

Magic Quadrant pour les plateformes de protection CPS

3 mars 2026 - ID G00830517 - 43 min de lecture

Par Katell Thielemann , Ruggero Contu , [et 2 de plus](#)

Les plateformes de protection des systèmes cyberphysiques, capables de détecter les actifs et leurs interconnexions dans les environnements de production ou critiques (tels que les systèmes OT, ICS, IoT et la robotique), sont devenues des outils de sécurité essentiels pour les CPS. Ce Magic Quadrant aide les responsables de la cybersécurité à identifier les fournisseurs les plus adaptés à leurs efforts en matière de sécurité des CPS.

Définition/Description du marché

Gartner définit les plateformes de protection des systèmes cyberphysiques (CPS) comme des produits qui détectent, catégorisent, cartographient et protègent les CPS dans les environnements de production ou critiques, en dehors du système informatique de l'entreprise. Elles y parviennent en analysant ou en interagissant avec les protocoles industriels et le trafic réseau opérationnel. Elles comprennent le comportement des actifs physiques et n'interfèrent pas avec le fonctionnement des CPS. Elles peuvent être déployées dans le cloud, sur site ou de manière hybride.

Gartner définit les systèmes cyber-physiques (CPS) comme des systèmes conçus pour orchestrer la détection, le calcul, le contrôle, la mise en réseau et l'analyse afin d'interagir avec le monde physique (y compris les êtres humains). Une fois sécurisés, ils permettent des performances sûres, en temps réel, fiables, résilientes et adaptables.

Le marché des plateformes de protection CPS existe parce que :

- **La surface d'attaque s'étend** : les systèmes cyber-physiques (CPS) constituent généralement des actifs essentiels à la création de valeur et, en cas de panne, peuvent

impacter la santé et la sécurité des personnes, interrompre la production ou compromettre des missions . Plus ils sont connectés, plus leur surface d'attaque s'accroît. De ce fait, ils deviennent des cibles de plus en plus prisées pour les rançongiciels, l'espionnage industriel ou les attaques à motivation géopolitique. Des perturbations opérationnelles chez les opérateurs de pipelines aux arrêts de machines dans les chantiers navals, le nombre d'attaques recensées ne cesse d'augmenter.

- **Les menaces sont en hausse** : des logiciels malveillants conçus spécifiquement pour les environnements industriels, tels que INDUSTROYER.V2 et Pipedream, font leur apparition.
- **De nouvelles vulnérabilités apparaissent** : elles restent difficiles à gérer, car les CPS ne peuvent pas être corrigés à volonté.
- **De plus en plus de réglementations, de directives et de cadres réglementaires émergent** : face à la multiplication des menaces pesant sur les organisations liées aux infrastructures critiques, les gouvernements reconnaissent que l'omniprésence des systèmes cyber-physiques qui les soutiennent est essentielle à la sécurité nationale et à la prospérité économique.
- **Les inventaires manuels d'actifs sont chronophages et coûteux** : les outils de sécurité informatique ne sont pas adaptés à de nombreux environnements CPS.

Fonctionnalités obligatoires

Les caractéristiques obligatoires pour ce marché sont les suivantes :

- Découverte, visibilité et catégorisation des actifs propres au fournisseur
- Support for modern, but also unique, industrial/industry-specific protocols (including reverse-engineered ones deployed decades ago), while not interfering with the operation of any device
- Detailed network topology and data flow diagrams
- Detailed pedigree of assets, including but not limited to the manufacturer, model, serial number, MAC and IP addresses, operating system, version, service pack, etc. — included for nested devices
- Vulnerability information and recommended actions to include contextualized CVE/CVSS scores and the likelihood of exploitability

- Threat intelligence information and simulations, as well as recommended actions, to include playbooks and policy enforcement remediation options
- Integration with IT security and asset management tools
- Risk scoring and recommended actions to include remediation options and impacts on alignment to standards

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, such as one for security teams, one for maintainers, one for engineers or one for OEMs, to support various use cases
- Machine learning capabilities to enhance asset discovery, establish behavioral baselines, improve anomaly detection and root cause analysis or fine-tune risk prioritization
- Strategic partnerships with original equipment manufacturers (OEMs) and other security vendors

Magic Quadrant

Figure 1: Magic Quadrant for CPS Protection Platforms





Vendor Strengths and Cautions

Armis

Armis is a Leader in this Magic Quadrant. It is headquartered in San Francisco, California, and offers two versions of its CPS protection platform: Armis Centrix cyber exposure management SaaS-based platform; and Armis Centrix for OT/IoT Security (on-premises).

Armis operates primarily in the U.S., followed by Europe, serving government as its largest sector, alongside healthcare, manufacturing and professional services. The company expects continued growth as organizations consolidate visibility tools into unified CPS

platforms to secure plants, warehouses and distributed sites, and support evolving federal mandates.

In 2025, Armis enhanced asset discovery with its improved Armis Centrix Smart Active Querying and nested device discovery; expanded threat monitoring with custom threat intelligence feed ingestion; and improved vulnerability management with breach and attack simulation.

