Market Guide for Operational Technology Security

Published 7 November 2023 - ID G00777207 - 19 min read

By Analyst(s): Katell Thielemann, Wam Voster, Ruggero Contu

Initiatives: Cyber Risk; Build and Optimize Cybersecurity Programs

Security for operational environments has evolved beyond a catch-all market into specific categories that support changing threats, security practices and vendor dynamics. Gartner is retiring the Market Guide for Operational Technology Security, and providing an overview of the new market dynamics.

Overview

Key Findings

- Legacy operational technology continues to interconnect with IT systems, and newly designed cyber-physical systems are being deployed with a growing variety of communications protocols. This forces security and risk management leaders to broaden their security strategies to include CPS security.
- SRM leaders have more tools and service options than ever, as distinct categories and industry-specific tools emerge to target specific use cases.
- The vendor landscape is also rapidly evolving; as platform-based solutions become a center of gravity, vertical-specific vendors emerge, professional services providers add OT security capabilities, mergers and acquisitions continue, and security vendors create bridges.

Recommendations

SRM leaders responsible for the cyber risks of OT systems security should:

- Anchor security efforts to operational resilience in the face of mounting threats by adopting an integrated security strategy beyond legacy systems. Include all CPS — e.g., OT, Internet of Things, industrial IoT or Internet of Medical Things — and IT in a joint governance model.
- Assess where they are on the typical end-user OT/CPS security journey, and lay the groundwork to accelerate efforts past asset discovery.

- Inventory the security solutions used in their organizations, and evaluate the growing list of solutions in new categories now on the market for best fit.

Strategic Planning Assumption

By 2027, 75% of security teams will have on-boarded at least five tools to manage cyber-physical systems (CPS) security in operational, production or mission-critical environments, which is a major increase compared with one or two they might use today.

Market Definition

This document was revised on 10 November 2023. The document you are viewing is the corrected version. For more information, see the Corrections page.

Gartner defines operational technology (OT) as "hardware and software that detects or causes a change, through direct monitoring and/or control of industrial equipment, assets, processes and events" (see Note 1).

OT security includes practices and technologies used to protect them, but these practices and technologies are now evolving into distinct categories to address the growing threats, security practices and vendor dynamics.

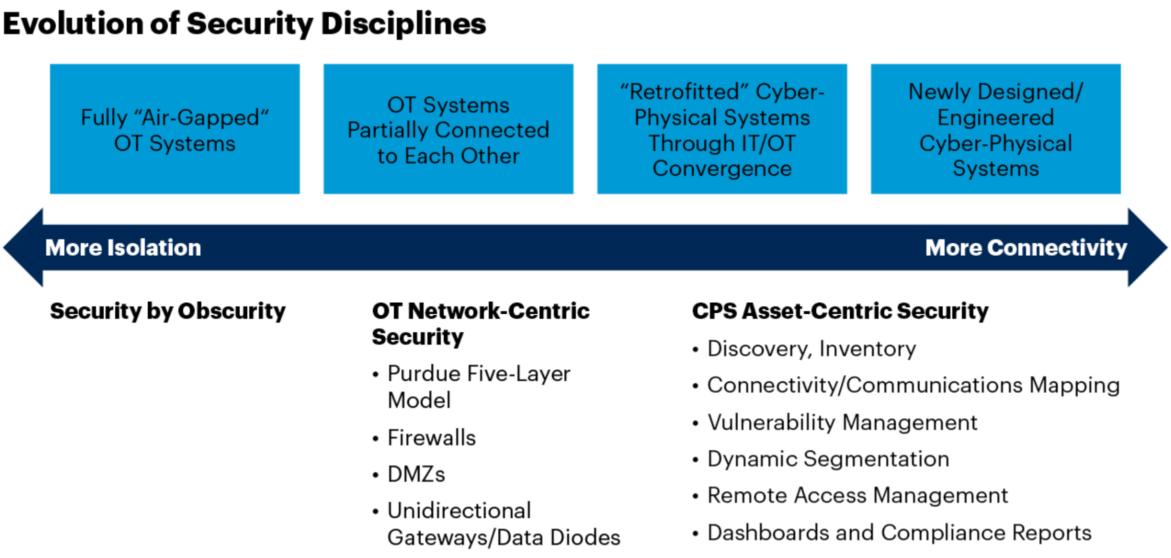
> Gartner is retiring the Market Guide for Operational Technology Security. The number of solutions now available to end-user organizations has greatly increased during the past five years, and they have evolved into categories that fulfill various needs. As a result, a single, amorphous market category of "OT security" is no longer helpful. New Market Guides will be created as categories grow, starting with the Market Guide for CPS Protection Platforms released in June 2023.

