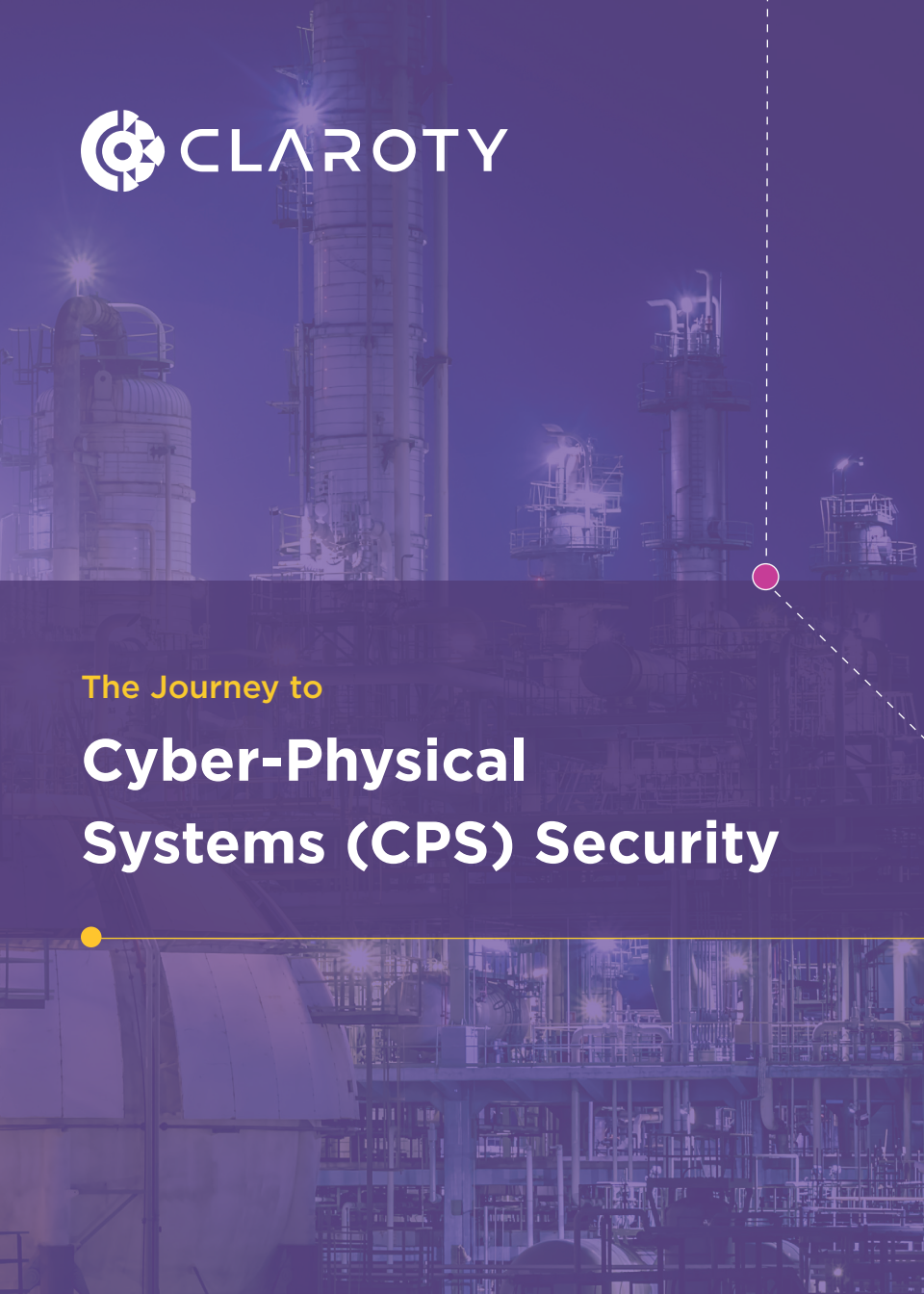


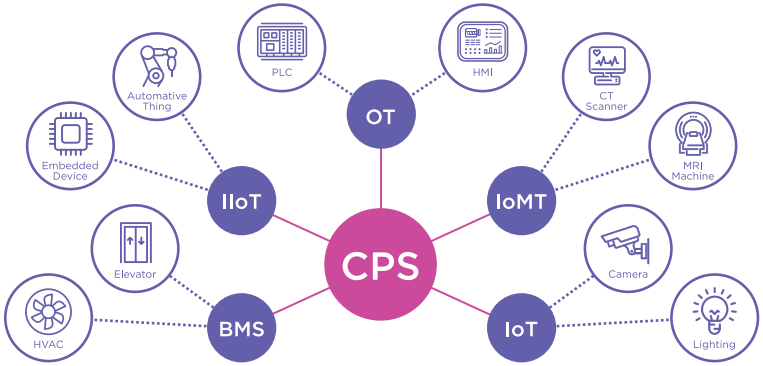
The Journey to

Cyber-Physical Systems (CPS) Security

TABLE OF CONTENTS

WHAT IS A CPS?

As defined by Gartner®, cyber-physical systems (CPS) are "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."



The term CPS encompasses the operational technology (OT) assets, building management system (BMS) equipment, internet of medical things (IoMT) devices, and other types of both legacy and modernized connected assets that underpin operations across critical infrastructure sectors. Key examples of CPS include patient monitoring systems and infusion pumps in hospitals, programmable logic controllers (PLCs) and engineering workstations at manufacturing plants, and connected HVAC systems and elevators within intelligent buildings, among many others.

THE CURRENT STATE OF CPS SECURITY

The current state of CPS security reflects changes to traditional security approaches in protecting cyber-physical systems. This reality has grown clearer and clearer over the past decade as the interconnectivity, variety, and prevalence of CPS in industrial environments have rapidly expanded.

Historically, the security priorities of industrial environments were largely limited to ensuring that OT assets remained air-gapped.

Today, however, it is commonplace for industrial environments to be intertwined with their IT counterparts and the Internet. This norm is the product of digital transformation — particularly, the explosion of IoT, IIoT, IoMT, BMS, and other types of CPS that organizations are increasingly implementing both alongside and in place of their legacy OT assets and traditional medical devices. These conditions have given rise to a vast, diverse, and ever-expanding web of cyber-physical connectivity: otherwise known as the Extended Internet of Things (XIoT).[1]

The benefits of the XIoT are undeniable — from efficiency, to innovation, to sustainability — but it is also exposing critical industrial environments to cyber threats. Case in point is the

1. Gartner, Tool: Cyber-Physical Systems Protection Platform Rating and Selection, By Wam Voster, Katell Thielemann, Published 21 September 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. [SG1]

scourge of ransomware and other destructive cyber attacks affecting CPS in recent years. Unfortunately, the connectivity such attacks exploit is growing at a rate that continues to outpace efforts to secure it. And, with Industry 5.0 on the horizon and once-futuristic technologies like edge computing and autonomous systems approaching mainstream, the risks are worsening.

For security leaders responsible for protecting their organization's CPS environment amid these conditions, the challenges are complex and seemingly countless. Key considerations include:

1. Ongoing expansion of the volume and diversity of CPS is increasing exposure

According to Gartner, the CPS protection platforms market is growing, as adoption accelerates due to increased threats, existing and new vendors position more aggressively in the market, and new entrants target underserved vertical industries.[2]

2. The frequency and severity of attacks affecting CPS are rising

During the first quarter of 2023, approximately **1 in every 31 organizations** worldwide experienced a ransomware attack on a weekly basis.[3]