In 2026, Armis plans to advance attack graph mapping, introduce agentic AI remediation for operations and deliver a CPS-specific code analysis.

In December 2025, ServiceNow announced its intention to acquire Armis; the transaction is expected to close in the second half of 2026.

Strengths

- **Deployment:** Armis has a mature outcomes-based proof of value process where presales, engineering and go-to-market teams jointly manage deployment, success criteria and executive checkpoints. Deployment services are available as professional services bundles, rather than per-hour fees.
- **Innovation:** In the past year, the company has introduced a fly-away portable version of Centrix; a programmable logic controller (PLC) module report that visualizes physical/logical architecture; automated factory acceptance testing (FAT) and site acceptance testing (SAT) testing with documentation; and Centrix Attack Path Mapping to simulate attack scenarios.
- **Training:** Training is provided through Armis University, with guided online learning, role-based paths, hands-on labs and release-specific training.

Cautions

- **Reduced CPS-specific messaging:** Recent marketing by Armis has been less focused on key CPS security use cases or specific industries and roles compared with competitors. This demonstrates an enterprisewide repositioning that could impact perceptions of Armis' commitment to the unique needs of CPS environments.
- **Market positioning:** As the platform's capabilities have evolved, Armis has shifted its market messaging several times, starting as a cyber asset attack surface management (CAASM) vendor for enterprise and cloud, then repositioning as a core CPS security vendor, and most recently as an exposure management vendor. This evolution risks

overshadowing Armis' position as a CPS protection platform provider, particularly if the ServiceNow acquisition accelerates enterprise and cloud strategies at the expense of unique CPS needs.

- **Customer support:** Client support could be improved for local languages in key markets such as France, Italy and Japan, where English proficiency is limited.

Cisco

Cisco is a Niche Player in this Magic Quadrant. Headquartered in San Jose, California, its CPS protection platform is Cisco Cyber Vision (built around the Sentryo acquisition in 2019), with Splunk added to the Cisco Industrial Threat Defense platform for cross-domain detection and remediation.

Cisco Identity Services Engine (ISE) is widely deployed in CPS environments; integration with Cyber Vision enables CPS asset data translation into security policies (Security Group Tags [SGTs]), supporting segmentation and compliance with standards such as IEC 62443.

Cisco has a strong presence in North America and Europe. The company expects continued growth in North America, driven by AI infrastructure data center buildout, and in Europe, driven by compliance requirements for critical entities under the NIS2 Directive.

Cisco is a trusted brand involved in large, high-visibility projects such as cyber resilient roadways for the 2028 Olympics.

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

Strengths

- **Geographic reach:** Cisco is a large global organization providing direct sales and support in nearly all countries through its own staff, partners, resellers and distributors with valid service contracts.
- **Operations:** The company's network of 80,000 global partners and 26,000 security partners can access a web portal with learning maps for product design and installation. Online tests are available for partner certification, and the Cisco Live on-demand library offers several thousands of videos featuring engineers presenting industry best practices, deployment options and product updates.

- **Marketing strategy:** To address limited awareness of its CPS protection platform, Cisco has launched initiatives such as Industrial Summits at Cisco Live, created industry-specific campaigns, sponsored S4x events and exhibited at the RSA Conference.

Cautions

- **Innovation:** Cisco's product enhancements lag those of competitors; in a December 2025 announcement, Cyber Vision 5.4 now supports ABB, Sauter, SEL, COTP and HTTP-UPNP protocols.
- **Vertical/industry strategy:** Cisco's cybersecurity focus within its Industrial IoT division is on manufacturing, energy and transportation. Organizations in other CPS-intensive verticals may require additional evaluation to ensure their unique needs are met.
- **Customer experience:** Gartner Peer Insights and inquiry data indicate that users report negative sentiment about Cyber Vision's licensing model and the effort required to determine whether a device is legitimate, unknown or a duplicate.

Claroty

Claroty is a Leader in this Magic Quadrant. It is headquartered in New York City, and offers two versions of its CPS protection platform: Claroty xDome as a SaaS-Based product; and Claroty Continuous Threat Detection (CTD) as its on-premises offering.

Claroty has a strong presence in North America and Europe, with growth there as well as in Asia/Pacific, driven by data center investments for AI, automation trends and regulatory pressures such as NIS2, METI/NISC and SOCI. The company's top three verticals are healthcare (bolstered by the 2022 Medigate acquisition), utilities and industrial manufacturing.

In 2025, Claroty enhanced asset discovery with Claroty Edge, visibility scoring, AI-driven inference from the new Claroty CPS Library, and improved network protection with Zone Policies and the Zone Matrix for guided segmentation.

In 2026, it plans to integrate xDome Secure Access into the platform, launch automated remediation for unmanaged medical devices and Windows-based equipment, and expand network segmentation and backup/recovery.

