COLORTOKENS

WHITEPAPER

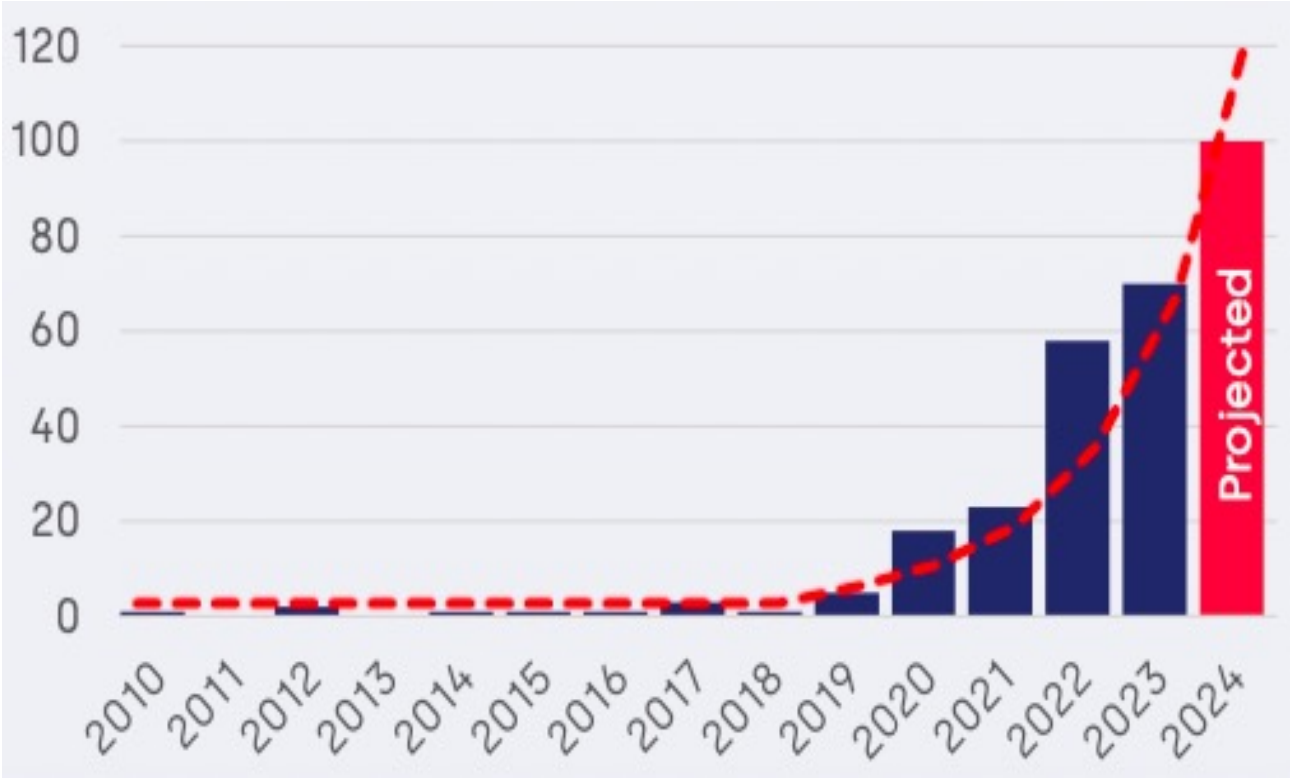
Are Your Operational Technology (OT) Systems Breach Ready?

An operational perspective of a practitioner

OT Systems Cybersecurity Trends – More Challenges Ahead

The next few years will likely see a dynamic landscape of cybersecurity challenges for Operational Technology (OT) or Industrial Control Systems (ICS) or Cyber-Physical Systems (CPS), necessitating proactive measures to mitigate risks and safeguard critical infrastructure and industrial processes. Cyberattacks targeting OT, ICS or CPS are expected to rise in frequency and sophistication.

According to this chart in the '2024 Threat Report' by the cybersecurity firm **Waterfall Security Solutions** and the **ICS STRIVE** incident repository, the attacks on OT infrastructure are nearly doubling annually and predicts 100 attacks with physical consequences in 2024.



Industry 4.0 had a phenomenal impact on how the global production and supply network operates through ongoing automation of traditional manufacturing and industrial practices, using modern smart technology, large-scale machine-to-machine communication (M2M), and the Internet of Things (IoT). This, however, brought new challenges on the cybersecurity front.

Industry 5.0, on the other hand, reflects a shift from a focus on economic value to a focus on societal value, and a shift in focus from welfare to wellbeing based on three key pillars - human-centric, resilient and sustainable. Industry 5.0 is a phase of industrial revolution that uses advanced technologies like artificial intelligence (AI), robotics, and the Internet of Things (IoT) to increase automation and efficiency. However, this increased reliance on digital technologies also brings new cybersecurity challenges.

