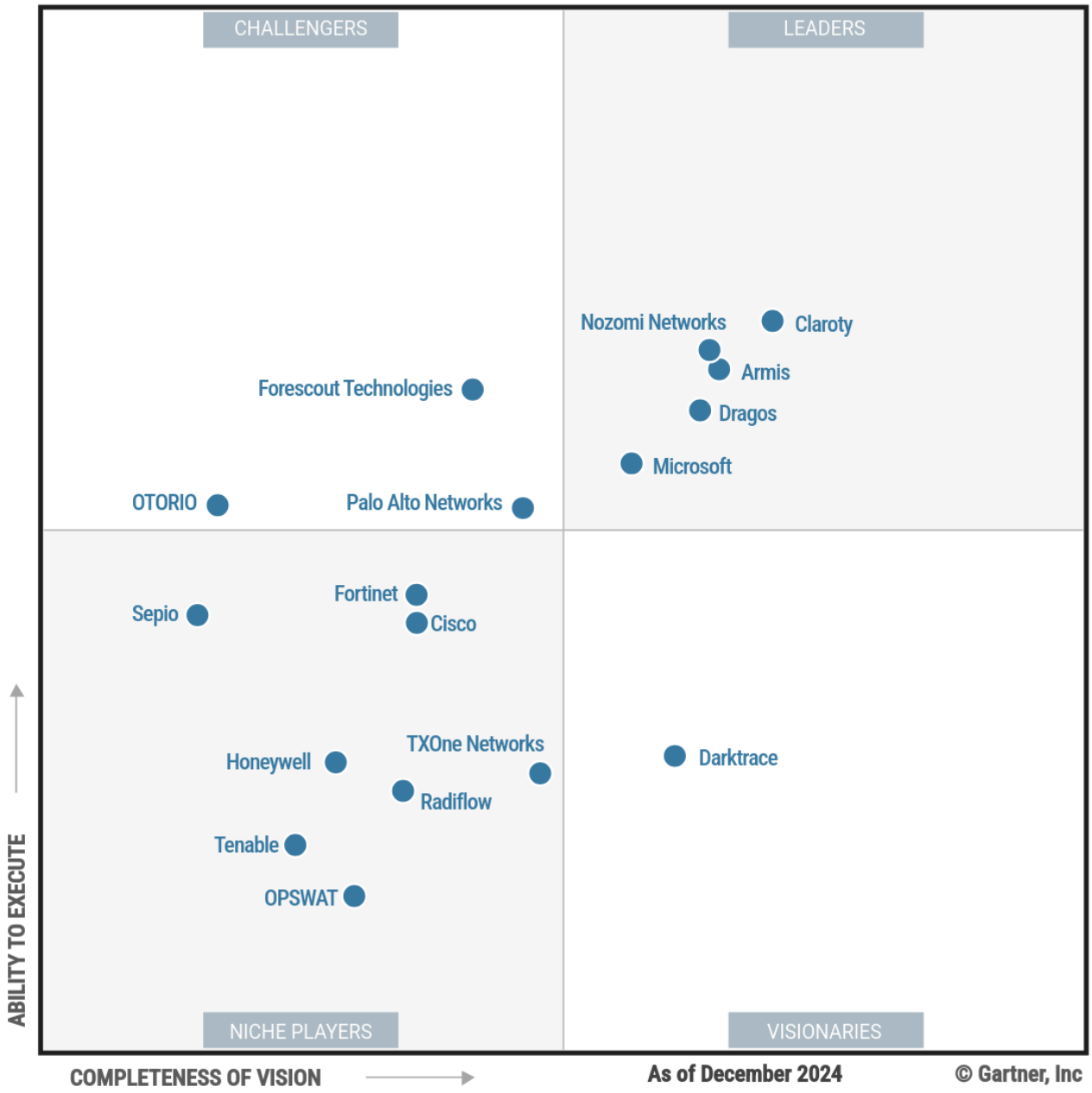
Common Features

The common features for this market include:

- Baseline and configuration management
- Incident response and forensics
- Network-segmentation-related features and functionalities
- Security frameworks compliance reports
- Various role-based user interfaces

Magic Quadrant

Figure 1: Magic Quadrant for CPS Protection Platforms



Gartner

Vendor Strengths and Cautions

Armis

Armis is a Leader in this Magic Quadrant. Its Armis Centrix Cyber Exposure Management Platform is the CPS PP. The Armis Centrix platform is delivered only as a SaaS solution. Armis's acquisitions of Silk Security and CTCI have increased its capabilities to prioritize vulnerability remediation and threat intelligence. It is known for its user interface and the ability to integrate with other platforms. It is suited for organizations seeking a cloud-based security solution that offers coverage for enterprisewide CPS and IT.

Strengths

- **Geographic strategy:** Armis has a broad sales and support presence, serving traditional markets in North America, Europe and Asia, as well as emerging markets like Latin America and Africa. This makes it suitable for globally dispersed organizations.
- **Product strategy:** Existing discovery tools like passive network analysis have recently been expanded with integrations and additional active querying capabilities to enhance both asset discovery capability and speed of deployment.
- **Operations:** As a SaaS platform, Armis Centrix collects real-time operational intelligence of platform usage to drive product improvements. The free Armis University caters to various learning needs and skill levels, covering navigation, feature usage, configurations, integrations and best practices.

Cautions

- **Overall viability:** Armis is largely held by venture capital firms and employees. Large investments in go-to-market efforts to capture market share have offset the profit from the platform. The rapid growth of the company size in 2024 and the two recent acquisitions require scalable processes to be successful.
- **Business model:** Customers can choose five different product suites designed to use features from each product. While the core offerings include protection of CPS networks and assets, advanced features are sold separately, meaning customers need to make additional investments to reap the full benefits of Armis Centrix.
- **Vertical/industry strategy:** Given its strategy to be an enterprise solution, the Armis Centrix platform can identify devices ranging from X-ray scanners to industrial cranes, but does not prioritize deep vertical industry knowledge.