Strengths

- **Vertical industry strategy:** Claroty continues to focus on unique industry needs by supporting vertical-specific asset information, device purpose mapping and business-centric risks. However, its split between healthcare and industrial capabilities bears watching.
- **Market responsiveness:** Claroty shows a mature process for gathering customer needs and adapting its roadmap. In 2025, Claroty Edge evolved from a single-host utility to a scalable discovery engine deployable on Windows, Linux and Docker. It also launched an AI-powered CPS Library to enhance asset visibility and vulnerability attribution.
- **Product strategy:** The company is shifting toward an outcome-driven playbook tailored to customer environments, emphasizing uptime and resilience while aligning visibility, exposure management, threat detection and segmentation.

Cautions

- **Geographic reach:** While global, Claroty does not have the same country-level reach as some of its competitors, which can challenge clients in regions with lower presence.
- **Customer experience:** Some clients report deployment challenges and longer time to value due to initial site network architecture knowledge and scoping gaps. Claroty Edge can help with initial scoping and should be considered for dynamic discovery and to help map optimal sensor placement.
- **Sales and pricing strategy:** Claroty is moving from an all-modules, site-based pricing model for xDome Industrial to a modular approach. While intended to support value- and outcomes-based strategies, this may increase confusion for clients in the short term.

Darktrace

Darktrace is a Visionary in this Magic Quadrant. The company is headquartered in Cambridge, U.K., and its CPS protection platform is Darktrace/OT.

Darktrace's customers are primarily based in Europe, followed by the U.S., with expansion into Australia and New Zealand driven by enforcement of the Security of Critical Infrastructure (SOCI) Act. Darktrace serves a diverse range of industries, with utilities and industrial manufacturing as its leading verticals.

In 2025, Darktrace added an operational overview interface with specialized CPS asset workflows and operational alerts, plus new features that include firewall rule analysis,

patching SLA analysis, CVE mitigation costs, CSV risk exports and IT/OT crossing point visibility.

In 2026, Darktrace plans to add new asset topology and architecture diagrams within the operational overview interface to enable users to explore sites or systems independently.

Strengths

- **Business model:** Following its acquisition by Thoma Bravo, Darktrace added dedicated CRO/VP-level CPS leadership and scaled CPS product management and marketing. Strategic partnerships with the UK's National Cyber Security Centre (NCSC), OEMs, hyperscalers and security vendors extend delivery coverage and enable coordinated go-to-market collaboration.
- **Innovation:** Darktrace Cyber AI Analyst automates SOC L1/L2 alert investigations by performing event correlation, hypothesis development and narrative summarization. Darktrace has also introduced postquantum cryptography posture tagging to identify assets involved in TLS and SSH communications for emerging security and compliance requirements.
- **Product strategy:** Darktrace's strategy aligns with expanding regulatory and compliance demands, as well as postquantum readiness. The company achieved FedRAMP High ATO and ISO 42001 certifications for its CPS platform components.

Cautions

- **Market responsiveness:** In 2025, Darktrace pivoted its roadmap in key capabilities such as risk and exposure management to catch up with competitors, while those competitors have attempted to shrink Darktrace's AI-first advantage by releasing their own AI-enhanced capabilities.
- **Customer experience:** Technical support is officially available in English, Spanish and Japanese; responses in other local languages are best effort only, which may constrain customers requiring broader localized support.
- **Marketing execution:** By positioning as the platform for continuous defense, Darktrace misses the production-centric nuances required in CPS environments.

Dragos

Dragos is a Leader in this Magic Quadrant. Headquartered in Hanover, Maryland, its CPS protection platform is the Dragos Platform.

Dragos operates primarily in North America. It also has a direct presence and continues to expand its footprint in the U.K., Europe, the Middle East, Australia/New Zealand and Asia/Pacific due to increased cyberthreats targeting critical infrastructure and large-scale digital transformation. The company serves clients across several industries, primarily utilities, oil and gas, and energy.

In 2025, Dragos launched Dragos Platform 3.0, with an improved user interface for navigation and workflows, AI-powered “analyst assist,” and expanded asset discovery and profiling.

In 2026, the company will focus on segmentation policy validation and enforcement via integrations, risk scoring and expanded AI capabilities. Dragos announced a strategic partnership with Microsoft in February 2026.

Strengths

- **Business model:** Dragos broadened its reach by acquiring Network Perception, launching a dedicated U.S. public sector LLC, partnering with OEMs such as Yokogawa, and launching Dragos Platform 3.0 with enhanced capabilities.
- **Enhancement and training:** Dragos assists customers in adopting and validating functionality of new releases with an early access process. These hand-selected clients then work closely with the Dragos customer success team over seven to 10 days to provide feedback, update documentation and update the customer training portal. This portal offers over 20 structured self-service training series; instructor-led courses are also available.
- **Vertical/industry strategy:** Dragos continues to deepen its oil and gas, energy and utilities focus while methodically targeting chemical, transportation and government markets by investing in understanding unique sector threats, trends and regulations.

Cautions

- **Geographic reach:** Dragos has only recently started building dedicated regional teams and partners in select regions such as the Middle East and Asia/Pacific, including Japan.
- **Innovation:** The company has historically lagged competitors when it comes to multiple asset discovery methods (including active discovery), device nesting granularity,

workflows, network segmentation and risk scoring. Addressing these gaps may present Dragos with challenges as it works to catch up.

