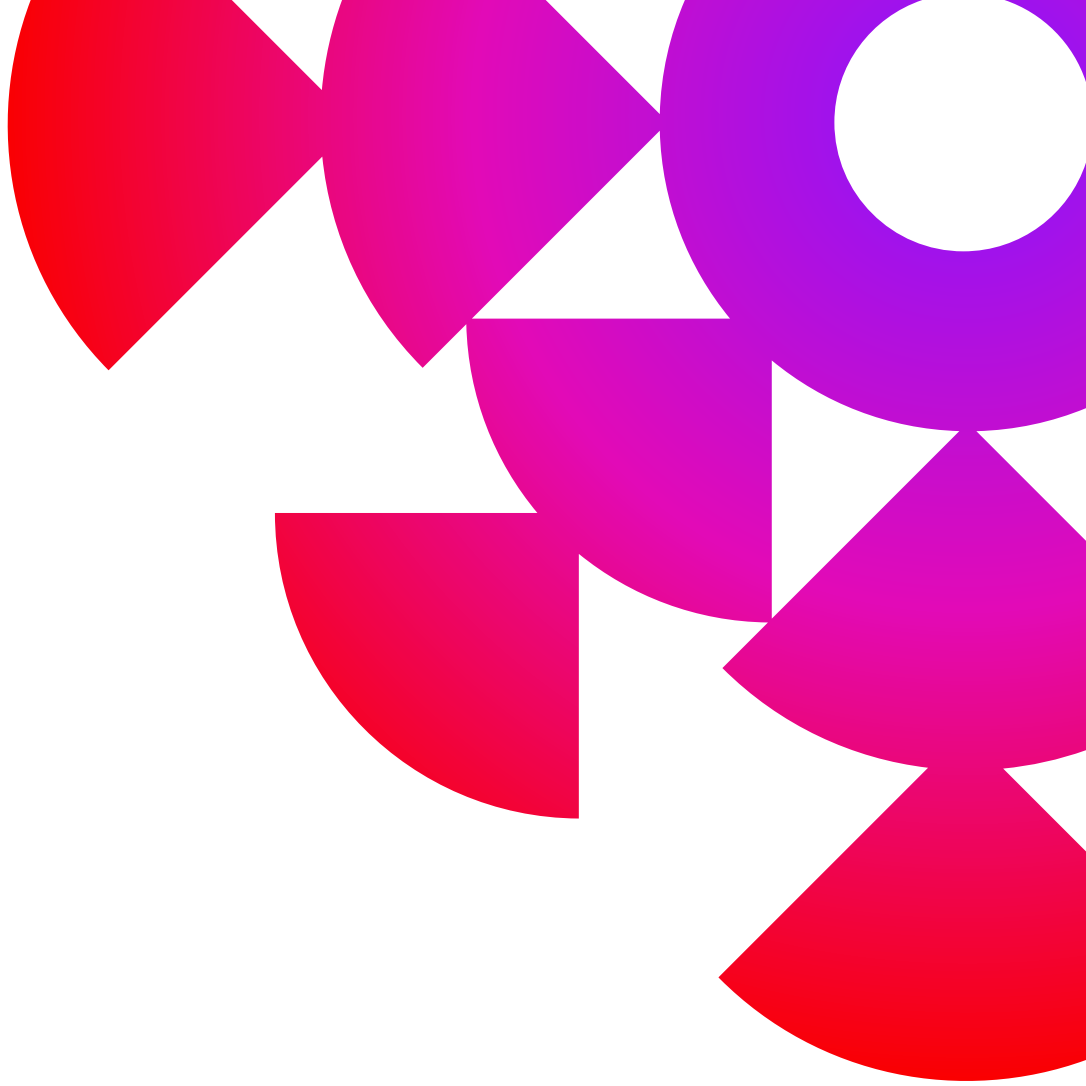


WHITE PAPER

IMPLEMENTING ZERO TRUST FOR INDUSTRIAL ENVIRONMENTS

CLAROTY ✦ ISTARI

TABLE OF CONTENTS

INTRODUCTION

The broad challenge facing many organizations today is the convergence of Information Technology (IT) and Operational Technology (OT). Whereas there are a plethora of solutions designed for managing risk, security controls, and vulnerability management on the IT side, there are few designed to meet the unique challenges and needs of industrial environments.

