CLAROTY

THE ULTIMATE BUYER'S GUIDE FOR

INDUSTRIAL CYBERSECURITY PLATFORMS

Protecting OT, IoT, and all other
Cyber-Physical Systems across the XIoT

TABLE OF CONTENTS

Read this guide to learn more about:

With a thorough understanding of the cybersecurity challenges industrial manufacturers face, this guide will provide a clear and actionable path towards vendor selection and implementation.

Cyber-physical systems (CPS) are what Gartner® defines 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."

Most commonly found throughout critical infrastructure and other industrial organizations, CPS encompasses the operational technology (OT) assets and rapidly proliferating range of newer types of connected devices that underpin manufacturing, power generation, transportation, and other physical processes. Key examples of industrial CPS include:

- Traditional OT assets such as programmable logic controllers (PLCs) and remote terminal units (RTUs)
- Internet of things (IoT) and industrial internet of things (IIoT) devices such as smart sensors that exchange data between plant and enterprise networks to optimize production
- Building management systems (BMS) such as smart lighting and ventilation equipment, elevators, and physical access mechanisms, patient monitoring in hospitals, intelligent buildings, smart electric grids, and autonomous vehicles. These smart networked systems interact with the physical world to support real-time, guaranteed performance in safety-critical applications.

Although these devices help to sustain our lives, they also greatly increase cybersecurity risks and attack surfaces. The need for CPS protection platforms, which were built to ensure the safety and security of these critical devices, is urgent. As industrial organizations look to bolster their cybersecurity posture, however, they will find that the CPS protection platform market is growing.

INDUSTRIAL CYBERSECURITY LANDSCAPE

Digital Transformation

Digital transformation has shifted the security posture of industrial enterprises and critical infrastructure organizations by connecting previously isolated operational technology (OT) environments with their information technology (IT) counterparts. Although IT/OT convergence has brought the promise of cost savings and resource efficiencies, this rise in interconnectivity has expanded the attack surface for cyber criminals, giving them new pathways into these inherently insecure OT environments.

32%

According to Fortinet, when a cyberattack occurred earlier this year, **nearly one-third (32%) of respondents indicated both IT and OT systems were impacted**—up from only 21% last year

Legacy Devices

Legacy devices in industrial environments were manufactured many times decades ago, without cybersecurity in mind, and many times lack the necessary features to protect them against cyber attacks. As digital transformation accelerates, these previously "air-gapped" devices are now being connected to the internet, causing new attack vectors to emerge. The cost of updating this equipment, however, outweighs the benefits of doing so, making projects challenging to justify. Replacing legacy devices may also cause operational disruption, as they may require downtime or reduced functionality, which can cause serious consequences.

1/3

More than one-third of ransomware attacks reported to the FBI last year impacted organizations in a critical infrastructure sector

Modernized Workforce

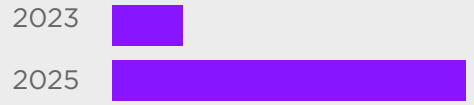
The recent shift to remote and hybrid workforces have raised concerns for industrial organizations trying to protect their critical infrastructure. And, ensuring that legacy devices and systems are up-to-date is a key priority. Legacy systems with outdated hardware and software are not easy to replace, and may be unable to accommodate cybersecurity best practices. They also have inherent security vulnerabilities and are often not compatible with security features including remote access.

68%

of organizations expect to face increased challenges in cybersecurity due to remote working

Remote Access

Seemingly overnight, organizations were forced to close their physical operations and shift to remote environments — putting business continuity plans to the test. With outdated technology and unmanaged access, organizations need a solution to protect their environments from modern threats. Similarly, industrial environments rely on remote access to enable both internal and third-party personnel to maintain assets. However, if not managed properly, remote access has the potential to bypass network segmentation measures — and, causes an expanded attack surface, introducing new entry points for cyber threats.



According to Gartner, by 2025, **insider risk will cause 50% of organizations** to adopt formal programs to manage it, up from 10% today.

Regulatory Requirements

As a result of the above changes in the industrial landscape, regulatory requirements have been set to establish minimum standards for cybersecurity, requiring industrial organizations to implement specific measures to protect their critical infrastructure from cyber attacks. More often than not, these regulatory requirements can be complex, difficult to understand, and costly to comply with — particularly for smaller organizations with limited resources. Without dedicated compliance teams in place, or partnerships with cybersecurity vendors, companies will not only struggle to meet requirements, but will also fail to improve their cybersecurity posture.

The pressure to reinforce cybersecurity measures has even become a presidential priority. **The White House recently announced a National Cybersecurity Strategy** increase regulation of critical industries by making them adopt basic cybersecurity practices.