Market Description

Following the same pattern as the evolution of IT security, the OT security market is rapidly changing to the point where it is becoming meaningless to call it a single market, as threats, complexity and innovative technologies evolve.

The traditional niche OT security market emphasized products focused on legacy industrial systems and operations-only networks and firewalls. The market is now shifting rapidly, as new tools and services with an ever-increasing array of features become available. As OT continues to connect to IT systems, and newly designed CPS are deployed, OT management, governance, infrastructure and security are evolving (see Figure 1).

Figure 1: Evolution of Security Disciplines



Evolution of Security Disciplines

Fully "Air-Gapped" OT Systems

OT Systems Partially Connected to Each Other

"Retrofitted" Cyber-Physical Systems Through IT/OT Convergence

Newly Designed/ Engineered Cyber-Physical Systems

More Isolation

More Connectivity

Security by Obscurity

OT Network-Centric Security

- Purdue Five-Layer Model
- Firewalls
- DMZs
- Unidirectional Gateways/Data Diodes

CPS Asset-Centric Security

- Discovery, Inventory
- Connectivity/Communications Mapping
- Vulnerability Management
- Dynamic Segmentation
- Remote Access Management
- Dashboards and Compliance Reports

Source: Gartner
743794_C

The evolution of security disciplines:

- **Security by Obscurity —** In many organizations, OT was initially deployed in a custom-made manner to do specific tasks, and security was not central to the design and architecture of systems. It has since been found to be largely a fallacy. However, the idea that those systems were fully "air gapped" has led to a "security by obscurity" mindset, with no security focus, out of the belief that no one was likely to discover and target these systems.
- **OT Network-Centric Security —** As systems began connecting to each other and then to enterprise IT systems, a network-centric security discipline emerged, anchored around the Purdue model and supported by firewalls, demilitarized zones (DMZs) and unidirectional data diodes.

- **CPS Asset-Centric Security** — As the complexity and variety of old and new assets have become a reality for many organizations, so has the recognition that new security practices are needed. Organizations are recognizing that OT is only one flavor of terms that end users use for the variety of cyber-physical assets with which they must now contend. This is in addition to the Internet of Things (IoT), industrial IoT (IIoT), smart buildings and even medical device technologies. For an increasing number of users, OT stands for "Old Tech," as they deploy more automation. All of these technologies have one thing in common: They do more than process data — they straddle the cyber and physical worlds. The ability to discover and inventory them is opening the door to asset-centric security, as well as several new categories of solutions.

Historical IT versus OT/engineering teams functional differences are becoming a liability when security is involved, as polarized priorities will help the attackers. Due to design, age or function, the unique requirements of OT systems now add to IT security concerns in ways that can no longer be ignored. Modernization efforts bring risk, reliability and safety discussions to the forefront.

Market Direction

Threats Are on the Rise and Shifting

Operational, production and mission-critical systems are core offerings for value and revenue creation in private industry, and for mission success in the public sector. If they go down, operations halt. The more connected they become, the more they expand the attack surface. This makes them increasingly attractive targets for ransomware and for the development of targeted malware.