Challenges associated with Industry 4.0 and Industry 5.0 include:

Increased attack surfaces - The growing number of connected devices and systems creates more potential entry points.

Data security - Industry 5.0 generates and shares large amounts of sensitive data, which must be protected from unauthorized access and theft.

Low-code development platforms - These platforms are used to create repeatable coding platforms, but it's important to ensure the code itself is secure by design.

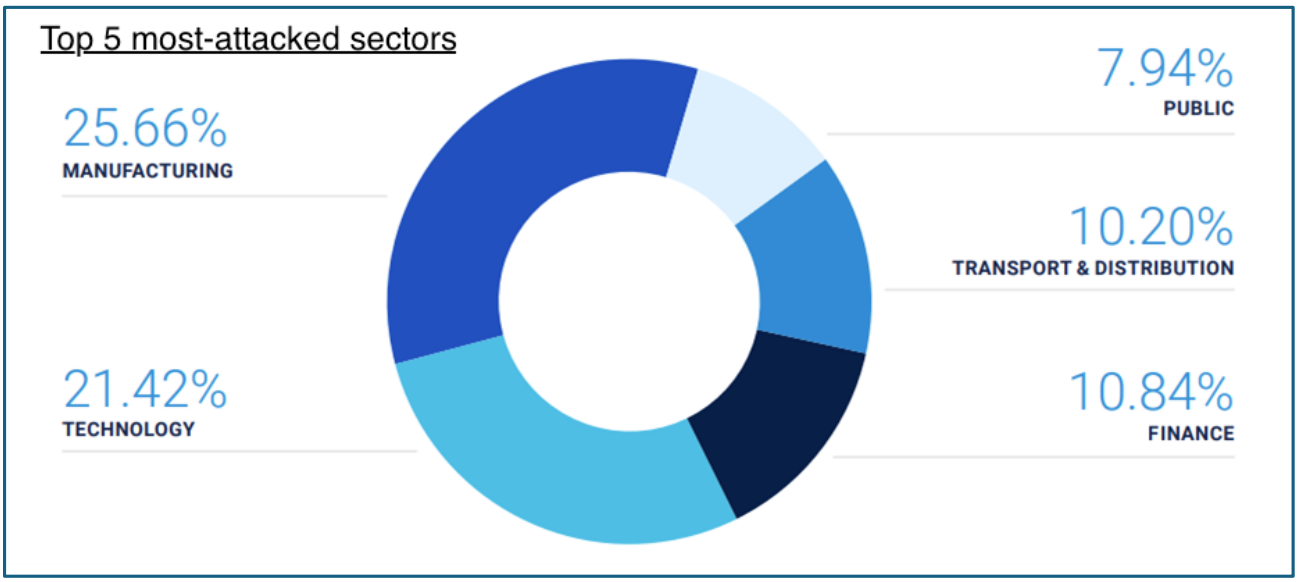
Complex supply chains - Manufacturing companies often have complex supply chains with many interconnected providers and suppliers, which creates a matrix of security considerations.

OT System Breaches with Physical Consequences

The **2024 Global Threat Intelligence Report by NTTDaTa** reveals that manufacturing has now overtaken technology as the most targeted sector, as we see a continued focus from adversaries on targeting supply chain critical infrastructure.

According to a study from British security software and hardware company **Sophos Ltd**, 60% of ransom demands in manufacturing organizations were for $1 million or more and 15% were for $5 million or more. The mean cost to recover from a ransomware was $1.67 million.

The most recent breaches with physical disruptions were not caused by direct manipulation of OT systems (a Stuxnet-like incident) but are downstream consequences of IT-based attacks, most often involving ransomware. Upon discovering a breach in the IT system, the OT system was often shutdown to prevent spread into OT system.



These are a few significant breaches that had physical consequences:

- The Colonial Pipeline ransomware attack in May 2021 is perhaps the most significant publicly declared cyber-attack against essential infrastructure in the U.S. When Colonial Pipeline became aware of the breach, they shutdown all systems including pipelines to lower the exposure. The company paid a ransom of more than $4 million, however it took more than 7 days to restore the full operations. The incident resulted in fuel shortages, fuel price increases and affected dependent industries such as airlines.

- Norsk Hydro, a Norwegian renewable energy and aluminum manufacturing company, faced a ransomware attack in March 2019 which affected thousands of servers and computers. The virus locked everyone out and encrypted key areas of the company's IT network. Hydro didn't pay the ransom and took up the task of removing the virus and rebuilding systems on their own. A bold and commendable move, however, they had to shutdown their OT system fearing the virus would spread into it. Hydro managed to restart the facility quickly with manual operations, but according to their earning report for the year, this incident cost $70 million in losses.
- The Hahn Group, a German industrial automation and robotics company, was the victim of a cyberattack in March 2023. the German manufacturer Hahn Group GmbH switched off all its systems as a safety precaution. A full, clean restoration of its systems took weeks thereafter.
- Belgian glass manufacturer Sprimoglass was hit by a cyberattack in March 2024 that halted its production. Another example of ransomware affecting the production operation and the company choosing not to pay the ransom.
- US paper and packaging manufacturer International Paper was hit by a cyberattack in November 2023. Out of an abundance of caution, International Paper coordinated an orderly shutdown of the mill to address the issue. This attack did affect a limited number of manufacturing systems at the Riegelwood mill.