CRITERIA TO CONSIDER AT THE COMPANY LEVEL

Maturity and Stability

When creating criteria for what to look for in a CPS security provider, industrial organizations must consider if the solution provider has strong financial backing, validation from top vendors, and market leadership. Having global leaders as both partners and customers proves that a product is thoroughly vetted with confidence and that the vendor can be trusted in the innovation, maturity, and longevity of not just their portfolio but in their mission, vision, and deep domain expertise.

Portfolio Breadth and Depth

A CPS security vendor should have a portfolio breadth that supports all use cases across the CPS security journey, and a portfolio depth that supports all types of CPS across the extended internet of things (XIoT), deployment needs, and network architectures. Ensuring that the vendor you are evaluating does not just provide one-size-fits-all solutions, but equally robust-yet-scalable SaaS and on-premise options as well. An efficient CPS security solution should meet any customer's unique needs and environment throughout their entire XIoT cybersecurity journey — no matter their maturity, network architecture, regulatory environment, or stance on the SaaS vs. on-premise debate.

Industry Contributions

Industry contributions including deep commitment to driving progress via research and public sector engagement is a must when evaluating CPS security solution criteria. CPS security providers with award-winning research teams empower the manufacturers of the vulnerable devices to improve the security of their products and, therefore, also improve the security of the critical operations and infrastructure those products support. By disclosing vulnerabilities in the XIoT devices that underpin your critical operations, research teams equip customers with stronger protection against the threats that matter most.

OT Centric Solutions

Many CPS use proprietary protocols and legacy systems which are incompatible with traditional IT security solutions. In many environments, traditional vulnerability scanners are unsafe, and patching is rarely permitted due to their low tolerance for downtime. That's why it is vital for industrial organizations to evaluate CPS security solutions that are OT centric and have the ability to gain granular visibility into their entire XIoT environment. Evaluations criteria should include ensuring the solution is purpose-built for OT environments, that it can provide granular visibility into the diverse mix of new and legacy devices located in many industrial environments, and that it can recognize the proprietary protocols used by OT, BMS, and other industrial assets that are invisible to generalized security tools.

KEY PRINCIPLES FOR ACHIEVING CYBER AND OPERATIONAL RESILIENCE

Gain CPS Visibility

A primary criteria for evaluating a CPS security solution is ensuring that it can provide visibility into your OT environment. This is arguably the most important criteria as it lays the foundation for your entire cybersecurity journey. It is impossible for organizations to protect their assets if they can't see or understand them. Gaining this visibility is one of the most fundamentally important yet challenging tasks facing security and risk leaders today. This is largely because XIoT assets typically use proprietary protocols that are incompatible with, and therefore invisible to, generalized security tools. Critical infrastructure environments may also encompass a diverse mix of new and legacy devices that communicate and operate in different ways, making it even more difficult to answer the question of what devices are in the environment. Further complicating matters is the fact that there is no one-size-fits all path to asset discovery. Every XIoT environment is unique, and most contain complexities that render certain asset discovery methods ineffective. That's why it is key to ensure your CPS security solutions offers multiple, highly flexible discovery methods that can be mixed and matched to deliver full visibility in the manner best suited to your distinct needs.

Integrate Your Existing IT Tools & Workflows with OT

Since most CPS use proprietary protocols and legacy systems, they are simply incompatible with traditional IT solutions — but that doesn't mean they have no place in OT. Rather than expanding your already-extensive tech stack, you should evaluate a CPS security solution that integrates with them. By extending your existing tools and workflows from IT to OT, you can safely uncover risk blindspots without endangering operations by integrating their already extensive tech stacks with a purpose-built OT security solution. This strategy will help organizations to take control of their risk environment and create further visibility across traditionally siloed teams by simply extending existing tools and workflows from IT to OT.

Extend your IT security controls & governance to OT

Since most CPS use proprietary protocols and legacy systems, they are simply incompatible with traditional IT solutions — but that doesn't mean they have no place in OT. Rather than expanding your already-extensive tech stack, you should evaluate a CPS security solution that integrates with them. By extending your existing tools and workflows from IT to OT, you can safely uncover risk blindspots without endangering operations by integrating their already extensive tech stacks with a purpose-built OT security solution. This strategy will help organizations to take control of their risk environment and create further visibility across traditionally siloed teams by simply extending existing tools and workflows from IT to OT.