Security company Waterfall Security Solutions reported 57 cyberattacks on industrial systems (out of 218 incidents they tracked in 2022), which had real world physical effects. [1] In addition, malware specifically designed to target industrial operations, such as Industroyer2 and Pipedream are emerging. [2,3] They are increasingly designed with a focus on flexibility, new functionality and ease of deployment. Offerings in the market have evolved to offer threat intelligence (TI) feeds and targeted threat research from in-house vendor teams. Recently, armed conflict in Ukraine and Israel has resulted in combined kinetic and cyber attacks on critical infrastructure.

More Vulnerabilities Are Surfacing

Year over year, the number of vulnerabilities disclosed in operational systems continues to grow. According to the ICS Advisory Project, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued 240 advisories affecting industrial control systems alone from 1 January to 24 August 2023. [4] This does not account for vulnerabilities in consumer, enterprise or nonindustrial-grade CPS components.

In many ways, the increasing number of vulnerabilities is due to more security researchers and vendors focusing their attention on these operational assets. However, it is also because, for a long time, manufacturers have not designed cybersecurity into their products by design and, by default, regarding the problem of vulnerabilities as something to take care of downstream (i.e., postsale).

Because a major issue with vulnerabilities in production or mission-critical environments is the inability to patch at will (see Note 2), offerings in the market are evolving to support careful remediation and offer guidance on alternative compensating controls.

Specialized Security Skills Remain in Short Supply

Skills shortages in such areas as production security engineering and industrial security operations remain acute. This has resulted in increasing demand for professional and consulting services that provide security assessments, remediation, specialized tools deployment, incident response or secure automation. Offerings in the market have evolved to improve ease of deployment for tools, digital-native friendly user interfaces (UIs) and playbooks, and services ranging from staff augmentation to managed services.

More Regulations, Directives and Frameworks Are Emerging

The rise in attacks against critical infrastructure-related organizations has accelerated the recognition that technology in operational environments in those sectors is key to national security and economic prosperity. As a result, new regulations, directives and frameworks are emerging, including:

- Directives from critical infrastructure sector risk management agencies (SRMAs) in the U.S. [5] —
  - The Transportation Security Administration (TSA) has been particularly active [6]

- A new U.S. Cyber Incident Reporting law for operators of critical infrastructure (see Quick Answer: What the Cyber Incident Reporting for Critical Infrastructure Act of 2022 Means for Security and Risk Leaders)
- In the European Union, the NIS2 directive and the EU Cyber Resilience Act [7,8]
- In Saudi Arabia, Item 3 of Article 10 NCA's mandate per Royal Decree number 57231, dated 10/11/1439AH [9]

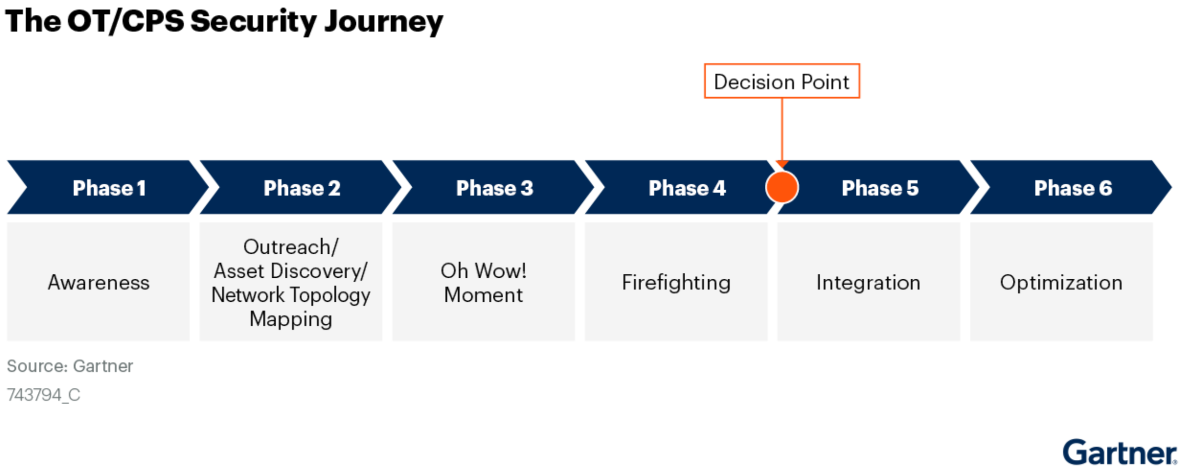
Market Analysis

A few important vectors directly affect the evolution of the OT security market.