The Need for Breach Readiness in OT Systems

In the ever-evolving landscape of cybersecurity, the concept of breach prevention has long been hailed as the holy grail of defense strategies. Organizations invest significant resources in firewalls, anti-virus, Endpoint Detection and Response (EDR), encryption, intrusion detection systems, etc. aiming to keep malicious actors at bay. Breach prevention solutions play a crucial role, actively collecting endpoint data to identify compromised systems and contain threats. Their ability to pinpoint infected assets is invaluable.

However, as cyber threats continue to evolve in sophistication and frequency, the vast number of breaches that are still occurring despite the above solutions being in place is a testament to the fact that they are not sufficient. It has become clear that breach prevention methods, while prudent and necessary, are alone not enough to assure the continuity of facility operations. The high number of recently announced breaches attests to this. Beyond breach prevention, organizations must posture their industrial environments to be resilient by design, so they can be positioned to not shutdown OT systems and be able to continue production even in the face of an attack. It has become increasingly apparent that a proactive approach to security is necessary.

Historically, businesses have heavily invested in fortifying their cybersecurity defenses with the aim of preventing breaches altogether. Despite robust prevention measures, cyber threats continue to evolve, making breaches almost inevitable. Relying solely on prevention strategies creates a false sense of security and leaves businesses vulnerable to the evolving tactics of cybercriminals.

Why is breach prevention not always sufficient? Here are some attack vectors to consider: zero-day exploits, insider threats, Advanced Persistent Threats (APTs), and cloud and remote users. **(Want to know more about these attack vectors?** (Click Here)

This acknowledgment prompts a fundamental question: If breaches are inevitable, how can organizations mitigate their impact and swiftly recover? Introducing "breach ready – a strategic shift that places emphasis on preparedness and response rather than solely relying on the prevention of breaches. Breach readiness acknowledges the harsh reality that no system is entirely impervious to attacks. To transition from a reactive to a proactive approach, OT stakeholders must focus on being **Breach Ready** – a strategic shift that places emphasis on preparedness and response rather than solely relying on the prevention of breaches.

One could argue that being breach-ready is more critical for OT systems. Present-day OT systems will typically have a combination of proprietary and non-proprietary hardware and software. Many OT systems currently in the production environment have vulnerabilities. Proprietary hardware and software in OT systems are not immune to cyber threats. There are quite a few vulnerabilities published for proprietary devices. Typically, the timeframe of OT vulnerability resolution through OEM patches can be anything between a few weeks to several months. Shutting down the OT system, with vulnerability, is not an option and OT system must be ready to handle the breach.

The zero-trust approach, specifically **microsegmentation** is instrumental in achieving proactive breach readiness by operating under the assumption that a breach has already occurred, rather than merely focusing on preventing breaches.

The Zero Trust Approach for OT systems

OT systems focus on distributed design such that not all components or functionalities go down simultaneously due to single point of failure. This is done to minimize the impact of an issue (a failure or a breach) and allow uninterrupted control and monitoring of most of the facility.

For OT systems, the focus has been on north-south traffic control and not on east-west (or lateral) traffic. Traditional methods of securing the network perimeter using firewalls and antivirus detection seek to protect against attacks from the external internet. At times VLANs and ACLs are implemented within each level of PERA model, however they provide limited granularity and visibility in managing the east-west traffic. The challenge with this approach is that the adversary needs only to be successful once; the defender must be right every time. All successful ransomware or malware attacks in the past have, by definition, penetrated the perimeter defenses.

There are standards and guidelines specific to OT cybersecurity that are constantly updated to address new challenges due to connectivity and lessons learned in the field. Each one of these standards recommends best practices for implementing Zero Trust Architecture (ZTA) including network segmentation in OT systems.

(Want to know more about Zero Trust Architecture? (Click Here)

- The **National Institute of Standards and Technology** (NIST) **Special Publication (SP) 800-82** provides guidance on how to secure operational technology (OT) while addressing their unique performance, reliability, and safety requirements in energy, manufacturing, transportation, and other sectors.
- **NIST SP 800-82r3** section 5.2.3 elaborates Network Security framework and emphasizes on zero trust approach including network segmentation. While NIST SP 800-82 provides a very good framework for OT cybersecurity, it refers to IEC 62443 for specific approaches.
- **ISA/IEC 62443**[1] , a series of standards developed by the **ISA99 standards committee**, provides a systematic approach to identifying and mitigating cybersecurity risks throughout the lifecycle of OT Systems.
- The IEC 62443 series of standards for OT cybersecurity leverages the Purdue Enterprise Reference Architecture (PERA) model and proposes further segmenting PERA functional levels into zones and conduits. IEC 62443-3-3 section for FR 5 – Restricted data flow specifically recommends logically segmenting networks to reduce exposure of network traffic and reduce the spread of unnecessary and undesirable traffic.