Cisco

Cisco is a Niche Player in this Magic Quadrant. Its Industrial Threat Defense CPS PP consists of Cyber Vision, built on the 2019 Sentryo acquisition, along with Splunk, Secure Firewall, Identity Services Engine, Secure Equipment Access and Talos threat intelligence. Cisco sensors can be embedded into select Cisco Catalyst routers and switches, providing a network-centric approach to detection, investigation and response in CPS environments. Cisco's 2024 Splunk acquisition aims to harmonize signals from multiple data sources for a unified IT systems/CPS cybersecurity pane of glass for organizations. The solution is suited

for large organizations with a global industrial footprint that prioritize single vendor solutions.

Strengths

- **Sales execution/pricing:** Cisco's CPS deals involve high-touch presales engagements with the industrial specialist team. Its pricing model for multiyear contracts is suited for large-cap organizations with heavy multinational and industrial footprints.
- **Geographic strategy:** Cisco supports many geographic areas, both direct and partner/channel-based, including partnerships with OEMs that also resell Cisco products.
- **Marketing strategy:** As a leading global company, Cisco has a long track record of top-tier business-to-business (B2B) marketing campaigns and a broad reach that can attract CPS security end users in search of solutions.

Cautions

- **Product strategy:** While Cisco's Industrial Threat Defense has out-of-the-box integration between its products, it is lagging in a seamless user experience as users must switch between those products.
- **Innovation:** Cisco's innovations, such as the Encrypted Visibility Engine and SnortML in Secure Firewall, are more IT-centric than CPS-centric and unlikely to show tremendous value within mature CPS security programs.
- **Vertical/industry strategy:** Cisco's limited CPS vertical focus on manufacturing, energy and transportation may limit its expansion and development of the CPS PP to meet a wider set of use cases and value.

Claroty

Claroty is a Leader in this Magic Quadrant. Its xDome and CTD are the CPS PPs. Claroty's 2022 Medigate acquisition accelerated its healthcare position, its ability to offer a cloud-based solution and the release of capabilities, such as contextual risk scoring, remediation playbooks and compliance reporting. Two versions of the platform are available: xDome (SaaS-based) and CTD (on-premises). It also offers services and healthcare-specific features, such as Clinical Device Efficiency. xDome is suited for organizations in manufacturing, healthcare, commercial buildings and critical infrastructure. CTD is suited for organizations

who are not ready for or cannot use cloud solutions, such as those in oil and gas or transportation.

Strengths

- **Market responsiveness:** Claroty has a mature process to gather customer needs, evaluate the threat landscape and assess competitors. This allows it to respond rapidly to market needs, as evidenced by the recent addition of compliance reporting in response to government directives and frameworks, and continuous threat exposure management (CTEM) tailored to CPS security.
- **Product strategy:** Claroty has experience executing its product roadmap, as demonstrated by its focus in 2024 on visibility quality with multiple data collection capabilities, creation of tiers for visibility quality and zone policy development for segmentation.
- **Vertical/industry strategy:** When it acquired Medigate for healthcare solutions, Claroty became one of the first companies in this market to recognize specialized industry needs. It has dedicated business leaders and functions aligned to industry requirements to coordinate vertical product and go-to-market efforts.

Cautions

- **Pricing**: Claroty's pricing options can be confusing. For example, it offers software per asset and per site; per bed pricing for healthcare; and capital expenditure (capex) and operating expenditure (opex) models for hardware; as well as a mix of lease, subscription, perpetual licenses and bundling models.
- **Geographic strategy:** While a global company, Claroty does not have the same reach at the country level as some of its competitors, and over half of its revenue comes from North America. This can be a challenge for prospects in regions with low or no presence.
- **Operations:** Claroty has one close cloud partner (Amazon Web Services). While Claroty has an on-premises offering, there are a couple of months of lag for full-feature parity with xDome, as SaaS solutions are easier to update.

Darktrace

Darktrace, acquired by private equity firm Thoma Bravo in October 2024, is a Visionary in this Magic Quadrant. Its Darktrace/OT is the flagship CPS PP, which deploys AI to learn a

baseline of “normal” behavior within an organization, detecting anomalies outside the norm that could signify cyberattacks, insider threats and vulnerabilities. The platform is part of an overall Darktrace AI-based cyber defense portfolio that identifies and mitigates attacks and insider threats across IT, CPS, cloud and email. Darktrace is suited for organizations that value AI-based risk scoring capabilities and a low price point, have deployed Darktrace in IT already, and need global coverage and support.

Strengths

- **Geographic strategy:** The company has a global coverage, providing direct sales and channel support in 27 countries. This benefits prospective customers seeking global coverage and support.
- **Product strategy:** Darktrace/OT is part of the wider product portfolio that ranges from network to cloud and endpoint security. It is based on self-learning AI that autonomously learns normal behavior in a CPS environment, enabling real-time anomaly-based threat detection without relying on signatures.
- **Financials:** Darktrace has a large customer base beyond its CPS PP offering, and is profitable. Nearly all revenue comes from annual subscriptions for a solid cash flow that allows continuous investment in new features and capabilities.

Cautions

- **Operations:** Many customers use Darktrace entirely offline, which makes gathering real-time operational intelligence about the platform’s usage impossible.
- **Market responsiveness:** As both an IT and CPS security vendor, Darktrace is maturing its ability to keep its fingers on the pulse of the quickly evolving CPS security market.
- **Marketing strategy:** CPS PP buyers may perceive Darktrace as an IT security solution shoehorned into a CPS environment. Industry recognition like Darktrace’s status as Microsoft’s U.K. Partner of the Year amplifies this perception, undercutting confidence in Darktrace’s knowledge of industrial operations.