Organizations Are Pushing Past the Awareness Phase

Gartner has documented the typical security journeys that organizations go through (see Figure 2).

Figure 2: The OT/CPS Security Journey



Source: Gartner
743794_C

The journey aligns with six key phases:

- **Phase 1. Awareness:** In this phase, new prioritization and focus arise, typically driven by a breach that causes bottom-line impacts; board, C-suite and CIO involvement; or digital transformation initiatives that force organizations to revisit their risk positions. Also, warnings and bulletins from government agencies, such as the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) and the European Union Agency for Cybersecurity (ENISA), are increasing. Vertical-specific compliance requirements are involved, and the team usually tapped to figure it out is IT security, which brings IT-centric biases to the task and quickly realizes it is stepping into new and foreign environments where it isn't always welcome.

- **Phase 2. Asset Discovery/Network Topology Mapping:** Once an organization reaches the Awareness Phase, the next step is to figure out what connected systems exist in the environment and what the risk profiles look like. This usually involves reaching out to the teams supporting OT assets to find out what enterprisewide IT architecture and OT security policies and procedures exist. Reality usually quickly sets in that there is a lack of security visibility into "brownfield" operational environments that have been connected to improve productivity or control costs. There is also a lack of security controls in new CPS deployed via IIoT/IoT efforts managed by business units seeking more digital transformation. The next step often involves a proof of concept (POC) effort, with one or more CPS protection platform solutions.

- **Phase 3. The "Oh Wow!" Moment:** Invariably, these POCs become eye openers. For example:
    - Unmanaged assets are connected everywhere.
    - Operational systems are deployed with their default credentials unchanged.
    - OT networks that were initially designed to be highly segregated have become flatter than realized.
    - Access to ports on all kinds of systems in all kinds of remote locations is wide open.
    - Original equipment manufacturers (OEMs) are accessing the machines they sold remotely, and no one is managing this.
    - Disclosed vulnerabilities on old OSs have never been evaluated for possible patching.
    - The functional silos between separate security disciplines (e.g., cybersecurity, physical security, supply chain security, product security, health and safety) are creating seams that bad actors can exploit.
    - Operational environments in which security is lacking are centers of value creation for most organizations; however, no centralized governance exists to help make sense of it all. Recognition develops that roles and responsibilities for a wide variety of (security-related) processes and decisions have never been made clear, let alone agreed-on.

- **Phase 4. Firefighting:** In this phase, actions are prioritized. Governance gaps can be tackled with the creation of steering committees, such as when risk assessments can uncover high-value assets where security efforts need to be fast-tracked. The focus is usually on network segmentation reviews, secure remote access, patching when practicable or incident response plan updates. However, efforts to mitigate security concerns are often seconded to business and production needs, and this phase can be lengthy.

For some organizations, reaching Phase 4 enables a decision point. For some, it triggers a shift to a steady state, as they decide that they have neither the need, nor the resources, to push on to Phase 5. For others, the activities deployed in Phase 4 create a new awareness trigger, and they decide that integration and optimization phases offer rewards not just for security, but for the organization as a whole.

- **Phase 5. Integration:** This is the stage in which OT security is integrated and coordinated with IT and other security governance, monitoring and reporting. Previously siloed security disciplines converge under a newly created chief security officer (CSO) role. For example, security tools converge and offer broader situational awareness, and security policies are updated to account for non-IT-specific environments. This phase may include integrating with a security information and event management (SIEM) or security orchestration automation and response (SOAR) solution. Organizations may start moving toward end-to-end broader security approaches for their operational or mission-critical environments that mirror IT security practices, and include incident response, TI, threat hunting or deception. This mirroring does not imply a direct equivalency. OT environments remain unique, and IT security disciplines must still be tailored accordingly.