- **Geopolitical shifts:** As geopolitical tensions rise, deep ties in specific countries could become liabilities elsewhere. U.S. mandates for domestic technology for power grids, water systems and industrial controls systems favor Dragos domestically, but may become a liability in other markets.

Forescout Technologies

Forescout is a Challenger in this Magic Quadrant. It is headquartered in San Jose, California, and its CPS protection platform is part of the Forescout 4D Platform.

Forescout's customers are primarily in the U.S., followed by Europe and Asia/Pacific.

Forescout serves clients across several verticals; its top three are national and international governments, banking and financial companies with data centers, and healthcare.

In 2025, Forescout launched the 4D Platform, combining asset discovery, risk management, threat detection, integrations and automation under a single governance view.

In 2026, the company plans to launch an agentic AI skills-based solution, as well as eyeSentry for cloud-native capabilities and life cycle management that scale across small and dispersed sites.

Strengths

- **Operations:** Forescout is partnering with NVIDIA for high-performance on-premises GenAI and agentic applications. The Forescout 4D Platform aggregates anonymized telemetry from many devices into a secure data lake for intelligence generation. Forescout also provides e-learning with videos, slides and quizzes on platform setup, policy design and detection.
- **Market responsiveness:** Forescout responds quickly to customer requests and has established partnerships for remote access and custom-built protocol parsers for unknown protocols.
- **Sales execution/pricing:** Beyond regular proof of value engagements, Forescout offers a "test drive" environment where prospects can provision a virtual instance of the platform. Fly Away Kits are available for air-gapped assessments of critical sites and hardware evaluation.

Cautions

- **Vertical industry strategy:** While healthcare providers make up almost one-fifth of Forescout CPS protection platform revenue, a large portion comes from outside the usual verticals such as chemicals, construction or pharmaceuticals.
- **Investment strategy:** In a rapidly changing threat landscape and with end-user CPS security needs increasing, it is unclear what part of the overall 4D Platform will benefit from future product development investments because it spans both IT and CPS (OT, IoT, IoMT).
- **Customer experience:** While customers generally like the Forescout 4D Platform, some cite a drop in customer support quality.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. It is headquartered in Sunnyvale, California, and its CPS protection platform is the Fortinet OT Security Platform, built around FortiGate Next-Generation Firewalls and extending the Fortinet Security Fabric to meet industrial CPS needs.

Most of Fortinet's customers are in Europe, followed by the U.S. and Asia/Pacific. Fortinet serves a diverse range of industries, with consumer products, utilities, and industrial electronic and electrical equipment as leading verticals in the CPS security market. Its growth in the energy sector is driven by the Open Process Automation Forum.

In 2025, Fortinet enhanced CPS asset discovery with deeper protocol decoding, improved fingerprinting and behavior-based classification of programmable logic controllers (PLCs), human-machine interfaces (HMIs) and servers. Network segmentation was improved through AI-assisted recommendations and dynamic network access control (NAC)-driven enforcement.

In 2026, Fortinet plans to enhance its OT View module for detailed CPS asset and protocol information, as well as enable centralized risk scoring across sites with unified analytics integrating SIEM and SOAR.

Strengths

- **Sales execution/pricing:** Proof-of-value and pilot deployments are led by consulting systems engineers (CSEs) and CPS security specialists who understand operational context. Flexible pricing supports on-premises perpetual, on-premises subscription and

SaaS subscription models, along with enterprise agreements and unlimited-user constructs to align procurement with customer preferences.

- **Product strategy:** Fortinet's OT security platform combines asset and vulnerability data with operational instructions to prioritize CPS security tasks and reduce unnecessary alerts.
- **Operations:** The Fortinet Fabric-Ready Partner Program has grown to over 400 technology partners, with recent integrations including Armis, CrowdStrike, Equinix, Qualcomm and ServiceNow.

Cautions

- **Vertical industry strategy:** Fortinet's OT Security Platform lacks CPS industry-specific unique capabilities, limiting relevance for buyers seeking deep vertical expertise.
- **Business model:** Clients report to Gartner that they must purchase several Fortinet products to get full value, which increases costs and single-vendor dependency.
- **Market understanding:** Fortinet is still building its CPS sales resources while investing to better align with global and regional system integrators and managed security service providers. Its partner-led sales model can result in inconsistent technical depth across partners, requiring customers to validate CPS-specific skills and escalation paths for complex issues.

Honeywell

Honeywell is a Niche Player in this Magic Quadrant. Headquartered in Charlotte, North Carolina, its CPS protection platform is the Honeywell OT Cybersecurity Platform.

Honeywell's customers are mainly in the Middle East, followed by the U.S. and Asia/Pacific, with expected growth in these regions. Honeywell serves clients in several verticals; its top three are energy, chemicals and consumer products.

In 2025, Honeywell incorporated STIX-based threat feeds enriched with reputation lookups and Google Threat Intelligence for higher fidelity detections and more accurate threat prioritization.