- **U.S. Cybersecurity and Infrastructure Security Agency** (CISA) published a comprehensive guide on the zero-trust maturity model for critical infrastructure. This guide from CISA helps understand the risks associated with interconnected systems and how zero trust principles can help mitigate these risks effectively. In a publication on guidance for Zero Trust, CISA noted - "As a result of the increased interconnectedness within connected communities, traditional perimeter-based security measures are no longer sufficient to protect networks from intrusion and secure critical infrastructure data."
- The National Institute of Standards and Technology (NIST) **Special Publication (SP) 800-207** outlines seven basic tenets of zero trust and ZTA, where data sources and computing services are considered resources; communication is secured regardless of network location; access to individual enterprise resources is granted on a per-session basis; and access to resources is determined by dynamic policy, including the observable state of client identity, application/services, and the requested asset, and may include other behavioral and environmental attributes.
- **CISA's Zero Trust Maturity Model** (ZTMM), which serves as an industry and government-backed approach for zero trust implementation, provides additional context to NIST's zero trust tenets.

The zero trust security approach encourages the practice of micro-segmentation. Connected communities should segment networks into subnetworks to create smaller, more manageable surfaces to protect. This way if a malicious actor gain access, micro-segmentation minimizes lateral movement, contains the threat, and restricts malware from spreading across the entire environment, preventing a breach from becoming a crisis.

Breach Readiness in the IT World

Cybersecurity in the IT world is evolving very fast. The zero trust approach is gaining momentum in the IT world. Microsegmentation is a key element in the zero trust methodology. Technological research and consulting firm **Gartner** predicts that by 2026, 60% of enterprises working towards zero trust architecture will use more than one form of microsegmentation.

Cloud Security Alliance estimates that 91% of organizations will adopt microsegmentation within 12–24 months. The IT world is leading the way in making systems breach ready by implementing microsegmentation.

The Future of Microsegmentation in OT

While OT system stakeholders are open to embracing emerging cybersecurity trends in the IT world, such as microsegmentation, there are certain challenges when it comes to implementing it in OT systems. In many of the breaches experienced by the manufacturing sector, microsegmentation would have enabled stakeholders to not shut down the OT system and continue production.

The current design and requirements of OT systems make it challenging to implement microsegmentation solutions that are available in the IT world. The key requirements of implementing any cybersecurity solutions in OT systems are –

- No adverse impact on the availability of core control, safety, and monitoring functions.
- No changes in the OT network architecture or configuration.
- High availability plus fail-over design/configuration available.
- A robust and proven solution.
- Support for proprietary hardware and software, legacy systems and other non-agentable systems, without the need for any upgrades or major changes in the OT system.
- Intuitive visualization to understand and categorize traffic.
- Easy and seamless implementation, without need for the OT system downtime.
- Comprehensive reporting and audit trail features that can also help in incident investigation.

ColorTokens' Agentless Xshield Enterprise Microsegmentation Solution is Designed for OT Systems

ColorTokens is recognized as a **leader in microsegmentation solutions** in the **Forrester Wave Q3 2024** report. ColorTokens' agent-based solution is widely implemented in numerous organizations and facilities. However, OT requirements, as explained above, needed an appropriate solution. ColorTokens designed an agentless solution using an appliance called the Xshield Gatekeeper. The Gatekeeper connects to the OT network switch like any other OT device (on the side and not physically in-line) and enables the Xshield platform to provide all the functionality that its agent-based solution would provide.