Historically, OT systems were invisible to IT due to separate networks and nonconnected devices. With more and more "things" connecting to the internet, the rapid rise in remote work, and critical infrastructure undergoing digital transformation, the attack surface is more prominent than ever. Traditional enterprise perimeter lines are completely blurred.

Without a secure connection between IT/OT networks, the proper access controls and network segmentation, an attacker could not only gain a foothold inside a corporate network but also move laterally until they affect critical systems.

These challenges, among other factors, have motivated a reported 76% of all organizations to start implementing zero trust programs. Zero trust addresses key security challenges, such as gaining visibility and improving response times, applying context to make risk-based decisions, and coordinating security with a deeper understanding.

Now is the time to embrace zero trust security – and that must include incorporating OT. This white paper will discuss zero trust architecture best practices, identify five common challenges within industrial security, and offer recommendations for technology that addresses these challenges while supporting zero trust.

NIST'S ZERO TRUST BEST PRACTICES

The National Institute of Standards and Technology (NIST), part of the US Department of Commerce, creates best practices intended to establish a common language for discussing different security and privacy aspects.

Regarding zero trust, NIST states:

"Zero trust is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level [FIPS199]. Transitioning to zero trust architecture is a journey concerning how an organization evaluates risk in its mission and cannot simply be accomplished with a wholesale replacement of technology."

ZERO TRUST

IS	IS NOT
A strategic approach leveraging multiple data points that provide context to enable risk-based decisions.	An off-the-shelf solution.
A data and identity-centric and de-perimeterized approach that provides granular least privilege access enforcement.	A one-time project.
A set of principles and capabilities focused on resource protection and the premise that trust and access must be continually evaluated.	A single tool.
A policy enforcement methodology that leverages multiple contexts to ensure the right people have access to the right resources, with the right set of privileges.	The same for every organization.

NIST publication 800-207 outlines principles for zero trust architectures. Implementing zero trust principles within an industrial network requires a more tailored approach than traditional IT networks. OT systems are less hardened and more challenging to update and patch. They also oversee critical processes and cannot be replaced or powered down for updates without interruption of services and operations.

NIST'S TENENTS OF ZERO TRUST

Tenent	Industrial Environment Application
Visibility: Identify all resources (people, devices, apps, infrastructure, etc.) connecting to your organization and where data and resources reside within the organization.	Effective industrial cybersecurity starts with visibility into assets, sessions, and processes within an industrial network.
Context: Establish user and device contexts; what data, application, device, location, network are the user(s) and device(s) trying to access? What is their health and posture?	To make data-driven decisions, administrators need system information for industrial assets (model number, rack slots, firmware version, etc.), and information about device lifecycle, potential attack vectors, network connectivity, unauthorized connections, existing malware, process values and deviations.
Authenticate: Authenticate resources via centralized and federated identity.	Streamline user access by integrating corporate IdPs such as Active Directory, SAML, and OpenID Connect with industrial assets. Additionally, require users to enable 2FA or TOTP.

Control & Segment: Apply least privilege access policy, enforce MFA or PAM if resource/data is sensitive. Segment and control access only to the resources needed via central policy engine.	Segment the industrial network using "virtual zones," grouping together similar assets by their type, communication behaviors, and the kind of protocols that communicate under normal circumstances. Maintain the Purdue Model and do not allow direct connections to industrial assets. A remote access tool for OT should enforce a Least Privilege policy and have strong authentication to grant internal and external parties access to specific assets at predetermined times. Administrators should have full oversight of remote access sessions.
Log: Log and inspect all traffic, access and activity.	Leverage virtual zones. Create zone rules and policies to ensure all traffic remains within expectations. Monitor asset communication across multiple zones. Review activity logs for all sessions – including remote – to ensure only authorized changes are made to the network.
Adapt: Continually reassess risk and apply new controls if posture changes, or when access is no longer needed.	Use the latest OT purpose-built tools and technology designed to minimize risk to OT.

NIST asserts any enterprise environment can be designed with zero trust tenets. Most organizations already have some elements in their infrastructure. Zero trust architecture has its roots in geographically distributed organizations and/or has a highly mobile workforce, which has primed networks for implementing industrial control systems (ICS).

