‹›) FORESCOUT®

Active Defense for the Enterprise of Things.

Simple and Non-Disruptive Zero Trust Segmentation for OT

Safely Secure Extended OT Networks with
Advanced Risk Management and Dynamic Segmentation

Traditional approaches for securing OT (operational technology) devices on OT and ICS networks have long been dependent on maintaining the separation of industrial applications from IT networks and remote-access users. However, as OT organizations modernize their infrastructure with new technologies, such as Cloud SCADA, DCS and advanced Manufacturing Execution Systems (MES), traditional zoning strategies are no longer sufficient to keep OT environments safe.

Challenges in OT environments include:

- Risk of lateral movement of malware and malicious actors, inter-zone threats crossing over from IT, and remote users impacting cyber-physical and OT infrastructure
- Detection and mitigation of malware spread and inter-zone threats that affect cyber-physical and OT infrastructure
- Multivendor operational complexity and inconsistency in segmentation controls across extended OT environments

The Forescout Solution: Best in class for OT

If the challenges above sound familiar, now is an excellent time to evaluate the Forescout solution. It can help you simplify Zero Trust segmentation and optimize risk management when it comes to IT, OT and ICS devices in your heterogeneous Enterprise of Things (EoT). With the Forescout platform, you can:

"By 2021, 80% of industrial IoT [IIoT] projects will have OT-specific security requirements, up from 40% today." [1]

GARTNER

"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." [2]

FORRESTER RESEARCH

1

- **Accelerate Zero Trust segmentation** across IT and OT groups
- **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 environments
- **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

"Almost 20% of organizations observed at least one Internet of Things (IoT)-based attack in the past three years." [3]

GARTNER

Optimized Risk Management and Zero Trust Segmentation for IT-OT Networks

The Forescout solution 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 organizations' cross-domain, multi-use-case segmentation, and risk-mitigation challenges across extended OT environments to accelerate non-disruptive threat detection and response.

Forescout eyeSegment 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. This makes it possible to baseline OT traffic in real time without deploying agents or re-architecting infrastructure. It also lets you model the impact of segmentation policies before enforcing them.

EXTEND THE VALUE OF YOUR SECURITY & IT INVESTMENTS

- Address IT-OT convergence risk (lateral movement) with a unified segmentation policy approach
- Address OT device-related risk with granular segmentation policy planning, monitoring and response
- Enable non-disruptive and dynamic segmentation for sensitive OT environments by leveraging existing investment (infrastructure)

2

Forescout eyeInspect (formerly SilentDefense) protects critical infrastructure with patented deep-packet inspection (DPI) and a vast library of ICS-specific threat indicators. eyeInspect monitors network communications in real time and provides rich contextual information about network 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.
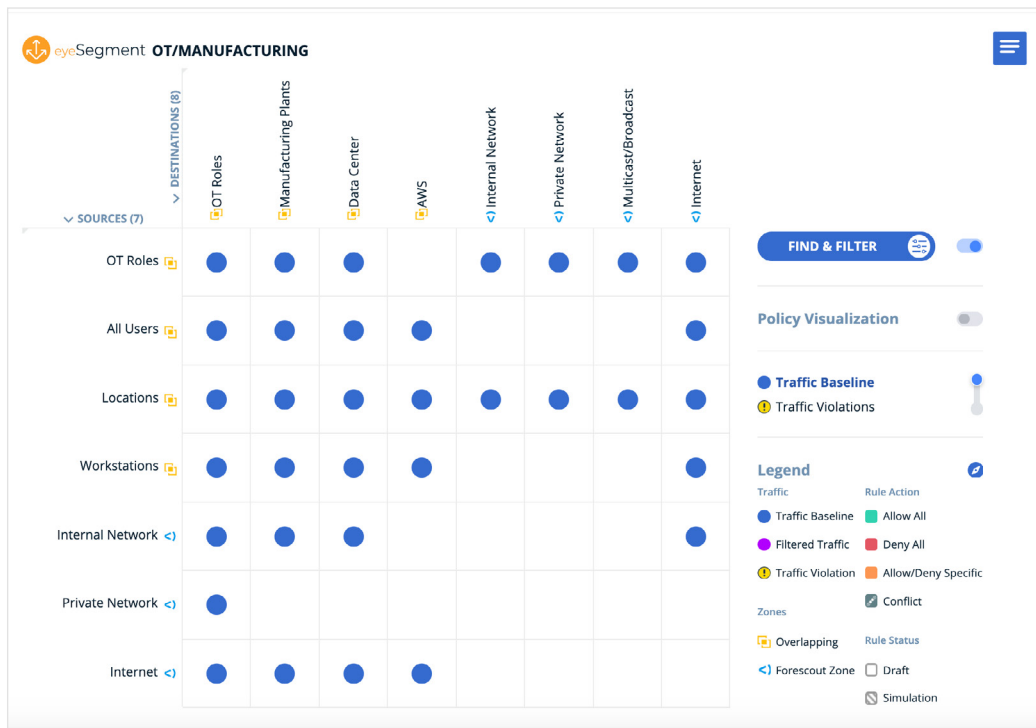