Dragos

Dragos is a Leader in this Magic Quadrant. The Dragos Platform is the CPS PP. It is built on the company’s expertise in industrial controls and employees with nation-level cybersecurity pedigrees, combined with proprietary intelligence-based threat detection. In addition, the

Dragos Platform is a cornerstone of the company's threat intelligence and incident response services add-ons. It is suited for organizations in the oil and gas, power and utilities, and manufacturing verticals that seek on-premises or cloud solutions, deep expertise in those environments, and the benefits of a community approach to threat intelligence and best-practice sharing.

Strengths

- **Thought leadership:** Dragos is a leading voice in CPS security. Its Year in Review and Threat Perspectives reports play a key role in educating the market on current challenges, and its relationships with the SANS Institute and government policymakers are effective marketing tools to highlight its place in the market.
- **Product strategy:** Dragos acquired Network Perception in 2024. Its NP-View solution provides important additional technical capabilities around network segmentation policy, access path analysis and facilitates low-impact deployment. The combination of approaches will enable visibility not only into what is, but also what can be inferred from assets and connections.
- **Product:** Dragos has released major updates in 2024 to include knowledge packs with more than 3,200 new detections, indicators of compromise and playbooks, as well as multiple new data collection methods (including a lightweight collector and active querying capability) and cloud-hosted options.

Cautions

- **Vertical/industry strategy:** Unlike competitors who cast a broad industry net to include healthcare, Dragos focuses primarily on the oil and gas, utilities (electric and water/wastewater) and manufacturing verticals.
- **Sales execution:** Dragos has a relatively smaller reach among vendors into channel partners that can open doors and increase indirect sales into new verticals and geographies. This may hinder its sales reach to prospects outside the industries and regions it serves.
- **Geographic strategy:** Dragos does not have the same reach at the country level as some of its competitors, and relies on a network of partners. A significant portion of its revenue comes from North America. This limits its reach to prospects for sales, deployment and support.

Forescout Technologies

Forescout Technologies is a Challenger in this Magic Quadrant. The Forescout Platform is the CPS PP, combining Forescout Technologies core capabilities with the acquisitions of SecurityMatters and CyberMDX, two CPS security providers focusing on industrial and healthcare CPS security respectively. It combines on-premises and SaaS components, such as eyeSight and eyeInspect for visibility, monitoring and compliance; eyeSegment for network segmentation; eyeControl for policy enforcement; and eyeExtend for security workflow automation. Forescout Technologies recently has emphasized innovation, developing fly-away kits and forming a strategic partnership with Microsoft. It is suited for organizations looking to combine security for CPS and IT environments into an enterprise risk and exposure management strategy.

Strengths

- **Overall viability:** Forescout Technologies has benefited from a profitable CPS PP business for the past three fiscal years and is cash-flow positive. This has enabled larger growth in employees dedicated to the CPS PP compared with competitors in engineering and customer success.
- **Marketing execution:** Forescout Technologies has a strong focus in the CPS security market, increasing the allocated marketing budget by 25% in 2024 and successfully focusing on competitive positioning by creating microsites specific to top competitors that explain differences between offerings.
- **Geographic strategy:** Forescout Technologies has comprehensive geographical reach, providing direct sales and channel partner support. Prospective buyers with global operations would benefit from this.

Cautions

- **Vertical/industry strategy:** Forescout Technologies focuses on the industrial, healthcare, government and financial industry verticals. Gartner clients do not report considering it as a vertical industry thought leader beyond marketing.
- **Sales strategy:** About half of Forescout Technologies' CPS PP engagements come from existing customers, which shows little head-to-head competition through proof of value.
- **Business model:** While Forescout Technologies enables integration or build of third parties into its platform, it does not use third parties for its core on-premises functionality.

This may present limitations in incorporating capabilities rapidly bidirectionally at a time when CPS security needs are evolving faster than ever.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant. Its FortiGate Next Generation Firewall, powered by FortiOS, is the core of its CPS PP. It's an extension of the Fortinet Security Fabric ruggedized to meet unique needs of industrial CPS environments. While its solutions were originally developed for IT, CPS security capabilities have been introduced in recent years. Its CPS PP works best when using multiple solutions, such as FortiManager, FortiAnalyzer and FortiOS; the latter is its multipurpose proprietary operating system. FortiGate can also integrate with other CPS PP vendors such as Armis, Claroty, Dragos and Nozomi Networks. The platform is suited for organizations with or migrating to Fortinet equipment.

Strengths

- **Overall viability:** As a large global network security vendor, Fortinet's investments into CPS security provide additional options for end users looking for whole-of-enterprise solutions.
- **Geographic strategy:** Fortinet supports a sizable number of geographic points of presence to serve the international CPS security market.
- **Product strategy:** Fortinet's focus on automation control vendors for innovative partnerships bodes well for the integration and compatibility of its platform within key vendor and OEM ecosystems.

Cautions

- **Market positioning:** Fortinet's CPS PP has limited organic CPS security, vertical industry and operational context, which makes it less attractive to production-centric prospects and more to network-centric prospects.
- **Business model:** Fortinet's business model centers on network security vendor consolidation and IT/CPS security convergence, as opposed to a more holistic industry and business-context-aware CPS security approach that many organizations seek.
- **Innovation:** Fortinet's focus on innovation focuses on developing strategic partnerships with OEMs and integrating with other CPS PPs. While this drives innovation from Fortinet's portfolio standpoint, it does not focus on innovation directly related to CPS security.

Honeywell

Honeywell is a Niche Player in this Magic Quadrant. Honeywell Forge Cybersecurity+ is its CPS PP, combining Cyber Insights (a network intrusion detection system acquired in 2023 with SCADAfence), Cyber Watch (central management platform), which offers an optional governance module for regulatory standards and frameworks compliance. It is among a growing list of industrial OEMs moving further into the CPS security market through the process of buying small CPS PP vendors. The platform is suited for organizations using Honeywell industrial solutions. While it is cloud-ready, most deployments today are on-premises.