As physical (OT) systems and devices come into the digital realm, IT leaders seeking to ensure support for zero trust initiatives should consider the common challenges affecting industrial networks and make thoughtful considerations.

COMMON CHALLENGE: GAINING VISIBILITY

Effective industrial cybersecurity starts with knowing what needs to be secured, which is why visibility is a core tenent of zero trust.

Gaining high caliber visibility for cyber-physical systems can be challenging for many reasons:

- Standard IT visibility solutions and scanning methods are typically incompatible with, and unsafe for, industrial networks
- Traditional industrial asset inventory solutions often require hardware that can be expensive, complex, and time-consuming to deploy
- Many industrial networks are geographically isolated and/or air-gapped, making them difficult to access in order to install hardware and software

- Traditional industrial asset inventory methods, such as passive data collection and offline file-parsing, may not be compatible with or suitable for all networks and use cases
- The use of proprietary software, proprietary communication protocols, and unfamiliar devices

For industrial environments, visibility is needed across three dimensions:

Assets: This encompasses all OT, IoT, and IIoT assets on industrial networks, including serial networks. Visibility includes the critical attributes of each asset; model number, firmware version, and card slot, among others.

Sessions: This includes all industrial network sessions along with their bandwidth, actions taken, changes made, connectivity paths, and other details relevant to industrial network sessions.

Processes: This includes tracking all industrial operations, the code section and tag values of all processes in which OT, IoT, or IIoT assets are involved, and any abnormal changes to these assets' process values that could indicate threats to process integrity.

Visibility into these three areas is essential for effective risk calculation and reduction.

CLAROTY & VISIBILITY

Use an industrial cybersecurity platform that supports a comprehensive list of proprietary and standard XIoT protocols. Visibility should include network asset discovery and in-depth understanding of network communication, revealing what once was hidden to IT and OT administrators.

The Claroty suite of solutions offers both hardware and software options to gain visibility into an industrial network. Claroty Continuous Threat Detection (CTD) uses three discovery methods to reveal assets, sessions, and processes.

- Passive: Continuous, no-impact, real-time monitoring
- App DB: On-demand asset data enrichment from backup configuration files
- Active queries: Precise, periodic queries of network assets utilized only when such inquiries can be made safely and without impact

In addition, Claroty Edge delivers complete visibility without requiring network changes, utilizing sensors, or having any physical footprint at lower network levels.

Whether an organization prefers on-premises or SaaS, Claroty's purpose-built OT solutions rapidly discover and manage all XIoT assets to deliver full industrial network visibility.

COMMON CHALLENGE: DETECTING THREATS

Once visibility is established, organizations can start applying context to their industrial network.

Contextual information around device lifecycle, potential attack vectors, network connectivity, unauthorized connections, existing malware, process values, and deviations are all necessary to be able to detect threats and manage vulnerabilities effectively. There are challenges associated with using all this context to quickly and accurately identify threats.

More specifically, detecting all of the different types of threats that can impact OT networks requires multiple approaches, and often multiple tools—many of which must be configured individually for each OT network at each site. Particularly for enterprises with numerous sites across vast geographic areas, these conditions can hinder not just threat detection, but also other OT security initiatives, too.

CLAROTY & THREAT DETECTION

Optimal threat detection is not simply being able to identify one type of attack. A tool needs to use a broad spectrum of threat engines to bring context to an environment.

Claroty CTD uses five detection engines to automatically profile all assets, communications, and processes in industrial networks and alert users in real-time to anomalies, known, unknown, and emerging threats.

Anomaly detection	OT asset protocols are unique because they were not designed with connectivity in mind. If you can't properly translate OT protocols, you run the risk of creating a high volume of false positives, or worse, being entirely unable to identify the asset. A solution needs to understand OT asset protocols well enough to be able to identify changes in communications between network assets or zones in order to pinpoint previously unknown threats, such as zero-day attacks.
Security Behaviors	This engine is responsible for identifying any known techniques that have been used by attackers. This includes IT security patterns such as port scanning and man-in-the-middle attacks, as well as OT-specific security patterns such as TAG/address scans. An example of the type of known OT-specific techniques this engine looks for is the HAVEX attack. This specific attack included an OPC scanning module as part of the reconnaissance phase that was used to search for industrial assets on a network through ports often associated with SCADA devices. Once in the system, the attackers were able to map out the OT network for further exploitation.
Known threats	Known threat alerts are a common capability among IT security software vendors, but doing so for proprietary OT protocols and artifacts poses a unique challenge, especially when it comes down to understanding the code sections of configuration files. CTD is equipped with known signatures and indicators of compromise (IoCs), as well as proprietary threat signature research from Claroty's own Team82 research team.