EVALUATE CPS SECURITY VENDORS BY THESE CORE CONTROLS

EVALUATE CPS SECURITY VENDORS BY THESE CORE CONTROLS

CORE CONTROLS	EVALUATION CRITERIA
Asset Management Since industrial assets use proprietary protocols that are incompatible with standard inventory tools, manually maintained, error-prone inventories remain common. Operational risks are also prominent as manual asset management processes are no match for the pace at which the risks of vulnerabilities, end-of-life indicators, and outdated firmware are emerging. Additionally, standard tools and manual processes cannot provide the tracking and reporting needed for compliance with stringent asset SLAs and audits.	• Supports proprietary industrial protocols and provides a variety of collection methods • Continuously monitors and assesses asset activity, alerting to any changes • Optimizes workflows via reporting and integrations — streamlining SLA tracking • Provides alignment across enterprise and industrial environments with CMDB integration
Vulnerability and Risk Management Finding a vulnerability isn't enough. You also need to assess the affected asset's context and potential impact on your operations to prioritize and remediate the risk. However, industrial environments and the assets that underpin them are uniquely fragile and cannot tolerate the traffic generated by standard vulnerability scanners. Most industrial environments also have low tolerance for downtime, so patching occurs rarely, no matter the vulnerability or risk.	• Accurately matches exact assets with known CVEs based on vendor, model, and firmware version, to ensure efficient prioritization and remediation of network vulnerabilities • Identifies and analyzes known risks to calculate the most likely scenario in which an attacker could compromise the network • Evaluates and scores vulnerabilities based on the unique risk they pose to your network — enabling more efficient and effective prioritization and remediation
Network Protection Effectively segmenting industrial networks can be a tedious, error-prone process that entails defining and constantly tuning policies to your unique environment. Monitoring and ensuring compliance with regulatory and organization measures is also a challenging task — requiring granular, properly tuned policies that many organizations lack. Unsecured remote access is also a widespread challenge faced by industrial environments as common practices are risky and inefficient.	• Provides recommended segmentation policies that can be easily and automatically enforced via your existing infrastructure • Enables continuous monitoring to understand how assets communicate under normal circumstances — allowing for automatic alerts to any policy violations • Ensures support for all industrial use cases by tightly controlling, monitoring, and securing remote sessions

EVALUATE CPS SECURITY VENDORS BY THESE CORE CONTROLS

CORE CONTROLS	EVALUATION CRITERIA
Threat Detection The proprietary protocols in industrial environments are not compatible with traditional threat detection tools, rendering them ineffective and potentially disruptive. Industrial environments are also extremely complex making it difficult to identify potentially malicious deviations from accepted baselines. Due to this complexity, inherent insecurity, and a growing XIoT attack surface, industrial environments are increasingly targeted by malicious actors.	• Offers multiple detection engines to automatically profile all assets, communications, and processes in industrial networks • Has a deep understanding of proprietary industrial protocols and device behaviors to ensure each device receives the security policy appropriate for it — and prevents any future violations. • Provides a portfolio of threat capabilities that seamlessly integrate with your existing tech stack — bridging the IT-Industrial expertise gap.
Remote Access Most traditional remote access tools are designed for IT networks, and often have cumbersome access mechanisms and interfaces that are unsuitable for OT needs. In industrial environments, internal and third-party users must remotely access industrial assets for maintenance and other purposes; however, this requires administrators to maintain costly, complex infrastructure. OT remote users can also make unauthorized chances that pose risks to operations, and without role-and policy-based access controls or visibility into users' activities, organizations cannot identify or responds to incidents — exposing the OT environment to greater risk.	• Offers automated user provisioning with single sign on and just-in-time provisioning — allowing users to gain immediate, secure, and highly controlled access • Defines and enforces granular access controls for industrial assets at multiple levels and geographic locations • Supports Zero Trust architecture and the least privilege principle • Real-time session monitoring for troubleshooting, user supervision, and emergency termination if necessary • Supports the Telnet protocol to allow remote sessions to legacy assets

As the threat landscape continues to evolve and new attack vectors emerge, cybercriminals are becoming increasingly sophisticated in their tactics. To protect your critical industrial environment, it is key to partner with a CPS security vendor that meets your unique needs — and that starts with understanding what criteria is most important to evaluate. The right vendor should not only be able to align with the above core capabilities, but should support all use cases no matter where you are in your cybersecurity journey.

Claroty does this by providing unmatched visibility into all parts of the OT network, and provides support for all use cases across the entire CPS security journey. Due to our commitment to driving progress through our award-winning research team and our public sector engagement, our products are designed to equip our customers with even stronger protection against the threats that matter most. This coupled with validation from top automation vendors, who empower their own customers with our products, signifies the confidence and trust they have in the innovation, maturity, and longevity of not just the Claroty portfolio, but in our mission, vision, and deep domain expertise. The CPS security vendor selection process is not an easy one, that's why we've created this guide to ensure your organization knows what to look for in order to efficiently protect critical OT, IoT, and your entire XIoT ecosystem.

Gartner, Tool: Cyber-Physical Systems Protection Platform Rating and Selection, By Wam Voster, Katell Thielemann, Published 21 September 2022

About Claroty

Claroty empowers organizations to secure automation, control, and other cyber-physical systems across industrial, healthcare, commercial, and public sector environments: i.e. the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the leading investment firms and industrial automation vendors, Claroty is deployed at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.