Strengths

- **Customer experience:** Honeywell offers a global portfolio of both managed and professional security services. It provides CPS network assessments, penetration testing, tabletop exercises and risk assessments supported by three regional cybersecurity centers of excellence.
- **Operations:** Honeywell follows stringent security processes, focusing on product quality through code quality reviews, unit testing, integration testing, performance testing and security testing. It also offers extensive new customer activation and training programs for partners and employees.
- **Innovation:** Honeywell supports an extensive set of security frameworks, such as NIST, NIS2, OTCC (Saudi Arabia), SOCI (Australia) and NERC-CIP, that are coded into the product and provide audit-ready compliance reports via Cyber Watch.

Cautions

- **Marketing execution:** As Honeywell repositions its portfolio in CPS security, it is too early to say whether its SCADAfence acquisition will provide the necessary fuel to accelerate growth beyond the existing professional services-centric position.
- **Vertical specialization:** As an OEM and not a pure-play company, Honeywell's team is aligned to strategic business groups within the organization. Honeywell serves industries such as utilities, oil and gas, and healthcare, and focuses its CPS PP efforts to align with business unit strategies.

- **Geographical strategy:** Cyber Insights has had less visibility in the U.S. and Europe. However, Honeywell now has an opportunity to market it more aggressively in those significant markets, building on the small footprint of the Middle East- and APAC-centric SCADAfence acquisition.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its CPS PP, Defender for IoT, is part of Microsoft's enterprise cybersecurity portfolio and is primarily SaaS-based. Microsoft acquired CyberX in 2020 to accelerate its reach into CPS security. Its strategy is to bring security management of endpoint, identity, cloud, applications, security information and event management (SIEM), and CPS into one suite. The solution aligns presentation of the consolidated inventory system to the various personas within the security team. Its Defender for IoT is suited for organizations that use Microsoft across multiple enterprise security use cases, and those that are comfortable moving to an increasingly cloud-based delivery model.

Strengths

- **Geographic strategy:** With Microsoft's global reach, Defender for IoT is broadly available worldwide.
- **Product strategy:** Defender for IoT focuses on CPS-specific capabilities that include knowledge of myriad unique protocols, several asset discovery methods, OEM certifications, threat intelligence and vulnerability management. It integrates into Microsoft's enterprise suite.
- **Pricing:** Microsoft's market reach supports sales and pricing flexibility. Multiple products can be bundled competitively with other Microsoft products or bought as stand-alone. Licensing can be bought directly or through partners and resellers.

Cautions

- **Marketing execution:** Because it is only one of many solutions in the Microsoft portfolio, Defender for IoT is not prioritized in marketing. As a result, it is not as visible as its competitors when it comes to CPS security thought leadership positioning (e.g., reports, webinars or social media).
- **Vertical strategy:** As primarily an enterprise solution provider, Microsoft focuses more on horizontal product development and go-to-market strategies. As a result, it does not

focus on the special needs of any specific industry.

- **Sales strategy:** Microsoft's strategy for partnering with value-added resellers focuses on collaborating with Microsoft Security Partners who have experience in IT security and are only now expanding their service portfolios into CPS security. Most lack deep CPS expertise.

Nozomi Networks

Nozomi Networks is a Leader in this Magic Quadrant. The Nozomi Platform is its CPS PP, built on a go-to-market strategy that is based on innovation, business-centric features, customer feedback and partnerships with industrial automation companies. The management component for the solution can be on-premises (Nozomi Central Management Console) or cloud-based (Vantage). The Nozomi platform is known for focusing on both security and operational performance features. It is suited for organizations that favor technology-first partners and solutions purpose-built for CPS environments.

Strengths

- **Product:** The Nozomi Platform is feature-rich and built around components that can be bundled or individually purchased, depending on each organization's circumstances and maturity. Ten major industrial OEMs resell it.
- **Innovation:** Nozomi Networks has historically prioritized novel approaches. It has led the market in bringing AI and machine learning and cloud-based solutions to CPS environments, developing Guardian Air to detect wireless assets and Arc Embedded to deploy directly into programmable logic controllers, remote telemetry units and human-machine interfaces.
- **Geographic strategy:** Nozomi Networks has direct sales and support resources in multiple regions and an extensive global channel partner network. This allows support compliance and regulations in many countries and has fueled balanced growth globally.

Cautions

- **Vertical/industry strategy:** Nozomi Networks' focus on first-to-market continuous innovation can be a double-edged sword, as some early adopters have reported having difficulties adapting some of these innovations to their unique environments.
- **Sales strategy:** Nozomi Networks' sales resources remain in short supply for the emerging CPS security market, despite its use of a blended direct and indirect sales approach to

broaden global coverage with knowledgeable local resources. In discussions with Gartner, clients expressed difficulties finding the right match.

- **Sales execution:** Nozomi Networks' proof of concept process certified under ISO 9001 standards is designed to increase value recognition, but requires following a strict process in unpredictable custom-built environments.

OPSWAT

OPSWAT is a Niche Player in this Magic Quadrant. Its MetaDefender OT Security Platform CPS PP consists of MetaDefender products formed to address best-practice cybersecurity use cases like media, file, asset and network visibility. Known for its MetaDefender Kiosk, OPSWAT's ability to meet CPS security demands is evidenced by the market-level use cases that its products address beyond CPS PP. It acquired Bayshore Networks in 2021 and has an industrial cybersecurity heritage. Its platform is suited for organizations requiring enterprise-level functionality and partnerships.

OPSWAT did not respond to requests for supplemental information. Gartner's analysis is, therefore, based on other credible sources.

Strengths

- **Market understanding:** Founded in 2002, OPSWAT has a long history in industrial security and understands best practices, use cases and current market demands, which can be helpful to prospective buyers starting their enterprise CPS security journey.
- **Operations:** As a long-term established company, OPSWAT has mature processes to support customer needs.
- **Vertical/industry strategy:** OPSWAT has historically focused on critical infrastructure and high-security-needs organizations with sensitive missions, which could be advantageous to prospects in these sectors.

