Simple and Non-Disruptive Segmentation for Zero Trust in OT

Safely Secure OT Networks with Advanced Risk Management and Dynamic Segmentation

"IoT and network-enabled device technologies have introduced potential compromise of networks and enterprises... Security teams must isolate, secure and control every device on the network, continuously."

— *Mitigating Ransomware With Zero Trust, Forrester Research, June 8, 2020*

Traditional approaches for securing operational technology (OT) assets have long depended on maintaining the strict separation of industrial applications from IT business networks and external services. However, the digital transformation of industrial control systems (ICSs) has introduced remote access, cloud-based services, smart working and hybrid environments where IT, IoT and OT technologies work together to improve efficiency and increase profitability. Add the rise of sophisticated, targeted attacks on industrial infrastructure and converged networks and it's clear: traditional zoning strategies are no longer sufficient to keep OT/ICS environments secure.

Challenges in OT/ICS environments include:

- Increasing interdependency and interconnectivity between IT, IoT and OT systems, often distributed across multiple geographic locations
- Lack of basic authentication methods in controllers or other field devices
- Inability to detect and mitigate lateral movement of malware and malicious actors, inter-zone threats crossing over from IT, and remote users impacting cyber-physical and OT infrastructure
- Heterogeneous device and vendor landscape with inconsistent policy controls across OT environments

When applied in a way that meets the specific needs of OT/ICS, segmentation can improve an organization's security posture against an ever-evolving threat landscape and improve operational efficiency.

Why we need segmentation for OT/ICS

ICSs are complex, multi-vendor environments, often with geographically distributed resources and management systems. Each system has its own proprietary protocols and industrial applications, security requirements, and specific risk mitigation policies. OT operators and security team have to manage an increasing number of remote connections and transient assets – OT/ICS and SCADA engineers, system integrators or OEM vendors

Instead of patching, insecure-by-design OT devices must often be segmented from other parts of the network and monitored to detect unwanted changes

all connect to the OT networks, both locally and remotely, to support management and maintenance functions.

No wonder the classic IT approach doesn't work in OT/ICS environments. Most SCADA systems or controllers do not support authentication mechanisms, and traditional routers and firewalls cannot enforce security policies based on the content of network traffic (e.g., dangerous commands or unexpected process values). Nor is it enough to depend on security at the edge of the network. More protection is needed inside the network, where different OT and IoT assets and systems must communicate with each other and often rely on connections to other industrial subsystems to run the process.

While we all agree that zero trust network segmentation is a fundamental part of any cybersecurity framework, it remains very difficult to implement in an ICS environment because of the specialized expertise required – regarding OT and IoT device types, their roles in the control system, their security and operational risk, and their interconnectivity and interdependencies. Both your vendor and in-house team need this understanding to make informed decisions about how to segment and build zero trust policies without impacting industrial processes and causing downtime.

Risk management and zero trust segmentation for IT-OT networks

Forescout Continuum Platform helps you manage cybersecurity and operational risk and optimize mitigation while laying the foundation for zero trust segmentation across all cyber assets. With Forescout Continuum, you can:

- **Accelerate zero trust segmentation** across IT and OT groups using device profiling and control system baselines to draw granular policies
- **Gain an instant understanding of IT-OT segmentation state** in real time on any device, anywhere in the extended environment
- **Visualize traffic flows** based on logical taxonomy of users, applications, services, functions, locations, devices and risk level
- **Reduce the attack surface and maintain compliance** through dynamic segmentation across IT, IoT and OT networks
- **Optimize IT-OT workflows** and leverage existing investments with a consistent segmentation policy across the entire enterprise
- **Reduce compliance risk and cost** by efficiently managing inter-network access, requiring fewer hands on deck
- **Detect, isolate or block insecure and unwanted network traffic**, unauthorized access and non-compliant devices

Forescout Continuum provides in-depth device visibility for OT networks and enables effective, real-time management of a full range of operational and cyber risks. The solution addresses your cross-domain, multi-use-case segmentation, and risk-mitigation challenges across your digital terrain, including OT and IoT environments, to accelerate nondisruptive threat detection and response.

The platform helps you design and deploy zero trust segmentation by automatically mapping traffic flows to a logical taxonomy of users, applications, services, functions, locations, devices and risk levels across the entire enterprise network.

You're able to baseline OT and IoT traffic in real time without deploying agents or re-architecting infrastructure. Most importantly, you're able to model the impact of segmentation policies before enforcing them.