3. CPS security is now a focal point of the regulatory landscape

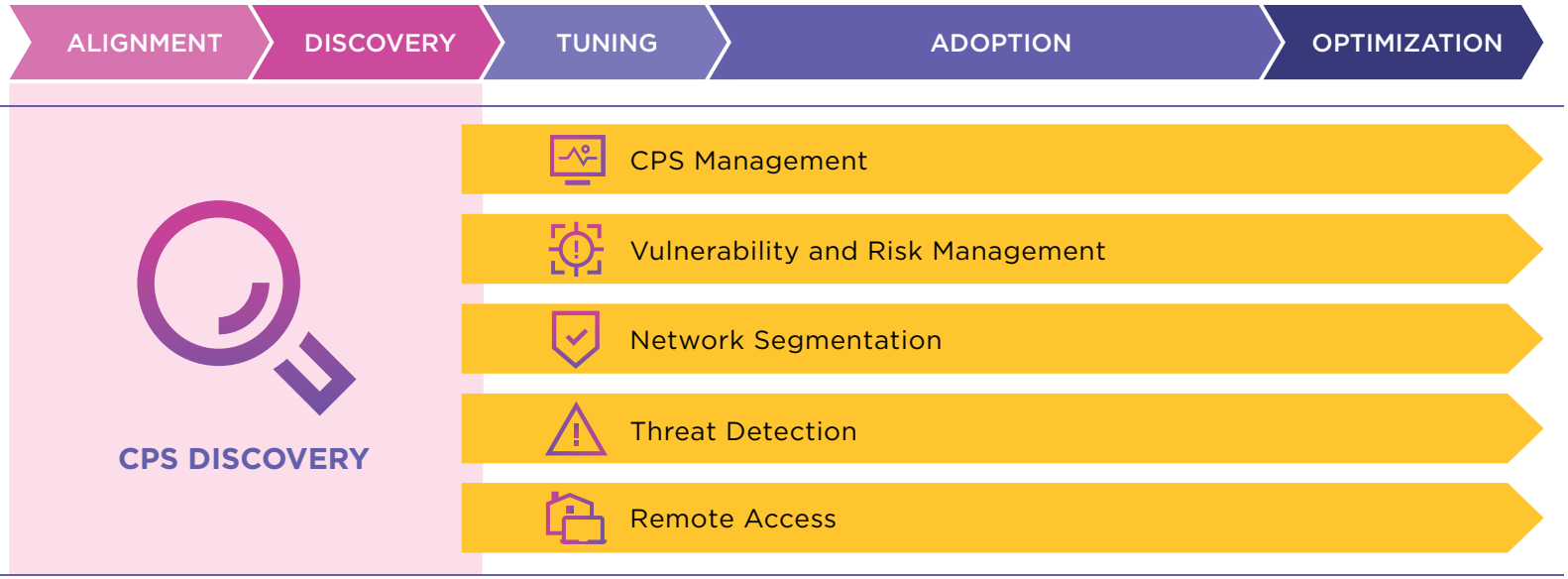
TSA, NIS2, NERC-CIP, SOCI, HHS 405(d), and NIST are among many regulatory bodies and standards entities that released CPS security-focused requirements or recommendations in recent years.

The importance of CPS security has been reinforced by the **U.S. Biden-Harris Administration's National Cybersecurity Strategy**, which calls for organizations in critical sectors to adopt key controls that extend to CPS.[4]

2. https://claroty.com/resources/reports/2023-gartner-market-guide-for-cps-protection-platforms
3. https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/
4. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

The Recommended Journey to CPS Security

Since CPS environments are integral to the availability, integrity, and safety of essential processes and infrastructure, are inherently complex, and are being increasingly connected — and exposed — to the Internet, securing them is both challenging and critically important. The remainder of this guide will draw upon the firsthand experience of CPS security practitioners, vendors, and researchers to examine these challenges, introduce a recommended journey to CPS security maturity, and offer strategic guidance on key use cases throughout this journey.