Cautions

- **Marketing strategy:** OPSWAT's marketing strategy misses highlighting its wider set of CPS security product offerings and the thought leadership it could provide in the market.
- **Market responsiveness:** OPSWAT's CPS MetaDefender portfolio of products are being adopted more slowly compared to other Niche Players in this Magic Quadrant. This is affirmed by a low volume of Gartner client inquiries and Peer Insights.

- **Business model:** OPSWAT's CPS security offerings strategy is confusing and unclear to anyone who has not already heard of or worked with the vendor. This is a missed opportunity for prospects to understand the range of offerings.

OTORIO

OTORIO is a Challenger in this Magic Quadrant. Its Titan platform is the CPS PP, retooled and rebranded to bring together product lines such as spOT (automated security and compliance risk assessment), remOT (secure remote access) and RAM2 (visibility, risk assessment, monitoring). Its central manager can be deployed on-premises or in the cloud. The Titan platform is best known for its attack graph capabilities and its ability to act as an overlay for other solutions. It is suited for organizations that want to visualize attack paths, simulate the impact of remediation actions and assess cybersecurity in the context of emerging regulations, such as NIS2 in Europe.

Strengths

- **Market responsiveness:** OTORIO is nimble and attentive to customer pain points and feedback. This has allowed it to mature its roadmap to provide operational context of vulnerability management, enhance case management and workflows, and support factory and site acceptance tests.
- **Product:** OTORIO was early in the market in bringing its patented Attack Graph Analysis engineer and simulation feature, which provides recommended exposure mitigation actions. It has gained quick traction as a result.
- **Marketing execution:** OTORIO has grown in the market via an inclusive approach, offering both proprietary data collection capabilities and an overlay solution that ingests data from other deployed CPS PP. This expands the number of demos clients can book and accelerates sales cycles. It can be attractive to end users with competitor offerings.

Cautions

- **Vertical strategy:** OTORIO does not structure its team to align to vertical industries and has no plans for any significant changes in industry alignment.
- **Geographic strategy:** As a relative newcomer to the market, OTORIO has limited global reach both directly and through partners. However, it is increasing its established presence in India, Europe and the Americas.

- **Business model:** OTORIO only refactored its offering in the last 18 months to align to a platform model and rebranded it as the OTORIO Titan platform, so its track record is not as established as others in this research.

Palo Alto Networks

Palo Alto Networks is a Challenger in this Magic Quadrant. Its Strata Network Security Platform ("Strata") is the CPS PP. It expands its security capabilities into CPS environments, using next-generation firewall (NGFW) as sensors to discover and identify assets, components, location and connections. The solution marks a departure from Palo Alto Networks' IT network heritage by investing in understanding CPS security-specific needs. This is evidenced by the industrial attributes, FDA classification, Purdue-level mapping, IEC 62443 zoning, support for private 5G security and alignment to regulations, such as NIS2. The Strata platform is suited for organizations that have, are migrating to, or are updating Palo Alto Networks equipment.

Strengths

- **Product features:** Palo Alto Networks enables easy deployment and provides mitigating controls due to the integration of Strata capabilities within its network security ecosystem. This is delivered with asset-based traffic control, policy and segmentation capabilities, as well as in-line network continuous security inspection and threat prevention.

- **Product strategy:** Palo Alto Networks introduced significant improvements in 2024 to its capabilities, particularly asset visibility, risk assessment, policy enforcement, compliance reporting and automation. Planned product additions include microsegmentation and AI-based threat hunting.

- **Innovation:** Palo Alto Networks has made significant investments in AI-supporting CPS security. This includes areas such as CPS asset identification and behavior analytics, AI with proprietary assistant, and GenAI vulnerability and risk posture information. It also delivered innovations in private LTE/5G security.

Cautions

- **Sales strategy:** Palo Alto Networks' sales strategy in support of its Strata product is unclear outside of its NextWave program with resellers. This could impact the success of its go-to-market strategy.

- **Sales execution:** Palo Alto Networks' tight coupling of Strata with its NGFW limits opportunities to sell the product to users of third-party networking equipment.
- **Vertical specialization:** Palo Alto Networks recognizes that vertical industry knowledge is uniquely important in CPS security, but not all industries it serves have the same level of thought leadership depth yet.

Radiflow

Radiflow is a Niche Player in this Magic Quadrant. Its OT/CPS security platform is an on-premises CPS PP, composed of the iSID (industrial threat detection), iCEN (centralized security monitoring), CIARA (risk management) and iSCAN (active scanning) modules. Sabanci Group acquired Radiflow in 2022, allowing it to deploy in a broader set of industries. It also recently added a paid service where analysts periodically review events generated by Radiflow's OT/CPS security platform and provide remediation recommendations. Radiflow is suited for organizations looking for a risk-driven approach to CPS security, or that operate heterogenous environments, as CIARA can ingest sensor data from competitive vendors as well.

Strengths

- **Product features:** Since Radiflow's founding in 2009, its CPS PP has evolved into a mature solution with support from a large ecosystem of partners. It recently added the ability to detect devices using railway-specific protocols.
- **Business model:** Radiflow has established a number of strategic partnerships with OEMs, resellers and global consultancy providers. This allows for enhanced service delivery, strategic collaboration and joint marketing.
- **Sales strategy:** Despite being one of the smaller players in the market in terms of headcount, Radiflow has built a comprehensive strategy for partnering with value-added resellers to enhance its market reach and service delivery.

Cautions

- **Operations:** Like some of its competitors, delivering hardware (like sensors) to remote locations frequently affects Radiflow's speed of deployment. It recommends that customers deploy servers locally so it can support installations remotely.

- **Overall viability:** Radiflow isn't profitable or cash-flow positive, as it's focusing on increasing the sales footprint and product portfolio to grow the overall business. However, industrial conglomerate Sabanci Group is committed to financing growth in the coming years.
- **Marketing strategy:** Radiflow relies on local partners for joint marketing events. While this expands its reach to other countries, these partnerships tend to dilute its messaging.