- **Phase 6. Optimization:** Security convergence is bearing fruit, and more data is emerging from the OT-centric security tools deployed. Organizations realize that the unprecedented visibility and data they can now access could benefit security teams with additional features, as well as nonsecurity teams in operations, maintenance, procurement or engineering. Gartner interactions show that some organizations have used data from CPS protection platforms to feed predictive maintenance efforts, for example, or to inform purchasing decisions, based on asset usage metrics.

CPS Protection Platforms Become a Center of Gravity

As production/service delivery assets increasingly connect to each other and to IT systems, and as IoT, IIoT, smart buildings or smart factory automation efforts accelerate, organizations must secure all types of CPS in their environments. And categories of tools are evolving to support them. One of the leading categories is CPS protection platforms (see Market Guide for CPS Protection Platforms).

The modularity associated with platform-based features and functionalities is attractive to end users, who can consume them based on their current needs and maturity. The platform business model also means that vendors can increasingly offer software as a service (SaaS)-based pricing models, which opens the doors to more cloud-based and analytics-centric solutions. Some vendors now offer passive and selectively active on-premises, as well as cloud-based solutions.

Attributes of these platforms include:

- Discovery, visibility and categorization of CPS assets

- Detailed pedigree of assets
- Support for proprietary industrial protocols
- Detailed network diagrams and data flows
- Vulnerability information
- TI management
- Integration with IT security tools

Other emerging categories include:

- CPS secure remote access solutions
- CPS cyber-risk quantification platforms
- CPS deception solutions
- CPS product security/security-by-design/security-by-default solutions
- CPS network-centric solutions (e.g., cloaking and microsegmentation)
- CPS security services
- CPS unidirectional data flow solutions

Vertical-Specific Vendors Are Emerging

Some vertical industries, such as healthcare, defense, and rail or maritime transportation, have unique security needs, due to the types of systems and protocols deployed, their unique sales cycles, or the safety and security cultures. Some vendors are embracing this uniqueness. They will market with solutions tailored to these vertical-specific environments. With personnel handpicked for their knowledge. Cloud providers eager to expand their market presence into operational environments are also targeting industry partnerships and showcasing the security practices embedded in their solutions.

Security Vendors Continue to Build Bridges That Sometimes Lead to Acquisitions

API connectors have accelerated the opportunity for strategic partnerships with security vendors wherever they focus across the organization. All CPS protection platform vendors have strategic partnerships with established IT security product vendors, for example. Examples include:

- Nozomi Networks partnering with IBM Security
- Radiflow partnering with RSA
- SCADAfence (now part of Honeywell) partnering with Check Point Software
- Claroty partnering with Rapid7
- Armis partnering with SentinelOne
- Dragos partnering with CrowdStrike

Other partnerships exist in the more-traditional technology and system integrator (SI) realm. Examples include:

- Cylera partnering with Kudelski Security
- Forescout partnering with Accenture
- Phosphorus Security partnering with Optiv
- OTORIO partnering with Atos

Relationships with industrial equipment manufacturers are also increasingly important. Examples include:

- Claroty and Yokogawa
- Nozomi Networks and Siemens
- Fortinet and Schneider Electric
- Dragos and Emerson

Should partnerships between OT manufacturers and security vendors lead to acquisitions, end users may need to think about interoperability. Most industrial environments are supported by systems from a variety of OEMs. The concern is what would happen if the equipment of one of these manufacturers could only be monitored by the CPS protection platform that has become a product of the same manufacturer.