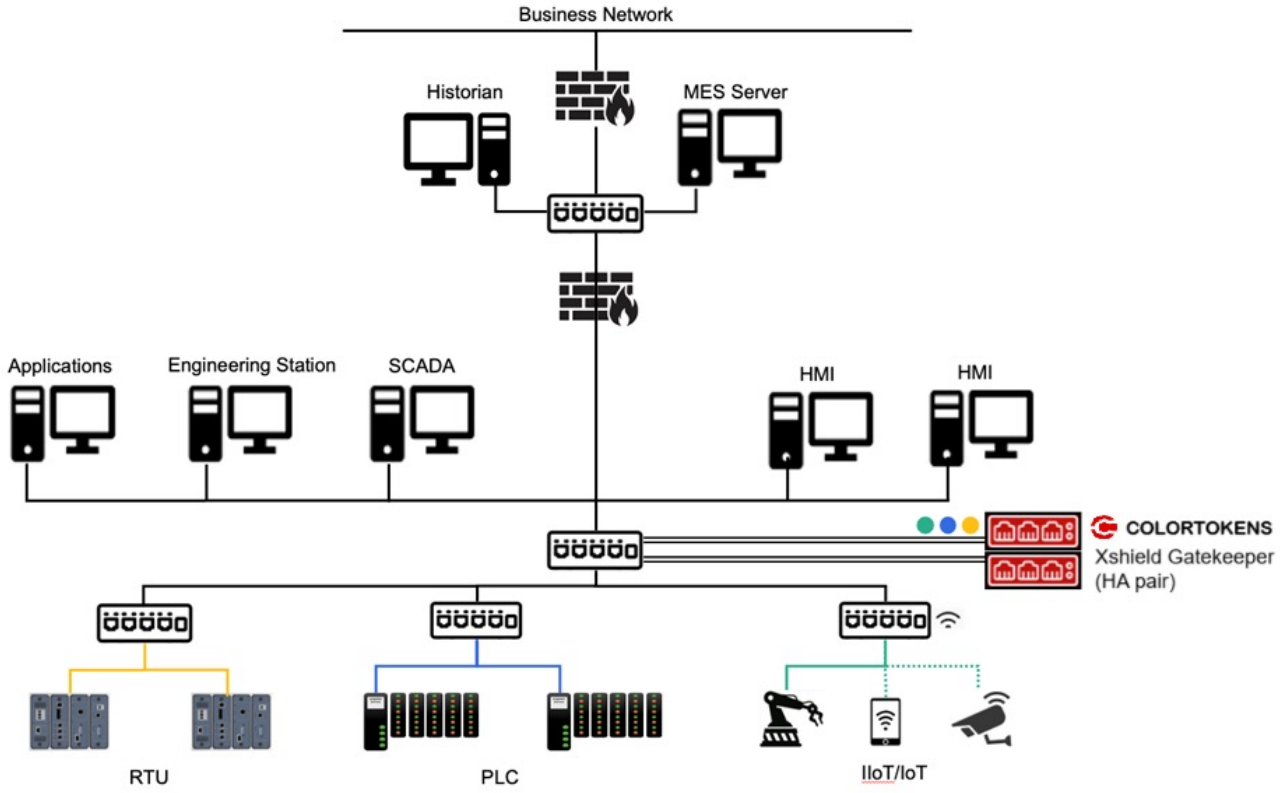


Figure 1 Gatekeeper Installation in OT Network

The Xshield Gatekeeper, as shown in Figure 1, is typically installed on a distribution switch. It can manage any IP based devices connected to the network. It also works across VLANs if the VLANs are extended to the switch where it is connected. A high availability configuration (redundant Gatekeepers) is provided for OT applications. Fail Open configuration is also supported to fail over to switch in case of an unlikely scenario of failure of both the Gatekeepers. The Xshield Gatekeeper deployed in critical applications is a server-grade appliance with dual power supplies and high-speed network interfaces. Gatekeeper specifications are selected based on the number of devices that need to be managed. The Xshield Gatekeeper runs on hardened Ubuntu Linux.

The key is to make this Xshield Gatekeeper a gateway for all devices that you would like to manage through the Xshield enterprise microsegmentation platform. This can be easily done by configuring Gatekeeper as a DHCP Relay. The Gatekeeper can also work as DHCP server, if that is the preferred option.

It is not unusual to have a static IP address for OT devices. For such devices IP address change is NOT required. The only changes you need to make for such devices is to configure the Gatekeeper as a gateway and subnet mask as /32 or 255.255.255.255. No changes are required in network topology or switch configuration.

Devices with static IP addresses, for which the gateway is not changed to the Gatekeeper, would continue their communication through the original gateway and the traffic won't be routed through the Gatekeeper.

Implementing Microsegmentation in OT Systems Seamlessly with ColorTokens' Solution

The focus of ColorTokens' agentless solution for OT system is seamless implementation. The Gatekeeper can be installed with the complete ColorTokens Xshield suite by a simple process which can be performed before connecting the Xshield Gatekeeper to the switch. This is a standard process, and it involves downloading an ISO image, make a bootable USB flash drive, and booting the appliance from this USB drive. The interactive and simple menu will allow you to install the ISO image on the Gatekeeper quickly.

At this point your Xshield Gatekeeper is ready to connect to the network switch. You will connect the WAN (or Upstream) and the LAN (or Downstream) ports of each Gatekeeper in the HA pair to the switch. If you haven't configured and registered the Gatekeeper, the configuration menu will be presented to do the initial set up. You will need to determine your WAN IP addresses (and Virtual IP address, in case of HA configuration). In this initial setup you can configure the WAN set up and register the Gatekeeper on the ColorTokens portal on the tenant specifically created for the end-user organization.