CPS DISCOVERY

It is impossible for organizations to protect their CPS if they can't see or understand them. That's why device discovery is arguably the most important step — as it lays the foundation for your entire CPS security journey. However, gaining this visibility is also one of the most challenging tasks facing security and risk leaders today. This is largely due to the following:

CPS Discovery Challenges:

Proprietary Protocols Prevail

ICS devices, OT assets, BMS, and other types of CPS typically use proprietary protocols that are incompatible with (and thus invisible to) standard security tools.

Diverse Assets are the Default

Industrial assets can have a decades-long lifespan, so their environments likely comprise a diverse mix of new CPS and legacy equipment that operate and communicate differently.

Network Complexity is the Norm

CPS environments often have complex architectures with serial networks or air-gapped segments that can be widely distributed across physical sites.

One-Size-Fits-All Discovery is a Myth

Despite the abundance of conventional wisdom touting passive monitoring as a 100% effective, one-size-fits-all method for CPS discovery, it is not. Gaining a full CPS inventory nearly always requires combining multiple discovery methods.

The Strategy for CPS Discovery

In order to combat these challenges and attain the caliber of visibility required for their CPS security journey, organizations are encouraged to adopt the following CPS discovery strategy:

1. Define Visibility Goals

During this phase of the strategy, it is key to align with CPS stakeholders on your current visibility challenges and define your CPS discovery requirements based on what outcomes you want to achieve. Aside from building a strong foundation for the rest of your CPS security journey, desired outcomes may include:

- ✔ Greater confidence in the accuracy and timeliness of your CPS inventory
- ✔ Easier compliance with internal and regulatory requirements
- ✔ Streamlined support for M&A due diligence activities

2. Choose Discovery Methods

Next, determine which discovery methods are needed to deliver the caliber of CPS visibility warranted by your requirements. You will likely need to combine at least two of the following methods in order to gain sufficient visibility:

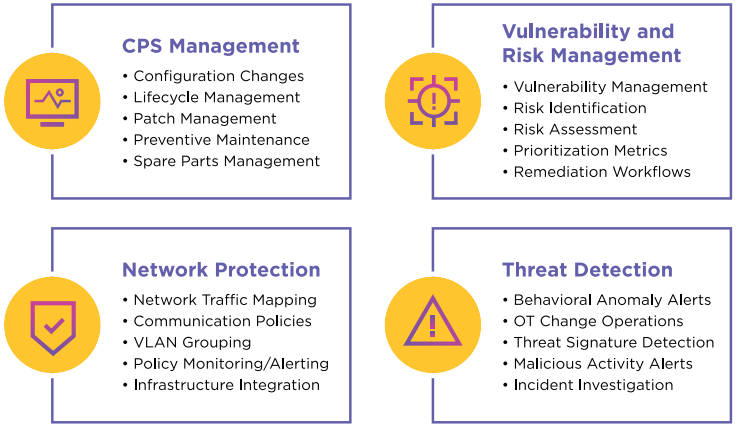
- ✔ Passive Monitoring
- ✔ Active Queries
- ✔ Configuration File Parsing
- ✔ Host-Based Discovery
- ✔ Integration-Based Discovery

3. Implement Discovery Methods

Once selected, execute your discovery methods to identify all CPS, collect their key details, and populate this information within a centralized CPS inventory.

4. Enrich CPS Profiles

Then, connect any existing CMDB or other security or operational solutions to your newly populated CPS inventory to further enrich device profiles across all solutions. Although ideal profiles include vendor, firmware, model, rackslot, and more — the specific details should map to your CPS management objectives and broader CPS security journey. For reference, the following use cases require a fully enriched profile for each device:



5. Leverage CPS Visibility

Finally, you can use the CPS visibility and workflows provided by discovery methods to operationalize device management and other core controls that align with your CPS security strategy.

CPS MANAGEMENT

Effective, efficient asset and change management is integral to operational resilience yet increasingly difficult for CPS owners and operators largely due to the following challenges:

CPS Management Challenges:

Error-Prone and Inefficient Manual Processes Prevail

Since CPS typically use proprietary protocols that are incompatible with standard inventory tools, manually maintained, error-prone inventories remain common.