Representative Vendors

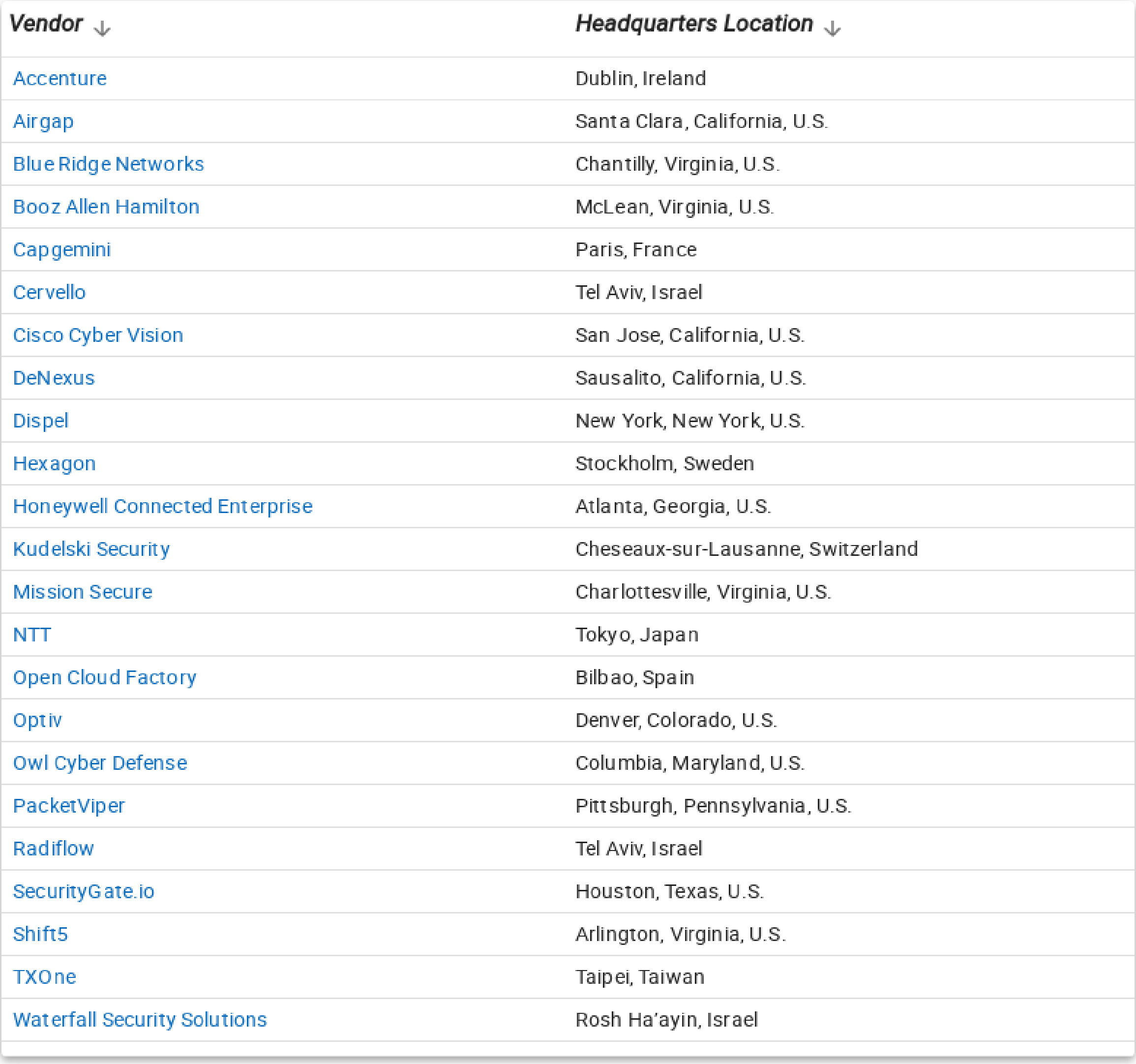
The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

The vendors listed in this Market Guide do not imply an exhaustive list, particularly as this Market Guide is being retired as specific categories are emerging. This section is intended to provide more understanding of the market and its offerings. (For a detailed list of 20 CPS protection platforms vendors, the current leading category, see Market Guide for CPS Protection Platforms and Table 1).