	This engine is powered by SNORT and YARA rules and serves to equip threat hunters and incident responders with the context needed to detect and prevent targeted attacks early on in the kill chain. Claroty's YARA and Snort rule engines can even work in code sections downloaded to the PLC, enabling our Deep Packet Inspection technology to assemble code sections to check for threats.
Operational Behaviors	An especially challenging risk to detect in OT environments is when attackers are able to lure standard OT routines into situations that enable them to penetrate the network and execute an attack. However, because these routines are generally standard, anomaly detection engines alone will not identify such an attack. CTD's Operational Behavior engine monitors the context and details surrounding ongoing operations using Deep Packet Inspection technology. It can penetrate operations down to the code level to reveal any changes made to an asset's configuration.
Custom Rules	CTD's last detection engine is the most flexible and relies on specific user-defined events to send alerts. These types of events are often out-of-range values for specific operations, or certain types of communications on the network.

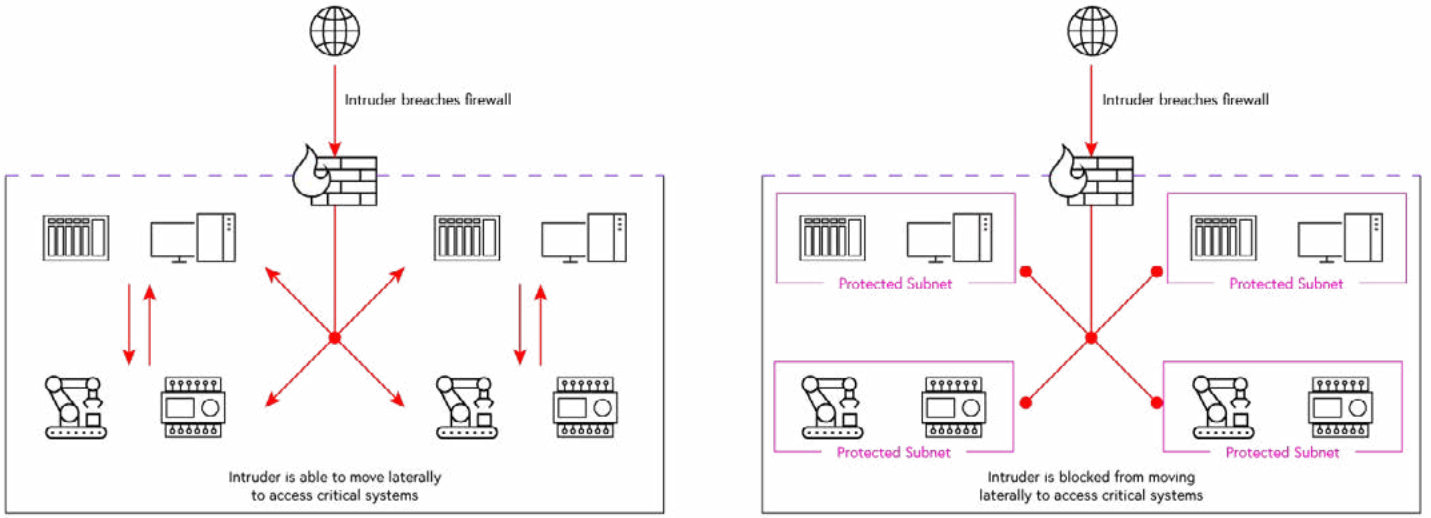
Using preventive maintenance as an example, if your organization has observed changes in packet behavior that often precede unscheduled asset downtime, an alert can be created for this type of behavior. Next time this behavior occurs you will be able to take proactive measures to remediate the asset in question.

COMMON CHALLENGE: NETWORK SEGMENTATION

Segmentation provides an invaluable defense against devastating network breaches by preventing attackers from gaining unfettered access to the network from a single point of entry.