Once you have completed registration, the Gatekeeper will be visible to the tenant users on the ColorTokens portal and from this point you can configure policies on the Xshield Gatekeeper and manage policies from the web-based Xshield administrator console UI.

The next step is to configure the LAN-side of ports from the UI. You can optionally make the Gatekeeper a DHCP Relay or Server. For devices with static IP addresses, you will need to change the subnet mask to /32 with the Gatekeeper as a gateway.

At this point, the Xshield Gatekeeper will start discovering all devices on the segment and VLANs. For supported OT communication protocols , Xshield would also bring valuable information such as manufacturer, model number, version number and serial number. You can tag, categorize, or group devices for intuitive visualization and policy deployment.

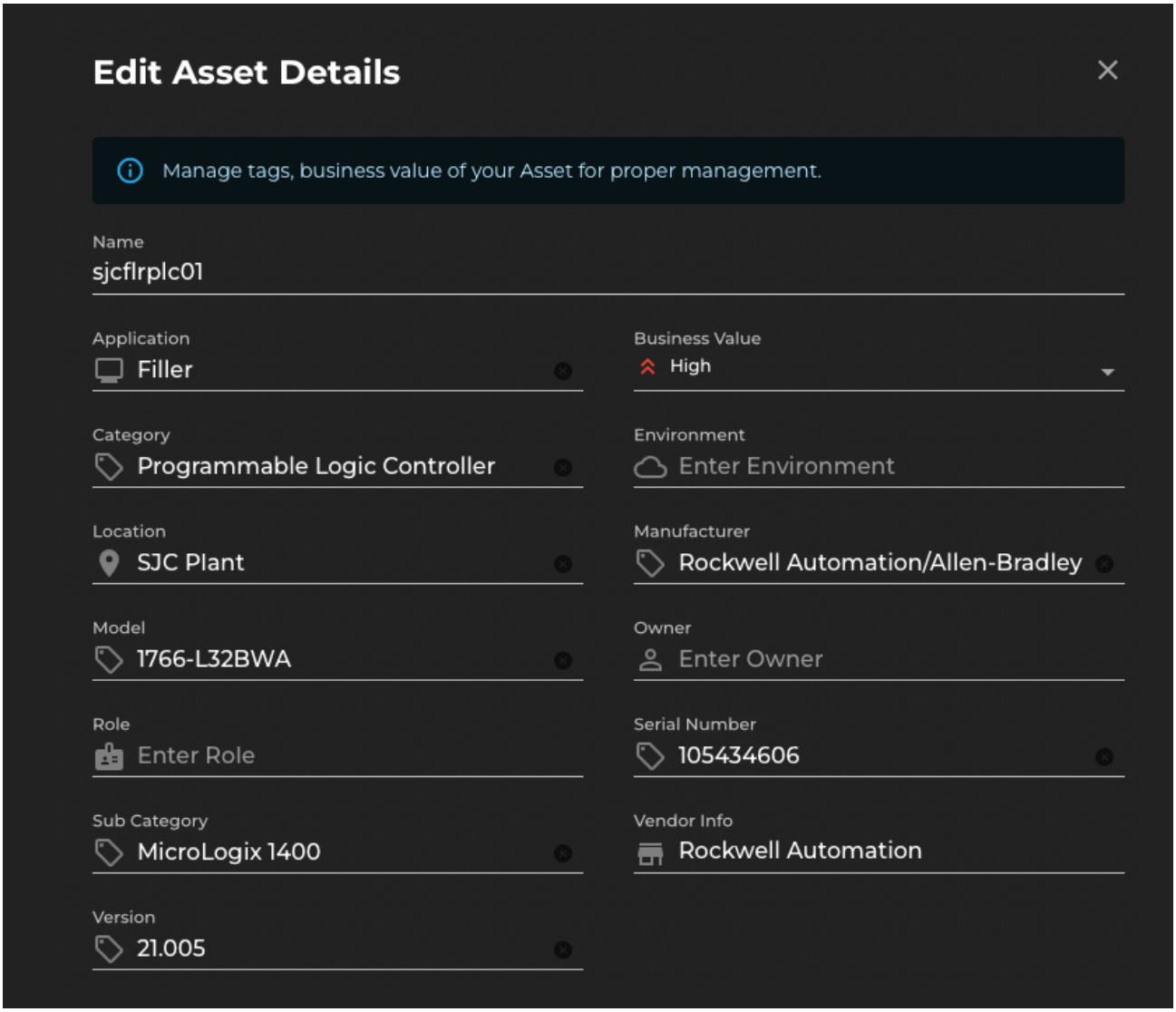


Figure 2 Example of PLC Device Recognition by Xshield

ColorTokens can use information from the end-user's existing or chosen asset visibility solution, if it can provide information through the open-standards-based API. In addition, ColorTokens partners with **Claroty** and supports integration with their **xDome** platform.