Operational Risks are Continually Evolving

Manual or otherwise inadequate device management is no match for the pace at which vulnerabilities, end-of-life indicators, outdated firmware, and other risk factors emerge.

Compliance Requirements are Stringent

Complying with SLAs and audits requires tracking and reporting on granular, CPS-specific details that standard tools or manual processes cannot provide.

The Strategy for CPS Management

1. Define CPS Management Priorities

Consider business objectives, current inefficiencies, governance limitations, regulatory requirements, supply chain dependencies, and risk insights from your CPS inventory to validate and prioritize your CPS management goals. These may include:

- Preserve operational safety, integrity, and uptime in all circumstances
- Adhere to internal and regulatory compliance measures
- Optimize lifecycle and obsolescence management
- Reduce maintenance costs

2. Address Immediate Gaps

Achieve early wins by pinpointing and mitigating high impact, low-effort operational risk factors evident in your CPS inventory. Common examples are:

- Unauthorized port scans
- End-of-life indicators
- Misconfigurations

3. Add Business Context & Integrate Data

Align CPS groups and ownership and synchronize their details with your existing CMDB or related solutions to create a real-time, single source of truth for CPS details.

4. Scale Business Processes

Recreate success on a larger, enterprise-wide scale by aligning workflows between IT and CPS environments. Having a global view of CPS details will allow you to:

- Plan procurement, maintenance, and related processes holistically across sites
- Better prioritize remediation and risk controls based on operational requirements
- Further streamline workflows and track progress

5. Enhance Business Value

Optimize workflows to drive predictive maintenance, proactive obsolescence management, and other key use cases that reduce risk, boost efficiency, lower costs, and deliver value enterprise-wide.

VULNERABILITY & RISK MANAGEMENT

An effective vulnerability & risk management program provides visibility into risks within connected devices, drives prioritization based on indicators of current and predicated exploitation likelihood, and informs remediation. However, there are several challenges that can make this difficult to achieve:

Vulnerability & Risk Management Challenges:

CPS Visibility is often Minimal

CPS assets use protocols that are largely invisible to standard security tools. If you can't identify a device, you can't assess (much less manage) its vulnerabilities and risks.

Context Gaps Hinder Prioritization

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.

Conventional Wisdom is at Odds with the Reality of Managing CPS Vulnerabilities:

Nearly 70% of CPS vulnerabilities disclosed in 2022 received a CVSS v3 severity score of "high" or "critical," yet less than 8% have been exploited. This discrepancy raises concerns about the conventional wisdom and solutions that recommend prioritizing remediation based on CVSS scores. Security teams following this recommendation are often not only overwhelmed; they may also be misdirecting resources towards vulnerabilities that are unlikely to be exploited, while overlooking those that are.

Standard Vulnerability Scanners are Unsafe

CPS environments and the assets that underpin them are uniquely fragile and cannot tolerate the traffic generated by standard vulnerability scanners.

Patching is Rarely Permitted

Most CPS environments have no tolerance for downtime, so maintenance windows (and, as a result, patching) occur rarely, no matter the vulnerability or risk.

The Strategy for Vulnerability & Risk Management

1. Define Program Objectives

It is essential to determine how you will define and measure risk, prioritize vulnerabilities, and establish measurable KPIs for your program. During this phase, be sure to:

- ✔ Consider CPS risk scoring requirements: Since most security leaders are now expected to quantify and account for their organization's CPS risk posture in the broader risk score shared with executive leadership, it is essential to ensure risk quantification mechanisms reflect true risk, align with existing GRC processes and risk tolerances, and consider business context.
- ✔ Establish vulnerability prioritization criteria that go beyond CVSS scores to also account for whether vulnerabilities are currently or are predicted to be exploited in the wild. Indicators from CISA's Known Exploited Vulnerabilities (KEV) catalog and the Exploit Prediction Scoring System (EPSS) can deliver such insights.