In 2026, the company plans to integrate deception technology in industrial environments by adding decoys, honey credentials and lure assets, creating a layered defense for industrial

environments to expose attackers. Honeywell will also implement zones and conduits into the platform to group assets into logical zones and map communication paths.

Honeywell is in the process of splitting into three companies, and its CPS security business will remain with the Honeywell Process Automation business.

Strengths

- **Geographic strategy:** Honeywell is a large global organization providing direct sales and support in nearly all countries through its own staff. This enables alignment with national or regional requirements such as NERC/CIP in the U.S. and NIS2 in the EU.
- **Scale:** Pre-business split, Honeywell is a global enterprise with over 100,000 employees. Since acquiring SCADAfence, development has focused on stabilizing the product suite, achieving regional regulatory compliance (such as with the EU Cyber Resilience Act) and aligning internal architectures.
- **Operations:** Honeywell's customer success managers reach out to assigned accounts to confirm awareness of new features, explain their value and provide opportunities for questions. Existing customers benefit from dedicated deployment services to accelerate time to value.

Cautions

- **Innovation:** Honeywell is working to catch up with competitors by advancing its asset discovery capabilities with active-only and mixed modes. Recent integrations with ServiceNow CMDB, Cyolo SRA and Fortinet SIEM also reflect efforts to close the gap on competition rather than drive innovation.
- **Marketing strategy:** Honeywell's marketing efforts often focus on regional compliance-focused marketing campaigns and participation in vertical industry events that target prospects who may be interested in production and automation solutions but are not decision makers for cybersecurity investments.
- **Business model:** Technology partnerships are mainly focused on hyperscalers such as Amazon Web Services, Microsoft Azure and Google, rather than other security vendors. This approach helps with cloud alignment and scale, but limits opportunities to engage with innovative CPS security.

Microsoft

Microsoft is a Niche Player in this Magic Quadrant. Headquartered in Redmond, Washington, its CPS protection platform is Microsoft Defender for IoT. Microsoft's customers are global and span many verticals.

In 2025, Microsoft did not prioritize its CPS security portfolio, focusing instead on AI in its enterprise solutions. Competitors' adoption of Windows Server Update Services (WSUS) has made Microsoft less relevant in Windows-rich CPS environments.

Microsoft's plans for 2026 in the CPS protection platforms market are unclear, and updates mentioned in last year's Magic Quadrant have not been announced. Should Microsoft choose to become a more active player, it has the resources to acquire a larger and more established vendor than CyberX, which provided its initial CPS security capabilities.

Microsoft did not respond to requests for supplemental information or to review the draft contents of this document. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Geographic reach:** With Microsoft's global footprint, Defender for IoT is broadly available worldwide alongside many other Microsoft offerings.
- **Operations:** As a global company, Microsoft has an established infrastructure for sales and support that enterprises can leverage.
- **Pricing:** Microsoft's market reach supports sales and pricing flexibility. Defender for IoT can be bundled with other Microsoft products (with up to five Enterprise IoT devices included in Microsoft 365 E5 pricing) or bought as a stand-alone product with site-based licensing.

Cautions

- **Marketing execution:** Defender for IoT is only one of many products within the Microsoft portfolio and is not prioritized in marketing, resulting in lower visibility compared with competitors' products in CPS security.
- **Vertical strategy:** As primarily an enterprise provider, Microsoft focuses on horizontal product development and go-to-market strategies, rather than on the unique vertical industry needs of CPS environments.

- **Innovation:** Microsoft has not recently invested in new feature updates for Defender for IoT, focusing instead on bug fixes for sensors in the 25.x series. In January 2025, it retired its on-premises management console.

Nozomi Networks

Nozomi Networks is a Leader in this Magic Quadrant. Headquartered in San Francisco, California, the company offers Nozomi Vantage, its cloud-based product, and Nozomi Central Management Console, its on-premises offering.

Nozomi Networks has a balanced global client base between Europe and North America, with momentum in Asia/Pacific driven by manufacturing-heavy economies maturing their defenses. The company serves clients across multiple verticals; its top three are energy, industrial manufacturing and natural resources.

In 2025, Nozomi Networks added AI-enhanced capabilities such as natural language investigations, anomaly detection, prioritized remediation and executive-ready reporting.

In 2026, the company plans to launch an asset change management module for life cycle management, as well as an enhanced operational data context module that merges performance analytics with predictive maintenance insights.

In January 2026, Mitsubishi Electric completed its acquisition of Nozomi Networks.

Strengths

- **Market responsiveness:** Nozomi Networks uses client feedback from advisory board sessions and surveys to inform agile development teams that work directly with early adopters to refine solutions.
- **Innovation:** In 2025, Nozomi Networks added controller logic, process variables and life cycle information from OEMs to asset pedigrees. The company also introduced automated deployment wizards, a physical map using wireless triangulation and multiple AI-assisted capabilities across critical capabilities of the platform.
- **Product strategy:** From wireless asset discovery to Arc-embedded technology and value-based buying options, Nozomi Networks adapts its roadmap and go-to-market strategies to meet the rapidly evolving needs of the customer.