Sepio

Sepio is a Niche Player in this Magic Quadrant. Its Sepio CPS PP relies on a trafficless approach. Its direct deployment on the network infrastructure, based on a software component (Scan Engine), enables visibility into CPS network architecture Level 1 and Level 2 without monitoring or decrypting network traffic. Its real-time threat protection includes hardware-based attacks, while minimizing operational efficiency disruption. Sepio has a strategic partnership with Lenovo. Sepio is suited to organizations seeking a CPS security solution closely integrated into hardware.

Strengths

- **Product:** Sepio's trafficless approach takes away the need for traditional sensors, probes or crawlers. This supports easy deployment and low architectural complexity.
- **Sales execution:** Sepio's very high customer retention rate in 2024 is evidence of its solid proof-of-value execution leveraging lab workshop and production deployment. This allows prospects to test the solution against attack scenarios and provide in-depth insights into customers' CPS environments' activity.
- **Operations:** Sepio deployments start with a kick-off process to focus on understanding business context to optimize tagging, risk scoring and playbook development. This translation of technical requirements to business logic helps create a trusted connection between teams.

Cautions

- **Sales strategy:** Sepio is revamping its approach to sales by focusing its small team on strategic accounts and verticals, and growing channel partnerships.
- **Geographic strategy:** While its strategic partnership with Lenovo can help with sales reach, Sepio itself has limited direct country coverage outside the U.S., Portugal, the U.K.,

Singapore, Brazil, Israel, South Africa and Nigeria.

- **Innovation:** Sepio's strategic partnerships for innovation focus on technology partners such as Lenovo and NVIDIA, neither of which have a recognized pedigree in the CPS field. Its top product innovation capabilities tend to focus primarily on visibility features more than aspects, such as threat and vulnerability management and risk scoring.

Tenable

Tenable is a Niche Player in this Magic Quadrant. Tenable OT Security CPS PP was built on the 2019 acquisition of Indegy, which has CPS security and operational expertise and an asset-centric approach that harvests various levels of details of a customer environment. The public company enjoys sustained growth and an established presence in vulnerability and exposure management. Tenable is suited for organizations with a complex industrial systems footprint and that require detailed asset data and network knowledge.

Tenable did not respond to requests for supplemental information. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Product:** Tenable's OT Security product is mature in terms of core capabilities such as asset discovery and vulnerability management, which is a core focus for the vendor. It integrates with the Tenable One platform for centralized security management and reporting.
- **Geographic strategy:** Tenable has sales and support resources in multiple regions, as well as an extensive global channel partner network.
- **Operations:** Tenable is a larger company with many years of cybersecurity experience across multiple disciplines and can therefore bring a mature, diversified approach to operations when compared to other CPS PP market leaders with more limited scope.

Cautions

- **Pricing:** Tenable CPS OT Security product licensing is priced by asset count, compared with other market leaders that have moved to site-based pricing. Asset-based pricing is confusing to many prospects who are looking for a CPS PP precisely because they do not know how many assets they have.

- **Market responsiveness:** After acquiring Indegy in 2019, Tenable has not kept up with the rapid pace of innovation of many pure-play competitors, opting instead for an add-on strategy to the overall Tenable portfolio.
- **Innovation:** With its vulnerability scanner Nessus and Tenable's wider positioning in IT security, the CPS OT Security product is more centered on exposure, risk and vulnerability management than aligned to the new market needs for which competitors are innovating.

TXOne Networks

TXOne Networks is a Niche Player in this Magic Quadrant. Its EdgeOne is its CPS PP, and is a combination of hardware, firewall, IPS devices and the EdgeOne management platform. It is purpose-built for CPS environments. TXOne Networks' strategy to secure CPS uses a life cycle approach that includes system hardening, network segmentation, secure remote access and maintenance. EdgeOne's sensor deployments are predominantly on-premises installations, with 1% of deployments adopting a cloud-managed solution. It is suited for organizations like semiconductor OEMs, highly automated manufacturers and critical infrastructure sectors.

Strengths

- **Product features:** The EdgeOne platform, alongside EdgeFire and EdgeIPS appliances, combines the role of the network sensor with in-line IPS and segmentation capabilities. As a result, it does not need to rely on third-party integration to protect vulnerable devices.
- **Innovation:** TXOne Networks has developed solutions with key CPS equipment manufacturers to embed security directly into the control and automation systems global enterprises use.
- **Business model:** Purpose-built for CPS environments, TXOne Networks' solutions target first-mover global customers in verticals with significant and growing capital expenditure.

Cautions

- **Operations:** TXOne Networks' EdgeIPS network appliances may provide overlapping capabilities and higher implementation costs in end-user organizations that have invested in NGFWs.

- **Customer experience:** TXOne Networks uses a personalized service-level agreement structure. While this ensures the platform meets each client's specific requirements, it can also create inconsistency in support and customer perception. TXOne still must earn the trust of clients deploying this in their production environment.
- **Overall viability:** A significant part of TXOne Networks' CPS PP revenue depends on a few very large customers who generate a lot of revenue, posing a significant risk should they decide to change course. Unlike many U.S.-based cybersecurity companies, TXOne Networks doesn't have a large "home market," so it must work harder to build awareness and trust in markets it enters.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

As this is a new Magic Quadrant, no vendors were added.

Dropped

As this is a new Magic Quadrant, no vendors were dropped.

Inclusion and Exclusion Criteria

Providers needed to meet the following criteria to qualify for inclusion.

General requirements:

- A provider must be actively participating in the enterprise (i.e., end-user) market as evidenced by actively investing in product capabilities and directly marketing to enterprise (i.e., end-user) customers even if working with channel partners.