You can choose devices to be managed by the Gatekeeper. You will start seeing traffic for all managed devices in the Xshield console. You are now ready to start implementing policies which can be done incrementally, one device or group of devices at a time.

Xshield provides two very important features to make your policy enforcement experience seamless and easy.

- Policy Test Mode: One can simulate impact of policy enforcement before you implement it.
- Template-based Deployment: For repetitive applications, users can create policy templates for efficient deployment.

Flexible, Real-time and Multi-dimensional Visualization

The visualization of assets and telemetry traffic is configurable along many dimensions for different user personas in the enterprise: infrastructure teams, application teams, and security teams.

The ColorTokens Xshield solution provides powerful foundational functionality needed for an OT cyber defense strategy, covering the key areas of visibility and microsegmentation.

The result is an enterprise architecture that is resilient by design so that the impact of an inevitable breach that enters the environment from either the IT network or the Industrial network is contained before critical damage occurs.

The journey to zero trust microsegmentation begins with a map. As shown in the Figure 3 below, Xshield discovers and visualizes all your network assets, devices, applications, and their dependencies.

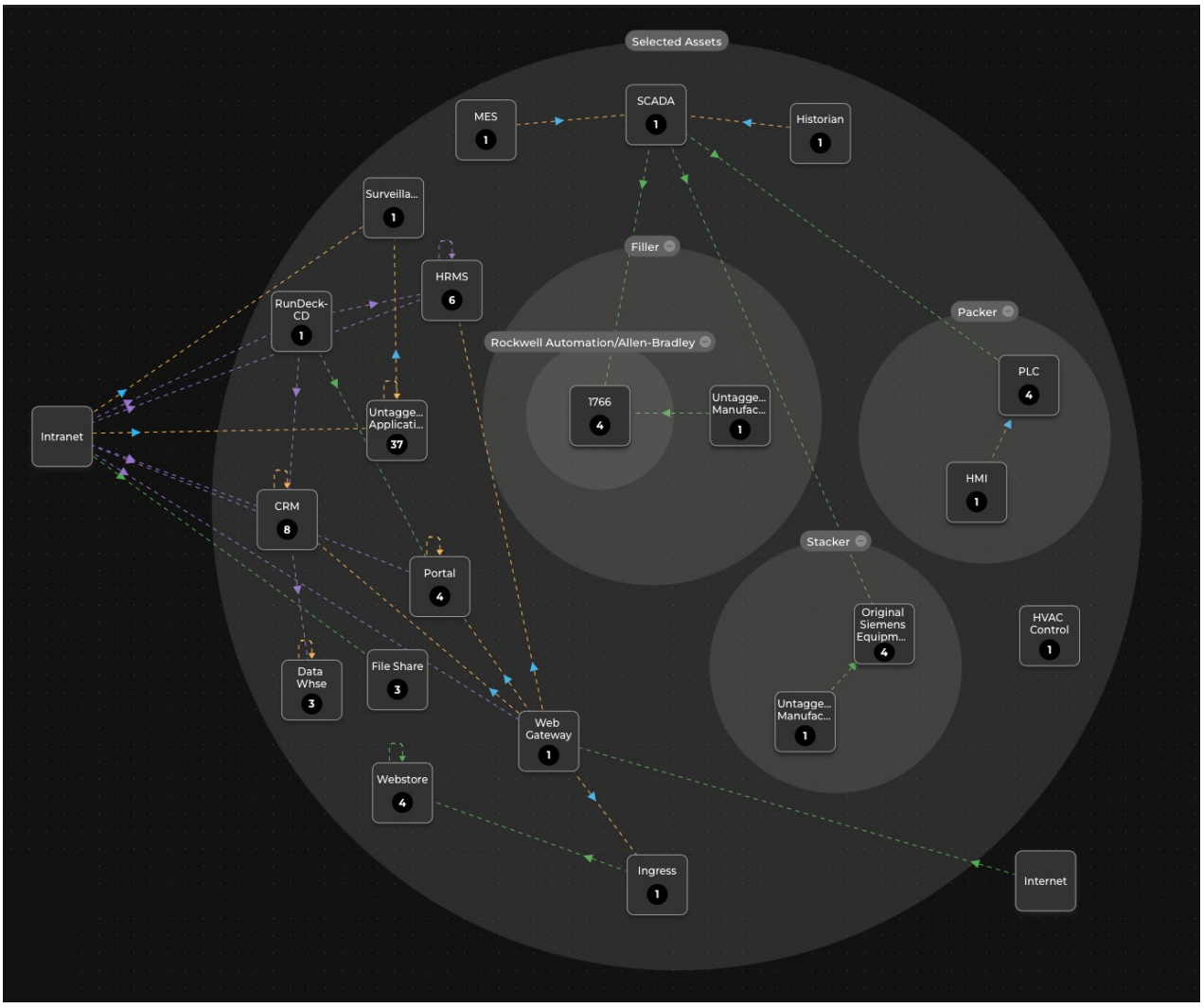


Figure 3 The ColorTokens Xshield Asset and Traffic Visibility Console

After visualization the Xshield administration console lets you set access and traffic policies to protect your network from lateral movement of malware or ransomware. Xshield's policy autosuggestion and reusable policy templates facilitate your policy authoring phase.