Table 1: Vendor List

(Enlarged table in Appendix)



Vendor ↓	Headquarters Location ↓
Accenture	Dublin, Ireland
Airgap	Santa Clara, California, U.S.
Blue Ridge Networks	Chantilly, Virginia, U.S.
Booz Allen Hamilton	McLean, Virginia, U.S.
Capgemini	Paris, France
Cervello	Tel Aviv, Israel
Cisco Cyber Vision	San Jose, California, U.S.
DeNexus	Sausalito, California, U.S.
Dispel	New York, New York, U.S.
Hexagon	Stockholm, Sweden
Honeywell Connected Enterprise	Atlanta, Georgia, U.S.
Kudelski Security	Cheseaux-sur-Lausanne, Switzerland
Mission Secure	Charlottesville, Virginia, U.S.
NTT	Tokyo, Japan
Open Cloud Factory	Bilbao, Spain
Optiv	Denver, Colorado, U.S.
Owl Cyber Defense	Columbia, Maryland, U.S.
PacketViper	Pittsburgh, Pennsylvania, U.S.
Radiflow	Tel Aviv, Israel
SecurityGate.io	Houston, Texas, U.S.
Shift5	Arlington, Virginia, U.S.
TXOne	Taipei, Taiwan
Waterfall Security Solutions	Rosh Ha'ayin, Israel

Source: Gartner (November 2023)

Market Recommendations

SRM leaders responsible for the technology, information and resilience risk of CPS security should:

- Anchor security efforts to operational resilience
- Assess where they are on the typical end-user CPS security journey described above
- Accelerate security stack convergence by inventorying all assets used in their organizations

Anchor Security Efforts to Operational Resilience

With ransomware attacks, global pandemics, supply chain disruptions and growing geopolitical concerns, most organizations are reevaluating their operational resilience. This includes coordinating the management of risk assessments, risk monitoring and the execution of controls that affect the workforce, processes, facilities, technology and third parties across risk domains used in the business delivery and value realization process. As security risks become cyber-physical, SRM leaders should seize the opportunity to combine that growing awareness with the expanding list of security tools at their disposal. Examples of best practices include:

- Reviewing where all security and safety governance is performed, and flagging any gaps, overlaps or opportunities for better alignment.
- Recognizing that IT-centric approaches will not be universally effective or even desirable and, therefore, need to be updated for production or mission-critical systems.
- Review IT/OT security governance.
- Modeling threat vectors across the entire operational threatscape.
- Clarifying and decentralizing risk ownership and raising security literacy in operations, while centralizing security continuous asset visibility and monitoring.
- Updating risk registers with scores based on the value of operations of entities, such as facilities, production lines or high-value assets.

Assess Where They Are on the Typical End-User OT/CPS Security Journey

Knowing what a typical journey looks like for similarly situated organizations can help SRM leaders map the way ahead and communicate the expected outcomes to senior leaders when asking for resources. Although security is usually viewed as a cost center, business-savvy SRM leaders will quickly realize that protecting their organization's value-creating assets can garner a different level of executive attention. This is particularly true if the investment in security solutions creates information valuable to other teams.

Gartner inquiries have uncovered that several end-user organizations that have deployed CPS protection platforms were able to share meaningful information with other teams in:

- **Operations and Engineering —** Asset usability, network topology and asset connectivity, redundancy mapping for resilience and business continuity management

- **Maintenance** — Asset profiles mapping to maintenance intervals
- **Compliance** — Dashboards and reports
- **Procurement** — Asset usage reports to support refresh/acquisition decisions
- **C-suite** — Enhanced operational situational awareness

This affords an opportunity to turn a security cost center investment discussion into a business-enabling discussion, which raises the profile of the SRM team in importance when it comes to digital transformation decisions.

Accelerate IT/OT Security Stack Convergence by Inventorying All Assets Used in Their Organizations

SRM leaders need to evaluate the growing list of stand-alone or platform-based options for interoperability with their IT security tools. To help them on their journey, SRM leaders are seeking more options than ever.