- A provider must demonstrate active participation in the CPS protection platform market as a pure-play provider without requiring the purchase of other products.
- Providers must meet Gartner's definition for the CPS protection platform market.
- The CPS Protection Platform must be generally available (GA) as of 15 September 2024. Gartner defines "general availability" as the release of a product to all customers. When a product reaches GA, it becomes available through the company's general sales channel, as opposed to a limited or controlled release, pre-GA, or beta version.

Global adoption and relevance:

- At least 100 unique enterprise (end-user) customers have purchased and deployed the provider's CPS protection platform in a production environment since general availability.
- Provider must offer cloud-based or managed, hybrid and on-premises.
- Paying CPS protection platform customers in at least eight of 22 industry categories (banking and financial industries; chemicals; consumer products; construction, materials and natural resources; education; energy; food and beverage processing; government, national and international; government, state and local; healthcare provider; industrial electronic and electrical equipment; industrial manufacturing; insurance; media and entertainment; pharmaceuticals, life sciences and medical products; professional services; retail and wholesale; software publishing and internet services; telecommunications; transportation; utilities; all others).
- Provider receives revenue from its CPS protection platform from at least three geographic regions (North America, Latin America, Asia/Pacific, Europe, Middle East and Africa, all others).
- At least $50 million in revenue in 2023;
  - or $5 million in revenue in 2023 and net new paying CPS protection platform customers added through July 2024 are on track to exceed 2023;
  - or vendor ranks among the Top 22 for the Customer Interest Indicator (CII) as defined by Gartner.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of the processes, systems, methods and procedures they use to be competitive, efficient and effective, and to improve their revenue, retention and reputation.

Product or Service: A vendor's core goods and services that compete in and/or serve the defined market. It includes current product and service capabilities, quality, feature sets, skills, etc. These can be offered natively or through OEM agreements/partnerships as defined in the Market Definition/Description section and detailed in the subcriteria. Evaluation factors include core product and service capabilities, the depth and breadth of functionality, and the availability of security add-ons.

Overall Viability: A vendor's overall financial health as well as the financial and practical success of the business unit. It also looks at the likelihood of the organization to continue to offer and invest in the product, as well as the product's position in the current portfolio. Evaluation factors include overall financial health and CPS PP's contribution to revenue growth.

Sales Execution/Pricing: A vendor's capabilities in all presales activities and the structure that supports them. It includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel. Evaluation factors include the execution of presales activities, the competitiveness of product and service pricing, and Gartner end-user client proposal reviews.

Market Responsiveness/Record: A vendor's ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. Also considered is the provider's history of responsiveness to changing market demands. Evaluation factors include general responsiveness to endpoint protection market trends, market share and relative share growth rate.

Customer Experience: A vendor's products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer interactions, technical support or account support. It may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc. Evaluation factors include customer relationship management, Gartner Peer Insights and Gartner client interactions.

Operations: A vendor's ability to meet goals and commitments, including the quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently. Evaluation factors include resources dedicated to CPS PP product development, certifications, internal security and end-user training programs.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	High
Customer Experience	High
Operations	High

Gartner (February 2025)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to convincingly articulate logical statements relating to current and future market direction, innovation, customer needs and competitive forces. We also evaluate how well these statements correspond to Gartner's view of the market.

Market Understanding: A vendor's ability to understand customer needs and translate them into products and services. It looks at whether a vendor shows a clear vision of its market,

listens to and understands customer demands and can shape or enhance market changes with its added vision. Evaluation factors include how vendors identify endpoint protection market trends and understand their buyers and competitors.

Sales Strategy: A vendor's ability to offer a sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service and communication. It also looks at partners that extend the scope and depth of market reach, expertise, technologies, services and the customer base. Evaluation factors include the attractiveness of product licensing and packaging options, deal strategies, vendor-supplied new client logo wins, and Gartner end-user client interactions and consideration rates.

Offering (Product) Strategy: A vendor's ability to offer an approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements. Evaluation factors include differentiated product functionality, execution against the roadmap over the past year and future roadmap.

Vertical/Industry Strategy: A vendor's strategy to direct resources (sales, product, development), skills and products to meet the specific needs of individual market segments, including verticals. Evaluation factors include performance in specific industries and strategies for vertical expansion.

Innovation: A vendor's ability to offer direct, related, complementary and synergistic layouts of resources, expertise or capital, for investment, consolidation, defensive or preemptive purposes. Evaluation factors include differentiated technical and nontechnical innovations made in the past 12 months and past innovations older than 12 months.

Geographic Strategy: A vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market. Evaluation factors include performance in international markets, product localization and geographic expansion strategies.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High

Evaluation Criteria	*Weighting*
Marketing Strategy	High
Sales Strategy	High
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	High
Innovation	High

Gartner (February 2025)

Quadrant Descriptions

Leaders

Leaders demonstrate balanced and consistent progress in relation to all Ability to Execute and Completeness of Vision criteria. They offer global and multivertical industry reach, depth, breadth and flexibility in CPS security capabilities, key knowledge of CPS environments, many partnerships and integrations, and proven management capabilities for enterprise customers. Leaders have a strong momentum in the market in terms of innovation, growth, sales and mind share. However, a Leader is not a default choice for every buyer. Customers should not assume that they must buy only from a Leader. Leaders may be less able to react quickly when Visionaries challenge the status quo in the market.

Challengers

Challengers have mature CPS protection platforms that can address the CPS security needs of the market. They also have strong sales and visibility in the market, which adds up to a better Ability to Execute than Niche Players have. Challengers, however, are often late to introduce new and emerging capabilities, lacking advanced functionality and customization,

ease of product use, a tightly integrated product and service strategy. Challengers may lack alignment with the market's direction. This affects their positions for the Completeness of Vision when compared with Leaders. Challengers are solid, efficient and practical choices, especially for customers that have established strategic relationships with them.

Visionaries

Visionaries deliver leading-edge capabilities that will be significant in the next generation of solutions, giving buyers early access to improved security and management. For example, Visionaries often offer novel approaches to solving challenges, such as with AI. Visionaries can affect the course of technological developments in the market but may not yet demonstrate a consistent track record of execution, may lack visibility in the market and often lack market share. Customers pick Visionaries for early access to innovative features or to extend an existing relationship with an IT vendor.