Figure 1. The eyeSegment matrix allows you to focus on what is important to you so that you can analyze and investigate a particular traffic pattern in your environment. No matter where you are in the matrix hierarchy, you can instantly create desired eyeSegment policies to segment a specific traffic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

The Forescout network segmentation solution addresses a wide array of use cases for OT. In every case, the Forescout 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:

- Mitigate risk, maintain compliance and reduce operational costs across OT networks

- Gain instant visibility into OT environments in real time to model non-disruptive segmentation policies

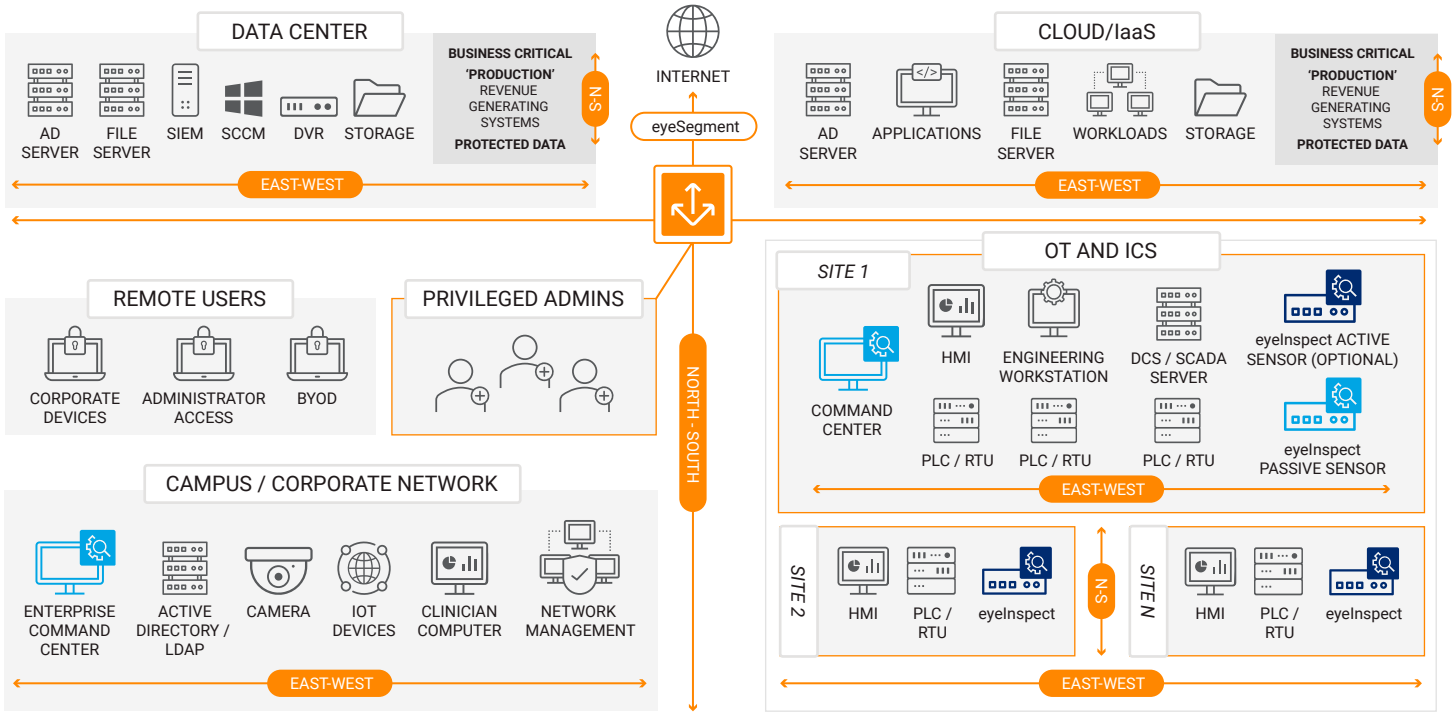- Accelerate IT-OT Zero Trust segmentation

Figure 2. The Forescout solution can help you mitigate threats and gain an instant understanding of your segmentation state in real-time. In the example above, eyeSegment keeps connected devices from crossing Healthcare and IT-OT domains.

1. Invest Implications: 'Cool Vendors in Industrial IoT and OT Security, Gartner Research, April 2018
2. Mitigating Ransomware With Zero Trust, Forrester Research, Inc., June 8, 2020
3. IoT Security Primer: Challenges and Emerging Practices, Gartner, January 2020

Don't just see it.
Secure it.

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeSegment   salesdev@forescout.com   toll free 1-866-377-8771

<) FORESCOUT.
Active Defense for the Enterprise of Things.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com