The good news is that the market is responding. New vendors and security features and functionalities for operational or mission-critical environments are now available. New categories are coming into focus — hence, the retirement of this generic Market Guide.

However, some best practices must continue to be followed:

- Demand demos and references.
- Conduct proof of value pilots between at least two vendors.
- Ensure that pilot programs are deployed in operational environments that represent real life.
- Engage production engineering teams throughout the process.

Evidence

The analysis in this research is based on primary and secondary research reflecting Gartner's many daily interactions with end users and technology providers.

[1] High-Impact Attacks on Critical Infrastructure Climb 140%, IBM (Security Intelligence).

[2] Industroyer2 Malware Targeting Ukrainian Energy Company, Techstrong Group (Security Boulevard).

[3] Feds Uncover a 'Swiss Army Knife' for Hacking Industrial Control Systems, WIRED.

[4] ICS Advisory Project, ICS Advisory Project.

[5] Sector Risk Management Agencies, Cybersecurity and Infrastructure Security Agency (CISA).

[6] Security Directives and Emergency Amendments, Transportation Security Administration.

[7] The NIS2 Directive: A High Common Level of Cybersecurity in the EU, Think Tank (European Parliament).

[8] EU Cyber Resilience Act, European Commission.

[9] Operational Technology Cybersecurity Controls, National Cybersecurity Authority.

Note 1: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Note 2: Examples of Constraints on Patching

- Careful planning that needs to take place so as not to introduce more risk to production uptime in operations.
- OEMs that play a key role in the operational phase of the life cycle of their products and have the burden to develop, test and roll out patches in tightly controlled, physical process environments.
- End users with an even heavier burden to know where these vulnerabilities are, and then determine whether patching, isolation, upgrades or a combination of these things make sense to their custom-made operations.
- Having to schedule deployment of patches and updates to coincide with the scheduled downtime of the production process.
- Unavailability of patches to production systems for out-of-support OS.

Document Revision History

Market Guide for Operational Technology Security - 4 August 2022

Market Guide for Operational Technology Security - 13 January 2021

Market Guide for Operational Technology Security - 5 November 2019

Market Guide for Operational Technology Security - 30 July 2018

Market Guide for Operational Technology Security - 17 August 2017

Market Guide for Operational Technology Security - 23 May 2016

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

CISO Effectiveness: Addressing the Cyber-Physical Systems Security Skills Gap

How to Develop a Security Vision and Strategy for Cyber-Physical Systems

3 Initial Steps to Address Unsecure Cyber-Physical Systems

CPS Security Governance — Best Practices From the Front Lines

Table 1: Vendor List

Vendor ↓	*Headquarters Location* ↓
Accenture	Dublin, Ireland
Airgap	Santa Clara, California, U.S.
Blue Ridge Networks	Chantilly, Virginia, U.S.
Booz Allen Hamilton	McLean, Virginia, U.S.
Capgemini	Paris, France
Cervello	Tel Aviv, Israel
Cisco Cyber Vision	San Jose, California, U.S.
DeNexus	Sausalito, California, U.S.
Dispel	New York, New York, U.S.
Hexagon	Stockholm, Sweden
Honeywell Connected Enterprise	Atlanta, Georgia, U.S.
Kudelski Security	Cheseaux-sur-Lausanne, Switzerland
Mission Secure	Charlottesville, Virginia, U.S.
NTT	Tokyo, Japan
Open Cloud Factory	Bilbao, Spain

Vendor ↓	*Headquarters Location* ↓
Optiv	Denver, Colorado, U.S.
Owl Cyber Defense	Columbia, Maryland, U.S.
PacketViper	Pittsburgh, Pennsylvania, U.S.
Radiflow	Tel Aviv, Israel
SecurityGate.io	Houston, Texas, U.S.
Shift5	Arlington, Virginia, U.S.
TXOne	Taipei, Taiwan
Waterfall Security Solutions	Rosh Ha’ayin, Israel

Source: Gartner (November 2023)