Niche Players

Niche Players offer solid products but rarely lead the market in terms of features and capabilities. Some vendors are Niche Players because they focus on a specific geographic region or specific market segment. Others are Niche Players because they excel in a specific use case, industry or a specific technical capability set. Niche Players can be a good choice for existing customers, customers in the vendor's target market segment or change-averse organizations in supported regions.

Context

Until recently, "OT security" was seen as a catch-all security market encompassing everything from intrusion detection/prevention services (IDS/IPS) vendors, point solution firewalls vendors, data diodes vendors, USB kiosk vendors and professional services providers. Three years ago, Gartner established specific cyber-physical security categories due to both rising end-user demand and rapid vendor innovations in response to a growing focus on CPS security.

CPS PPs, the first such category to achieve Magic Quadrant status, focus on securing CPS through a mix of discovery, visibility, prevention, protection, detection and response capabilities delivered via a single management console, either on-premises or cloud-based. Increasingly, vendors offer CPS PPs as a way to bring together network-centric and asset-

centric security approaches. This allows for multiple security capabilities to be added, such as vulnerability management, threat intelligence, visualizations, alerts, playbooks or feeds into other IT security (and inventory) tools.

Gartner sees the CPS PP market as nascent and poised for rapid growth as cyberthreat actors (nation-states and profit-motivated alike) increasingly target organizations in industries and critical infrastructure environments where CPS are prevalent. Meanwhile, end-user organizations continue to deploy CPS everywhere through automation and production transformation efforts. [1]

CPS PP customers increasingly seek tools that can be deployed in a way that will not interfere with production or mission-critical environments, but can fulfill multiple security use cases and still integrate into other IT security tools. Factors that are increasingly part of the purchase decision include:

- Fidelity of asset discovery and pedigree information
- Ability to quickly visualize topologies
- Vulnerability and exposure management
- Threat intelligence and attack path simulation
- Monitoring and fine-tuned customizable alerts
- Ease of deployment and management
- Global reach and support
- Reach to CPS beyond Purdue model-based architectures

Therefore, this Magic Quadrant goes beyond evaluating a vendor's ability to deliver core CPS PP products to assist buyers looking to achieve a holistic approach to CPS security.

Market Overview

This first Magic Quadrant for CPS Protection Platforms replaces the Market Guide for CPS Protection Platforms.

Much has changed since vendors in the CPS PPs market focused on passive asset discovery with SPAN or network TAPs. The race to ever greater fidelity of asset discovery and pedigrees has multiplied discovery methods, including:

- Safe active querying when known protocols are found
- Project file parsing
- Lightweight host-based executables
- Third-party integrations
- Use of networking equipment such as routers, switches and firewalls as sensors

In addition, innovations, partnerships and a platform-based approach now enable multiple security capabilities to be added to the platforms, such as exposure management, topology visualizations, alerts, playbooks, compliance reports, executive dashboards and benchmarking data.

The past two years have seen a marked increase in links between CPS security and IT security solutions. All CPS protection platform vendors have created partnerships and API feeds with established IT vendors of solutions such as:

- Configuration management databases
- Network access control
- Firewalls and switches
- SIEM
- Security orchestration, analytics and reporting
- Extended detection and response
- Security operations center
- Cyber asset attack surface management

The partnerships can be driven by both technology integration and go-to-market. This creates some confusion as sales executives from multiple companies approach the same end-user prospects presenting similar core capabilities packaged under different brands.

Vendors in this market display varying levels of maturity in terms of components and capabilities. For example: the breadth and depth of the protocols they support, whether and how they enrich vulnerability data, or whether they account for business and vertical industry context. Vendors also vary in their strategic decisions to continue to offer on-premises solutions versus shifting to a mix of on-premises and cloud options. Additionally, the quality and depth of ecosystem integration and support differ.

Capabilities such as DIN rail mounts for sensors are now common, and therefore are not seen as differentiating by the majority of Gartner clients. Most vendors offer partner- and vendor-delivered service wrappers to aid end users in deployments, monitoring, triage, investigation or incident response.

Trends Impacting CPS PP Market

The CPS PP market is growing due to five main trends:

Organizations are becoming aware of their blind spots. Asset-intensive organizations increasingly realize that CPS environments are value creation centers. A manufacturing company makes money by producing goods, for instance. Once largely "out of sight, out of mind," boards and C-suite executives increasingly want to know how their CPS production and mission-critical environments are protected.

Threats are on the rise and shifting. CPS are usually core value creation assets. If they go down, they halt production or derail missions. The more connected they become, the more they expand the attack surface. This increasingly makes them attractive targets for ransomware and the development of targeted malware. From operational disruptions of pipeline operators to halted machinery at shipbuilders, the number of disclosed attacks continues to rise.

More vulnerabilities are surfacing yet remain difficult to manage. Year over year, the number of disclosed vulnerabilities continues to grow. In many ways, the increasing number of vulnerabilities is linked to security researchers and vendors focusing their attention on these operational assets as they become increasingly connected. But it is also because, for a long time, OEMs regarded the problem of vulnerabilities as something to take care of downstream, postsale. Additionally, a major issue with vulnerabilities in production or mission-critical environments is the inability to patch at will, so solutions that can show alternative mitigations are needed.

Specialized security skills remain in short supply. Skills shortages in areas such as security engineering, security assessments and industrial security operations show that developing an effective security strategy that spans IT and CPS environments is difficult. This creates increasing demand for tools and playbooks.

More regulations, directives and frameworks are emerging. Due to increased threats to critical infrastructure-related organizations, governments are recognizing that the ubiquitous CPS technology landscape supporting them is key to national security and economic prosperity. As a result, new regulations, directives and frameworks are emerging.

⊕ Evidence

⊕ Evaluation Criteria Definitions

Get The App