The concept of physical network segmentation is common with IT networks, but it can be a drawn out and costly endeavor that involves investing in additional hardware for the network such as switches, routers, and access points. After identifying what a network actually looks like and how it behaves, understanding which pathways are critical is another major challenge that requires intimate architectural knowledge of the specific network being monitored and the assets within it.

While physical network segmentation might work for IT, industrial networks again pose a unique challenge. Industrial networks control critical processes, so any changes that could potentially cause downtime or disruption are out of the question. In addition, these critical physical systems are often in remote, hard-to-get-to places. OT network segmentation must include easy zone-level separation and cannot require network re-engineering or reconfiguration.



CLAROTY & SEGMENTATION

A cost-effective, efficient alternative to physical network segmentation is using virtual zones.

Virtual Zones are logical groups of similar assets that communicate with each other under normal circumstances. The behavioral patterns that characterize each Virtual Zone are used to create a granular set of rules and policies for how these assets communicate.

Virtual zones can also be used as a blueprint for future physical segmentation efforts, if needed.

Claroty CTD groups all assets into virtual zones using behavioral baselines and then enables users to create zone rules, manage zone policies, and visualize network communication. Virtual zones can help with creating micro-segmentation rules for the network by integrating with existing firewall or Network Access Control (NAC) tools.

The behavioral patterns that characterize each Virtual Zone are used to create a granular set of rules and policies for how these assets communicate. For example, when the system picks up communication between a group of PLCs and a group of HMIs, it will identify things like the communication protocol being used or if they are only performing read-only actions between the two groups. If the communication pattern between these assets were to change, an alert would be raised within the system.

With virtual zones, network segmentation does not have to be a costly and time-consuming endeavor.

COMMON CHALLENGE: VULNERABILITY MANAGEMENT

NIST recommends using several data sources to provide input to the policy engine to make access decisions. One of these input tools is a continuous diagnostics and mitigation (CDM) system to gather information about whether or not an asset has any known vulnerabilities.

OT vulnerability management is not possible without OT visibility. Before your team can evaluate which vulnerabilities to prioritize, they must first determine which common vulnerabilities and exposures (CVEs) exist within your OT environment – which many made-for-IT tools cannot do.

Manually documenting OT vulnerabilities is too complicated, and due to the complexity of industrial environments, it requires specialized technology. Furthermore, given the low tolerance for downtime in industrial and critical infrastructure environments – especially those with 24/7 operations – it would be impossible to patch every vulnerability present in an environment. In many cases, even the most critical vulnerabilities cannot be patched immediately.

CLAROTY & VULNERABILITY MANAGEMENT

The Claroty Team82 Biannual ICS Risk & Vulnerability Report: 2H 2021 underscores that exploitable flaws in ICS and OT products have been on an upward trajectory for some time. What's important now is to reinforce the importance of patching and mitigating vulnerabilities, how the industry is maturing to blunt the impact on software and firmware issues, and what decision-makers need to do to address this risk within the industrial enterprise.

A detailed, accurate inventory of OT assets is a prerequisite for identifying vulnerabilities, but that's just half of the puzzle. To pinpoint vulnerabilities in your environment, you must also be able to match your OT assets with a database indicating which CVEs are present in which assets.

Any such vulnerability database must comprehensively cover a vast array of asset models, firmware versions, and configurations in order to accurately identify all CVEs. And since many OT assets can have a useful life spanning several decades, extensive backlogs of older technologies which may still be in use must be accounted for.

Claroty developed an extensive database of vulnerable protocols, configurations, external connections, and other CVEs. CTD automatically compares each asset in an industrial environment to the database as well as to the latest common vulnerabilities and exposures (CVE) data from the National Vulnerability Database. As a result, users can identify, prioritize, and remediate vulnerabilities in industrial networks more effectively.

COMMON CHALLENGE: ACCESS CONTROL

The zero trust model is often summarized as "never trust, always verify." While many immediately think the application of this is managing device trust within a network, controlling user access to these devices is also a huge part of maintaining zero trust.

Zero trust implementation enforces accurate, least privilege, per-request access decisions for information systems and services.