2. Identify Vulnerabilities

Next, it is important to correlate your CPS inventory with CVEs and other weaknesses — and, if desired, extend any existing IT vulnerability scanners to compatible CPS — to pinpoint vulnerable assets and uncover risk blind spots in your CPS environment.

3. Prioritize & Firefight

Using KEV and EPSS data, you can prioritize the most important vulnerabilities in your CPS environment based on which ones are (or are likely to be) actively exploited, and then you can apply mitigations to the riskiest affected assets.

4. Mature & Scale Workflows

Use dedicated CPS workflows or existing IT ticketing, orchestration, and/or related tools to mature your CPS vulnerability management tactics into scalable workflows.

5. Optimize Risk Posture

Leverage strategic CPS insights and risk recommendations to drive proactive mitigations — and, if desired, extend any existing IT endpoint security solutions to compatible CPS — to further strengthen your risk posture.

NETWORK SEGMENTATION

Network segmentation is a Zero Trust-based control that help protect CPS environments yet is difficult to implement due to the following challenges:

Network Segmentation Challenges:

Segmentation Policies are Error-Prone

Effectively segmenting CPS networks can be a tedious, error-prone process that entails defining and constantly tuning policies to your unique environment. This issue stems from persistent visibility and expertise limitations.

Compliance is Inconsistently Enforced

Monitoring and ensuring compliance with regulatory and organizational measures requires granular, properly tuned policies that many organizations lack. This is due to a lack of understanding in terms of how CPS assets and users in your environment communicate under normal circumstances.

The Strategy for Network Segmentation

1. Define Segmentation Strategy

The network segmentation journey begins with considering business objectives, regulations, and insights from your CPS inventory to define segmentation goals and map out how your existing infrastructure will support your strategy. During this phase, desired outcomes include:

- ✔ Compensating for risks of EOL & other “unpatchable” assets
- ✔ Complying with regulatory requirements
- ✔ Shrinking the CPS attack surface

2. Create Zones & Policies

Next you should study devices’ communications, operations, and criticality to group them into zones, then create policies for how the CPS in each zone should communicate under normal circumstances. Zones should be based on:

- ✔ Your CPS environment’s topology
- ✔ How your CPS communicate
- ✔ Industry frameworks and standards, such as ISA/IEC 62443

3. Monitor Policies

Configure alerting rules that align with each zone’s policies, then monitor all CPS and their communications in the environment to detect any deviations from those rules.

4. Investigate, Tune, & Validate

Next, investigate any deviations, identify those requiring timely action, and prioritize remediations for the riskiest CPS. Then, tune and validate policies to ensure that, if enforced, none would negatively impact operations.

5. Enforce & Optimize Policies

Finally, import zones into your existing firewall and/or network access control (NAC) solution, mirror their respective policies within it, and then logically enforce those policies. Scale and enhance enforcement to optimize network protection over time.

THREAT DETECTION

No CPS environment is immune to threats, so being able to detect and respond effectively when they do surface is critical yet difficult.

Threat Detection Challenges:

Traditional Monitoring Tools are Incompatible

The proprietary protocols and critical — yet often delicate — physical processes in CPS environments are typically incompatible with traditional threat detection tools, rendering them ineffective and potentially disruptive.

CPS Environments are Complex

The intricacy of multisite industrial environments and their critical assets can make it difficult to identify potentially malicious deviations from accepted baselines.

Targeted Attacks are on the Rise

CPS environments are increasingly targeted by malicious actors due to their growing attack surface, inherent insecurity, and downtime intolerance.

Expertise and SOC Functional Gaps

Many security operations center (SOC) teams are trained to detect and respond to IT-centric incidents but lack the domain-specific knowledge and tools needed to defend CPS environments.