Cautions

- **Positioning and messaging:** Despite assurances from Nozomi Networks that the Mitsubishi Electric acquisition will not affect its independence, Gartner inquiries show that clients and competitors will closely monitor for any shifts.
- **U.S. public sector reach:** As the U.S. federal market grows and mandates Authorizations to Operate (ATOs) under FedRAMP, Nozomi Networks is still working toward achieving a Moderate-level ATO and lags several key competitors in this area.
- **Sales strategy:** The “partner-first” sales approach discourages direct transactions to enhance partner value. While this strategy can accelerate entry into new accounts, industries and regions, it risks diluting the client intimacy that has fueled the company’s innovation.

Palo Alto Networks

Palo Alto Networks is a Niche Player in this Magic Quadrant. It is headquartered in Santa Clara, California, and its CPS protection platform is Device Security, delivered as part of Strata Cloud Manager.

Palo Alto Networks has a strong presence in North America, followed by EMEA and Asia/Pacific, and expects continued growth through its integrated platform strategy, delivering CPS security capabilities alongside broader solution sets.

As a global company, Palo Alto Networks serves a broad range of verticals; however, not all industries receive the same level of thought leadership depth within its CPS protection platform, with the strategy focused primarily on government, healthcare and manufacturing.

Palo Alto Networks did not respond to requests for supplemental information. Gartner’s analysis is therefore based on other credible sources.

Strengths

- **Operations:** Palo Alto Networks offers comprehensive training and certification through Palo Alto Networks Education Services, including digital learning, instructor-led training and a cybersecurity academy.
- **Geographic reach:** As a large global organization, Palo Alto Networks provides direct sales and support in nearly all countries and maintains a network of global partners.
- **Broad portfolio:** The company has solid financials and an established global presence in cybersecurity, reporting \$9.2 billion for fiscal year 2025 and serving 70,000

organizations.

Cautions

- **Marketing execution:** Palo Alto Networks has reduced dedicated marketing focus on CPS security. In 2025, its press release activity specific to CPS security was considerably lower than that of competitors.
- **Innovation:** The company significantly decreased the release of features specific to its CPS protection platform in 2025 compared with 2024.
- **Vertical industry strategy:** By delivering CPS protection platform functionality as part of a broader enterprise-centric product set, Palo Alto Networks does not prioritize vertical-specific CPS security capabilities.

Tenable

Tenable is a Challenger in this Magic Quadrant. Headquartered in Columbia, Maryland, the company offers two versions of its CPS protection platform: Tenable One as its SaaS-based platform; and Tenable OT Security and Tenable Security Center as its on-premises offerings.

Tenable's customers are mainly in the U.S., followed by Europe, Canada and Mexico. Tenable serves a diverse range of industries and is expanding into hyperscale data center infrastructure by deepening the capabilities of its active queries across CPS protocols to identify unauthorized changes to HVAC and power systems.

In 2025, Tenable enhanced its CPS security offerings with agent-based deployment and centralized administration capabilities for bulk upgrades, policy pushes and signature updates across sites from a single console.

In 2026, it plans global subnet management for asset tracking and unauthorized traffic detection, as well as a CPS discovery engine for the vulnerability management products in its portfolio, including Tenable Vulnerability Management and Tenable Security Center.

Strengths

- **Geographic reach:** Tenable has broad geographic coverage through direct sales and support in key markets across North America, Europe and Asia/Pacific, complemented by extensive channel partner reach for global scalability.

- **Mature proof-of-value process:** Tenable uses a structured, phased methodology that respects unplanned or scheduled freeze days and safety change windows.
- **Targeted marketing:** Tenable has updated its messaging to place end users at the center, with guided demos and self-diagnosis.

Cautions

- **Vertical industry strategy:** Tenable's approach remains platform-led rather than deeply verticalized, emphasizing reusable cross-industry capabilities over differentiated vertical-specific packaging or go-to-market strategies.
- **Customer experience:** Customers cite a steep learning curve and navigation challenges for nonspecialists. Large environments require significant resources and dedicated personnel to operate effectively.
- **Innovation:** While Tenable demonstrates ongoing progress, it is still catching up in advanced CPS threat detection, as competitors have built detection mechanisms with AI-driven behavioral baselining and protocol-aware process semantics.

TXOne Networks

TXOne is a Niche Player in this Magic Quadrant. It is headquartered in Taipei, Taiwan. Its CPS protection platform is TXOne EdgeOne, a hardware-based solution deployable via in-line and offline modes through EdgeIPS and EdgeFire hardware appliances.

Most of TXOne's clients are in Asia/Pacific and Japan, with 2025 growth driven by semiconductor industry requirements for prevention-first protection. Key verticals include industrial electronics and industrial manufacturing.

In 2025, TXOne added network visualization, enhanced asset fingerprinting, improved threat detection aligned with the MITRE ATT&CK for ICS framework, and multisite management capabilities.

In 2026, the company plans to introduce AI-supported IEC 62443 zone design recommendations, a risk scorecard dashboard with remediation progress tracking, and ServiceNow Configuration Management Database (CMDB) integration.