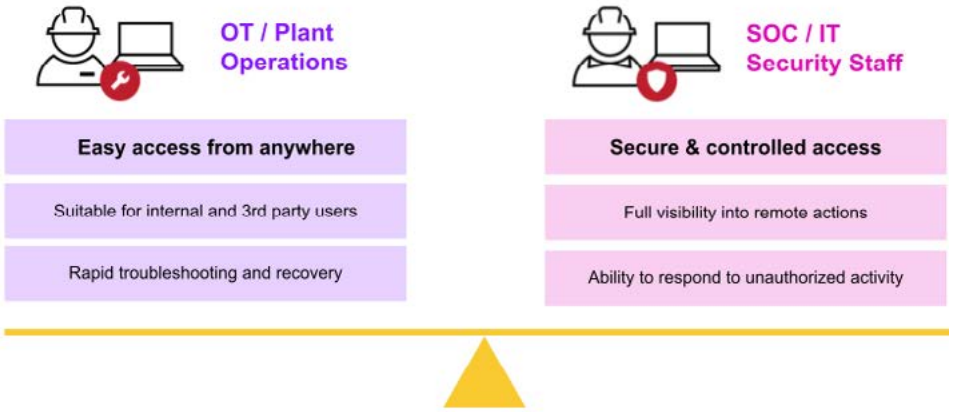
Least privilege user access has long been a challenge for industrial networks for many reasons:

- Access solutions must satisfy the security and usability needs of two types of users: internal and third-party vendors
- OT vendors often have specific requirements (.e.g., cannot share jump servers)
- Access to assets needs to be available for both routine and unplanned maintenance
- Traditional remote access tools were designed for IT networks, so they have cumbersome authentication mechanisms that are not suitable in an emergency

- Tools designed for IT do not offer the level of visibility needed to know who is logging in from where, for what purpose, and whether that purpose is legitimate

When choosing a remote access solution, decision-makers are having to balance different requirements to meet these challenges.

A DELICATE BALANCE OF REQUIREMENTS



CLAROTY & REMOTE ACCESS

Traditional IT remote access tools simply do not meet the needs of both plant operations and security staff. Remote access for industrial networks is only successful when a tool designed for OT is implemented.

Claroty Secure Remote Access (SRA) is the only remote access tool designed for OT. SRA reduces mean time to resolution (MTTR) and boosts uptime by making it faster and easier to connect to and repair OT, IoT, IIoT assets at any time, anywhere. It decreases the complexity and cost of safe, secure, reliable OT remote access by providing flexible configuration options, centralized management, and everything internal and third-party users need. It also minimizes the risks of OT remote access by empowering administrators to control, secure, and gain visibility into all remote connections and activities.

SRA is a unique solution that brings together features designed for OT engineers **and** administrators.

Zero trust access controls: SRA uses granular user access controls and strong authentication methods to ensure only authorized users have access.

Segregation of critical assets: All OT network segmentation is preserved, which eliminates risks of having direct connectivity to assets.

Visibility across all user activities: SRA allows you to monitor a user's session live or through recordings, paired with detailed activity logs of user actions.

Secure file transfer: With integrated anti-virus scanning, SRA ensures only safe files are uploaded and transferred to assets.

Around-the-clock access: Remote access for authorized users is available any time, including for remote sites with low network performance.

SRA integrates seamlessly with CTD to distinguish The Claroty Platform as the industry's first industrial cybersecurity solution to offer fully integrated remote incident management capabilities.

- CTD triggers alerts when users perform unauthorized or abnormal activities
- Risky sessions can be immediately disconnected directly from the alert
- All CTD alerts related to OT remote user activity include a direct link to the associated SRA session and the ability to monitor the session live
- Administrators can immediately disconnect the associated SRA session if necessary