Forescout Continuum protects critical infrastructure with patented anomaly detection and deep packet inspection (DPI) and a vast library of ICS-specific threat indicators. The platform monitors network communications in real time and provides rich contextual information about connected assets, protocols and content of communications.

With powerful functions such as Advanced Alert Aggregation and Asset Baselining, you can automate threat-detection and compliance tasks that reduce risk and support OT segmentation enforcement. For example, you may need to activate temporary segmentation policies to isolate vulnerable assets and contain detected malware threats.

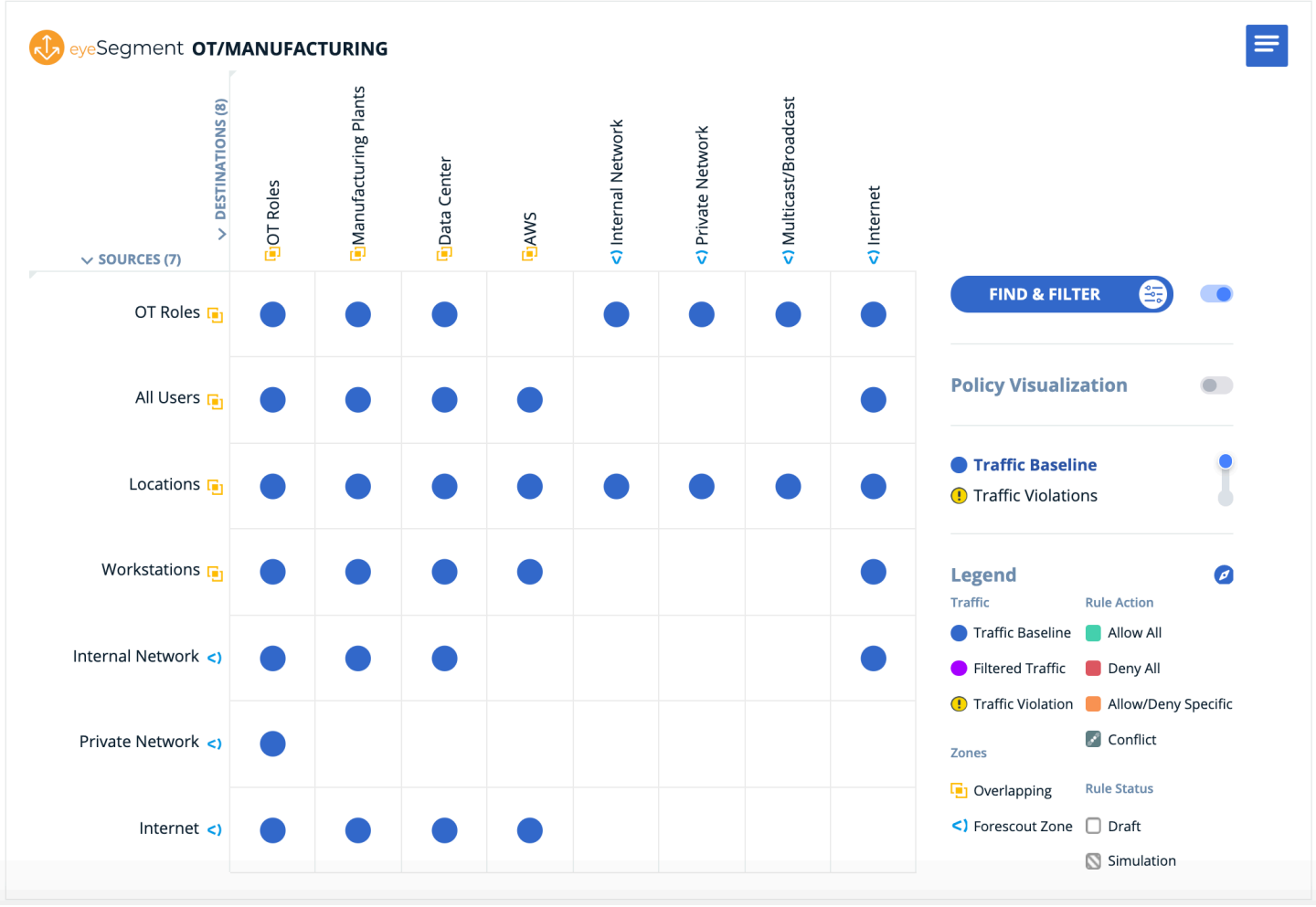

Figure 1. The Forescout segmentation matrix allows you to focus on what is important to you so that you can analyze and investigate a particular traffic pattern in your environment. No matter where you are in the matrix hierarchy, you can instantly create desired policies to segment a specific traffic pattern to protect your business while ensuring production and business continuity.