Strengths

- **Operational intelligence:** TXOne gathers real-time metadata (never payloads) to understand clients' product usage and update their roadmaps and training strategies accordingly.
- **Innovation:** Recent launches include TXOne Deployment Assistant for batch device provisioning across hundreds of devices; AI-powered auto rule learning for automated rule generation based on traffic analysis; and Stellar Cyber-Physical System Detection and Response (CPSDR) for sequential traffic flow analytics.
- **Product strategy:** In 2025, TXOne enhanced visibility, segmentation, threat detection and management capabilities. The updates included custom TCP/UDP port mapping for OT protocols on nonstandard ports, as well as SageOne integration for unified orchestration across edge network security and Stellar endpoint protection.

Cautions

- **Market reach:** A significant portion of TXOne's CPS protection platform revenue depends on a few very large customers; because it has other CPS security solutions, only a small percentage of full-time employees are dedicated to the platform.
- **Sales strategy:** TXOne has a small direct and indirect sales footprint in key markets such as the U.S., where it is underpenetrated.
- **Vertical industry strategy:** While diversifying with other product lines, TXOne's CPS protection platform footprint remains dominated by the semiconductors industry.

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

No vendors were added, as no vendors new to the CPS protection platform market met the inclusion criteria for this Magic Quadrant.

Dropped

For this Magic Quadrant, the following vendors have been dropped:

- **Opswat**, as it did not meet industry reach and geographic reach criteria.
- **Otorio**, as it has been acquired by Armis since the publication of the previous Magic Quadrant and Critical Capabilities research.
- **Radiflow**, as it did not meet industry reach, geographic reach and revenue criteria.
- **Sepio**, as it did not meet customer count, industry reach and revenue criteria.

Inclusion and Exclusion Criteria

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

General requirements:

- Each 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 only via channel-based sales.
- Each provider must demonstrate active participation in the CPS protection platform market as a pure-play provider without requiring the purchase of other products or services.
- Each provider must meet Gartner's definition for the CPS protection platform market.
- The CPS protection platform must be generally available (GA) as of 25 November 2025. 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 must have purchased and deployed the provider's CPS protection platform in a production environment since general availability.

- Each provider must offer cloud-based or managed, hybrid and on-premises deployment options.
- Each provider must have at least 10 paying CPS protection platform customers in at least eight of 22 industry categories: banking and financial industries; chemicals; consumer products; construction, materials & natural resources; education; energy; food & beverage processing; government national & international; government state & local; healthcare provider; industrial electronic & electrical equipment; industrial manufacturing; insurance; media & entertainment; pharmaceuticals, life sciences & medical products; professional services; retail & wholesale; software publishing & internet services; telecommunications; transportation; utilities; all others.
- Each provider must receive revenue from its CPS protection platform from at least three geographic regions, with at least two of them at or above 10% (North America, Latin America, Asia/Pacific, Europe, the Middle East and Africa [EMEA], all other).
- Each provider must have accrued at least \$50 million in revenue in 2024, or have generated above \$5 million in revenue and, through July 2025, be on track to add more net new paying CPS protection platform customers (logos) than in 2024.

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. This criterion 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 the CPS protection platform'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, and service-level agreements. 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 protection platform development, certifications, internal security and end-user training programs.

Ability to Execute Evaluation Criteria

<i>Evaluation Criteria</i>	<i>Weighting</i>
Product or Service	High
Overall Viability	Medium

<i>Evaluation Criteria</i>	<i>Weighting</i>
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (March 2026)

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. This criterion 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. This criterion 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, and 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

<i>Evaluation Criteria</i>	<i>Weighting</i>
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	High

<i>Evaluation Criteria</i>	<i>Weighting</i>
Innovation	High
Geographic Strategy	Medium

Source: Gartner (March 2026)

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 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 e 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 market visibility, which contributes to a better Ability to Execute than that of Niche Players. Challengers, however, are often late to introduce new and emerging capabilities, and may lack advanced functionality and customization, ease of product use, and a tightly integrated product and service strategy. Challengers may also lack alignment with the market's direction, which affects their positions for 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 influence the course of technological developments in the market, but may not yet demonstrate a consistent track record of execution, may lack market visibility, and often have limited market share. Customers choose 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

Cyber-physical systems (CPS) protection platforms — the first CPS security category to achieve Gartner Magic Quadrant status — focus on securing CPS through a mix of discovery, visibility, prevention, protection, detection, reporting, alerting and response capabilities delivered via a single management console, either on-premises, cloud-based or in hybrid model.

Increasingly, vendors offer CPS protection platforms as a way to bring together network and asset-centric security approaches, exposure management, risk scoring and compliance reporting. 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 protection platform market as maturing and continuing to grow rapidly 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, which further expands the attack surface.

CPS protection platform 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 vendors' ability to deliver core CPS protection platform products; it also assists buyers seeking a holistic approach to CPS security.