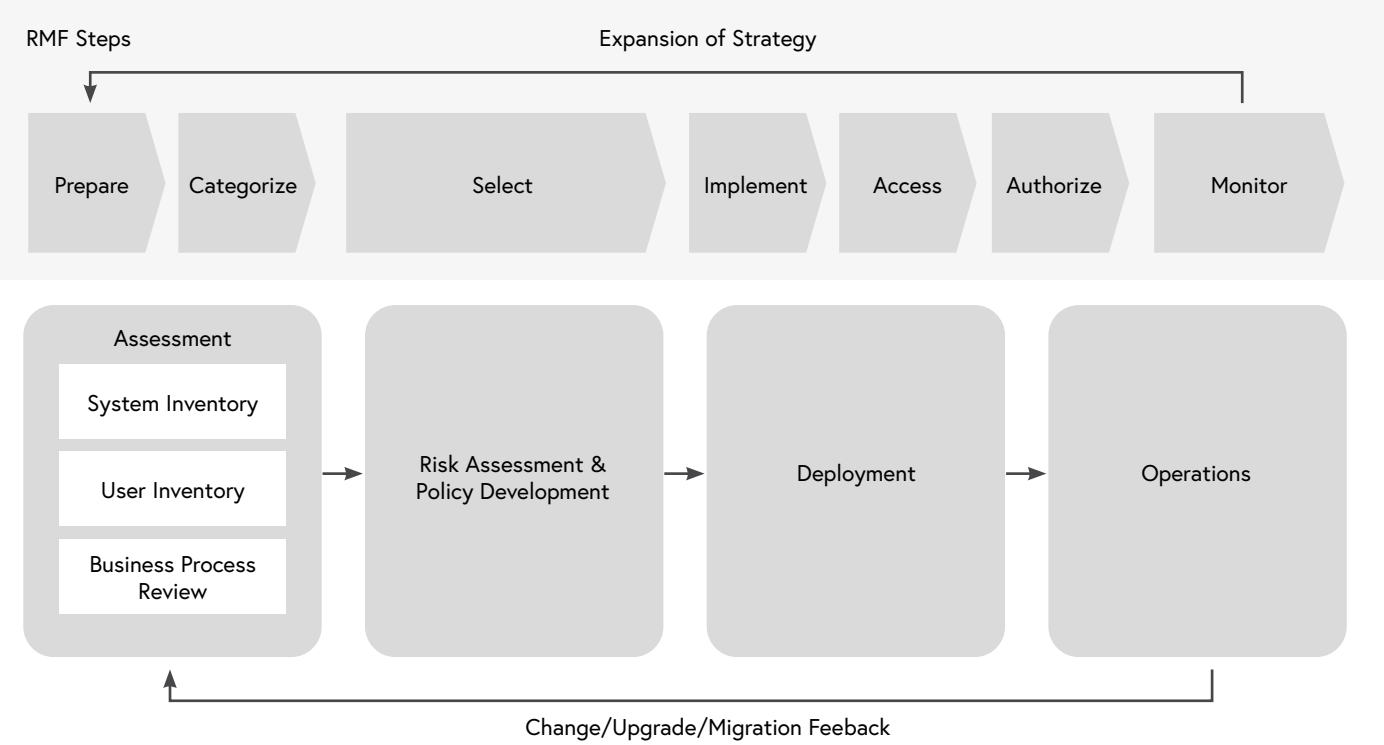


Figure 12: ZTA Deployment Cycle

CONCLUSION

Zero trust should be a lens through which everything happening in an organization's environment is examined. When your organization includes industrial networks and OT, these examinations take on more gravitas because of how much the world relies on cyber-physical systems.

The Claroty Platform brings together the capabilities needed to implement zero trust controls for an industrial environment, regardless of its scale, architecture, or the maturity of the existing cybersecurity programs.

WORKING WITH A PARTNER TO IMPLEMENT ZERO TRUST

The zero trust philosophy is a reflection of a variety of regulations and best practices, and a successful zero trust project is a continuous journey rather than a final destination. Some may opt to partner with a guide as they embark on the path to zero trust. Nearly every consulting firm is offering zero trust services in some form, but choosing a partner that is uniquely positioned to assess, recommend, and solve specific challenges your organization is facing will be imperative for success. ISTARI offers three core services, including strategy training, strategy development, and strategy health checks.

To learn more about Claroty's suite of products that support zero trust, request a demo.

ABOUT CLAROTY

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

ABOUT ISTARI

ISTARI was established in 2020 by Temasek, an investment company headquartered in Singapore, on the thesis that it requires a collective approach of talent, knowledge and technology to become cyber resilient. The client-centric model they created has become our blueprint for working with, investing in and nurturing digital leadership talent for global businesses.

The ISTARI Collective includes Sygnia, Ensign InfoSecurity (EIS), BlueVoyant, Claroty, Armis and Prevalent AI. Headquartered in London, ISTARI has a global presence in the Europe, US and Singapore.

CLAROTY ✦ ISTARI