The Strategy for CPS Threat Detection

1. Monitor for Known Threats

Initially, you should passively monitor your CPS environment for malware, malicious traffic, and other indicators of known cyber threats.

- ✔ All alerts should be automatically enriched with chain-of-events context from both your environment and the MITRE ATT&CK for ICS framework, where applicable.

2. Prioritize, Firefight, & Tune

Then, focus on responding to alerts for the most critical threats, prioritize remediation for the riskiest assets, and identify and integrate existing tools that can be leveraged for alert management and response.

- ✔ SIEM, SOAR, EDR, and similar tools tend to deliver the most value for CPS threat detection.

3. Monitor for Unknown Threats

Next, monitor network traffic for anomalous behaviors, build custom alerting rules, and further enrich EDR and SOC capabilities with CPS context.

4. Mature & Scale Workflows

Enhance incident response and investigation capabilities with processes and procedures to mature your CPS threat detection tactics into scalable workflows.

- ✔ For example, analyzing PCAP downloads for known signature alerts can aid security teams' investigation efforts.

5. Optimize Risk Posture

Finally, use CPS insights and risk recommendations to inform controls that proactively reduce your attack surface and strengthen risk posture.

- ✔ By monitoring for EOL devices, key changes, and communication violations, you can drive segmentation initiatives, enhance asset management, and support other controls to further reduce the attack surface.

REMOTE ACCESS

The CPS that underpin industrial environments many times lack even the most basic cybersecurity protections. This is due to the following challenges:

Remote Access Challenges:

End-User Complexity: Increases MTTR

Since most traditional remote access tools are designed for IT networks, they often have cumbersome access mechanisms and interfaces that are unsuitable for OT needs.

Administrator Complexity: Increases TCO

Internal and third-party users must be able to remotely access industrial assets when needed for maintenance or other purposes. However, managing this access requires administrators to maintain costly, complex infrastructure while addressing users' onboarding and troubleshooting needs.

Poor Visibility and Security Controls: Increase Exposure to Risk

OT remote users could make unauthorized changes that pose risks to operations. These risks are compounded by using traditional remote access tools that give cybersecurity staff poor visibility into users' activities and do not enable such staff to implement role-and policy-based access controls for users.

The Strategy for Remote Access

1. Assess the OT Landscape

Review OT/CSP asset inventory & IT/OT convergence. Identify both domains' access points. Engage with stakeholders, understanding remote access challenges in the converged environment.

2. Define & Operationalize Access Strategy

Segment users based on prior insights, considering their unique roles, use cases, target systems, & current security policies & risks. Allocate permissions to simplify the user experience. Familiarize users with these new policies & their benefits, including reduced MTTR & onsite travel needs.

3. Refine Workflows Using Zero Trust Principles

After user segmentation, establish granular access controls. Implement zero trust & RBAC principles for optimized workflows, reducing administrative complexities. Continuously seek user feedback, aiming for workflow enhancements.

4. Manage & Monitor Remote Sessions

Prioritize session management. Collaborate with OT operators & security teams, identifying operational barriers. Initiate continuous monitoring & proactive incident planning to rapidly detect & contain any incidents in the event of a breach.

5. Drive Continuous Improvement

Further mature your OT remote access program by periodically optimizing policies, integrating within the security and broader business ecosystem, and driving added benefits through streamlined audits, enhanced resilience, reduced emissions, and cost savings.

SUMMARY

As the threat landscape continues to evolve and new attack vectors emerge, malicious actors are becoming increasingly sophisticated in their tactics. Unfortunately, there is no one-size-fits-all approach to building a CPS security strategy that will protect against all manner of threats. That's why It is important to understand that your CPS journey is unique. The journey to CPS security is not an easy one, that's why we've created this guide to ensure your organization is equipped with the initial steps to efficiently protect critical OT, IoT, IoMT, and your entire XIoT ecosystem.

For a deeper dive into the CPS journey and how to support your organization's unique use cases, visit claroty.com.