Market Overview

Much has changed since vendors in the CPS protection platforms market focused on passive asset discovery with Switched Port Analyzer (SPAN) or network Test Access Points (TAPs). Market demand for higher 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 few 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:

- IT service management (ITSM)
- Configuration management databases (CMDB)
- Network access control (NAC)
- Firewalls and switches
- Security information and event management (SIEM)
- Security orchestration, analytics and reporting (SOAR)
- Security operations centers (SOCs)
- Cyber asset attack surface management (CAASM)

They have also deepened partnerships with CPS secure remote access pure-play vendors if they do not have the capabilities in-house, as well as with OEMs such as Siemens, Schneider Electric, Yokogawa, or Mitsubishi Electric.

The partnerships can be driven by both technology integration and go-to-market considerations, but they underscore the central role CPS protection platforms play as fit-for-purpose solutions for CPS environments. On the flip side, all these partnerships can create some confusion, as sales executives from multiple companies may 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, differences exist in whether they discover wireless assets, the breadth and depth of the protocols they support, whether and how they enrich vulnerability data, and whether they account for business and vertical industry context. Vendors also differ in their strategic decisions to continue offering on-premises solutions versus shifting to a mix of on-premises and cloud options. Additionally, the quality and depth of ecosystem partner integration and support may vary.

A recent development that no vendor can escape is AI. Whether used to augment asset details, model attack paths, enable natural language queries to probe for the existence of vulnerabilities, or create custom reports, every CPS protection platform vendor is embedding some form of AI into their offerings.

Trends Impacting CPS PP Market

The CPS protection platform market is growing due to several key trends:

Organizations are becoming aware of their blind spots. Asset-intensive organizations increasingly realize that CPS environments are value creation centers. For instance, a manufacturing company makes money by producing goods. A utility company can only fulfill its mission if services are delivered. 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 or production impacts at a large automotive company in the U.K. impacting the country’s GDP, 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. 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.

New industry verticals are emerging. For example:

- Explosive AI demand is driving rapid interest in data centers, where CPS support high-value electrical, cooling and building management systems with high uptime SLAs.
- The retail industry is automating rapidly, connecting point-of-sales (POS) systems to CPS that support inventory and antifraud use cases.
- Le secteur des transports doit composer avec une liste croissante de préoccupations liées à la signalisation et au péage intelligents des routes, aux opérations maritimes et portuaires et à la gestion des bagages dans les aéroports.

Levées de fonds et fusions-acquisitions. Face à la demande croissante des entreprises cherchant à réduire leurs risques cybernétiques liés aux systèmes cyber-physiques et à l'arrivée constante de solutions innovantes sur le marché, les cinq dernières années ont été marquées par un flux régulier de levées de fonds, ainsi que par une augmentation du nombre de valorisations liées aux fusions-acquisitions. L'annonce récente du rachat d'Armis par ServiceNow a établi un nouveau record, valorisant l'entreprise à 7 milliards de dollars.

Instabilité géopolitique. La cybersécurité s'inscrit de plus en plus dans les tendances technonationalistes, certains pays imposant le recours à des fournisseurs nationaux ou interdisant celui de fournisseurs provenant de certains pays jugés préoccupants. Le rôle essentiel des systèmes cyber-physiques (CPS) dans le maintien des infrastructures critiques risque d'accentuer cette tendance.

⊕ Preuve

⊕ Définitions des critères d'évaluation

© 2026 Gartner, Inc. et/ou ses filiales. Tous droits réservés. Gartner est une marque déposée de Gartner, Inc. et de ses filiales. Cette publication ne peut être reproduite ni diffusée sous quelque forme que ce soit sans l'autorisation écrite préalable de Gartner. Elle présente les opinions du département de recherche de Gartner, qui ne doivent pas être interprétées comme des faits avérés. Bien que les informations contenues dans cette publication proviennent de sources jugées fiables, Gartner décline toute responsabilité quant à leur exactitude, leur exhaustivité ou leur pertinence. Bien que les recherches de Gartner puissent aborder des questions juridiques et financières, Gartner ne fournit aucun conseil juridique ou financier et ses recherches ne doivent pas être interprétées ni utilisées comme tels. Votre accès à cette publication et son utilisation sont régis par la [Politique d'utilisation de Gartner](#). Gartner est fier de sa réputation d'indépendance et d'objectivité. Ses recherches sont réalisées de manière indépendante par son département de recherche, sans intervention ni influence de tiers. Pour plus d'informations, veuillez consulter les « [Principes directeurs relatifs à l'indépendance et à l'objectivité](#) ». Les recherches de Gartner ne peuvent être utilisées comme intrants, ni pour la formation ou le développement de l'intelligence artificielle générative, de l'apprentissage automatique, des algorithmes, des logiciels ou des technologies connexes.

[À propos](#) [Carrières](#) [Rédaction](#) [Politiques](#) [Index du site](#) [Glossaire informatique](#) [Réseau de blogs](#)
[Gartner](#) [Contact](#) [Envoyer des commentaires](#)

The Gartner logo, consisting of the word "Gartner" in a blue, sans-serif font with a stylized dot on the letter 'i'.

© 2026 Gartner, Inc. et/ou ses filiales. Tous droits réservés.