The Xshield Enterprise Microsegmentation platform lets you manage multiple types of policy enforcement points, both agentless and agent-based, from the central policy decision point. There is no need to maintain different tools to protect today's diverse network topology which includes data center servers, cloud workloads, Kubernetes containers, OT/IoT and user endpoints. This simplifies administration and saves on staffing and training.

Xshield uses an innovative approach to microsegmentation implementation: it immediately improves your security posture by giving you risk-appropriate enterprise-wide control of risky ports and sensitive or privileged flows. Then it progresses to continuous improvement with fine-grained application-specific zero-trust controls, as shown in the Figure 4 below.

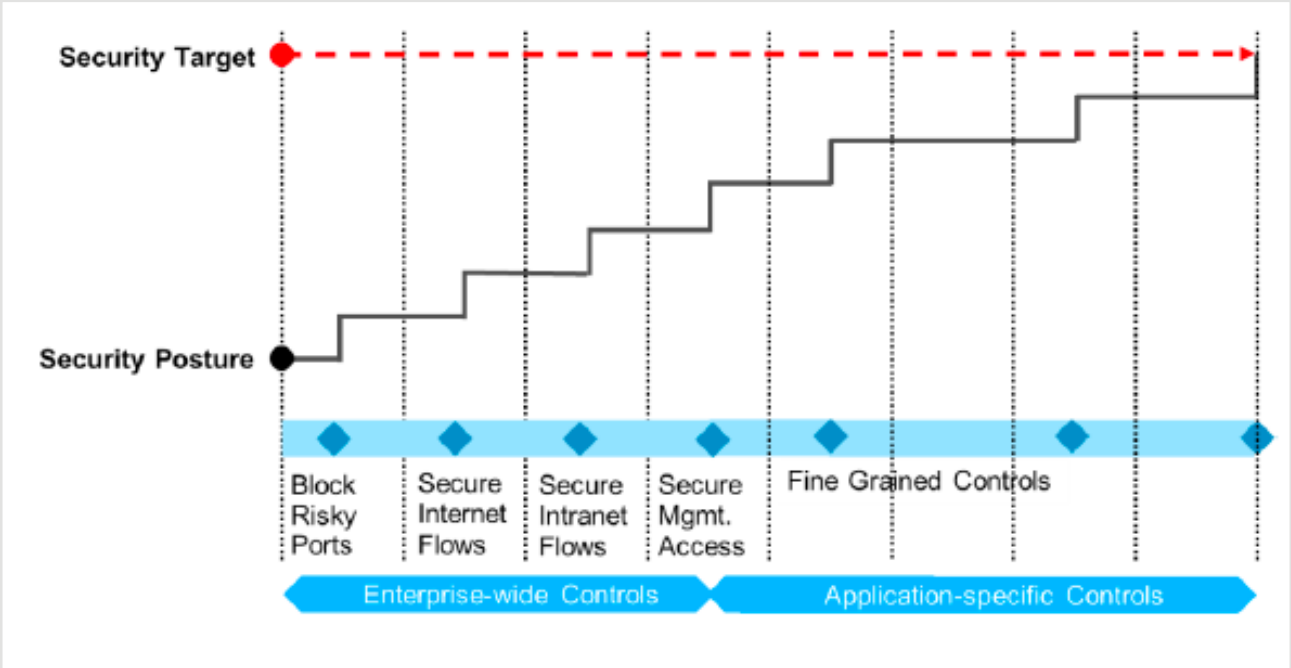


Figure 4. Immediate security benefits and continuous incremental improvement

Xshield lets you measure risk and communicate the immediate and on-going improvements in your security with dashboard visualizations.

Figure 5. Xshield Risk Dashboard

About ColorTokens:

ColorTokens, the premier enterprise microsegmentation provider, specializes in making organizations “breach ready” by halting the lateral spread of ransomware and malware within intricate network infrastructures using its innovative ColorTokens Xshield™ platform. The platform visualizes traffic patterns between workloads, devices, and users, enabling organizations to enforce granular micro-perimeters, swiftly isolate critical assets, and respond to breaches effectively. By thwarting ransomware and malware attacks, ColorTokens safeguards businesses, ensuring significant savings in potential disruptions. A US corporation headquartered in Silicon Valley, ColorTokens has offices in the US, the UK, Europe, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please go to colortokens.com