Forescout's dynamic network segmentation solution addresses a wide array of use cases for OT and IoT. In every case, the platform's flexibility helps to reduce the risk of business disruption and minimize operating costs related to segmentation projects. Below are a few key use cases:

- Monitoring and assessing the security posture of a vendor or contractor accessing the OT network, remotely or while on-site, and granting access only to the required network segments
- Segmenting IT and IoT networks from OT networks as well as segmenting unpatchable assets
- Simulating changes to OT segmentation policies and visualizing the implact on traffic flows so you can fine-tune policies without causing disruption

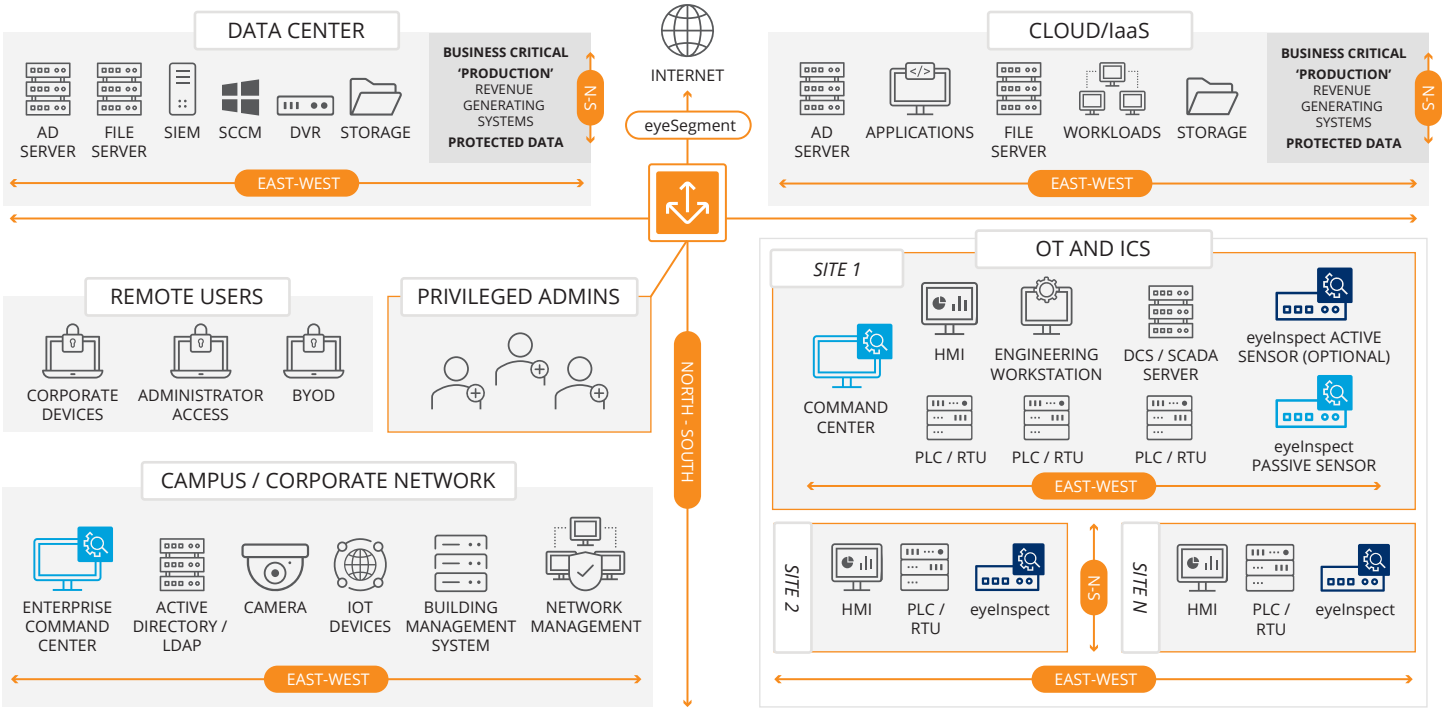

Figure 2. Forescout Continuum can help you mitigate threats and gain an instant understanding of your segmentation state in real time. Here, Forescout's segmentation component, eyeSegment, keeps connected devices from crossing IT-OT domains while Forescout's network monitoring and threat detection component, eyeInspect, monitors for cyber and operational risks in the OT/ICS environment. In this way, segmentation policies can be updated dynamically as the threat landscape changes.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com