FORESCOUT
Active Defense for the Enterprise of Things™

Non-Disruptive Zero Trust Segmentation for Healthcare

Actively Defend Extended Healthcare Networks with Advanced Risk Management and Dynamic Segmentation

Traditional approaches for maintaining secure healthcare networks have long been dependent on maintaining separation of healthcare applications from IT networks and remote access users. However, as healthcare organizations modernize their infrastructure with new technologies such as IoMT (Internet of Medical Things) devices and cloud applications/services, traditional zoning strategies are no longer sufficient to keep healthcare environments safe.

Challenges include:

- Risk of lateral movement of threats that cross from IT and remote users into cyber-physical and extended healthcare infrastructure
- Difficulties related to detecting and mitigating the spread of inter- zone threats
- Multivendor operational complexity and inconsistency in segmentation controls across extended healthcare environments

> **“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.”** [1]
>
> FORRESTER RESEARCH

The Forescout solution: Best in class for healthcare

If the challenges above sound familiar, now is an excellent time to evaluate how Forescout's solution can help you identify, segment and enforce compliance of IT, IoT, OT (operational technologies) and IoMT devices in your heterogeneous Enterprise of Things. With the Forescout platform, you can:

- **Gain real-time insights about IT-OT and healthcare network segmentation states** of any device, anywhere
- **Identify, classify and segment medical devices running legacy OSes**
- **Accelerate Zero Trust segmentation to prevent known threats and reduce risk** across IT and Medical groups
- **Simplify threat analysis** with fewer tools and dashboards
- **Optimize IT-healthcare workflows** and leverage existing investments with a consistent segmentation policy across the entire enterprise
- **Mitigate risk and maintain compliance** through faster threat response by prioritizing alerts according to the risk level
- **Reduce compliance risk and cost** by efficiently managing cybersecurity detection and response, requiring fewer skilled personnel
- **Map and visualize network flows** to identify and eliminate the use of insecure, clear-text protocols

EXTEND THE VALUE OF YOUR SECURITY & IT INVESTMENTS

- Help security and clinical engineering teams address risk and compliance with a unified segmentation policy approach
- Enable non-disruptive and dynamic segmentation for sensitive healthcare environments by leveraging existing infrastructure investments

> **"Connected medical devices represent a fast-growing threat attack vector, and the lack of device manufacturer standardization and interoperability has created a significant problem for clinical care network operations."**
>
> **PEDRO ABREU**
> **Chief Product and Strategy Officer, Forescout**

REDUCE RISK

Optimize risk management using automated policies

Forescout provides in-depth device insight and enables effective, real-time management of a full range of operational and cyber risks. It uses granular device insights to streamline and simplify management while also mitigating the risk of compromise across disparate device types and network tiers.

The Forescout platform:

- Continuously discovers, assesses and classifies all IP-connected IT, IoMT, OT and IoT devices
- Determines compliance status by using non-disruptive profiling capabilities and granular medical device details
- Identifies and helps you eliminate weak and default passwords
- Applies network access controls and orchestrates safe device remediation workflows

> **"Forescout identifies and classifies the device, injects the information from the SIEMs and moves that device over to a segmented network. This is how we're getting to Zero Trust."**
>
> **DOMINIC HART**
> **Manager Information Security Architecture, IT&S Security, RWJBarnabas Health**

SAFELY SEGMENT

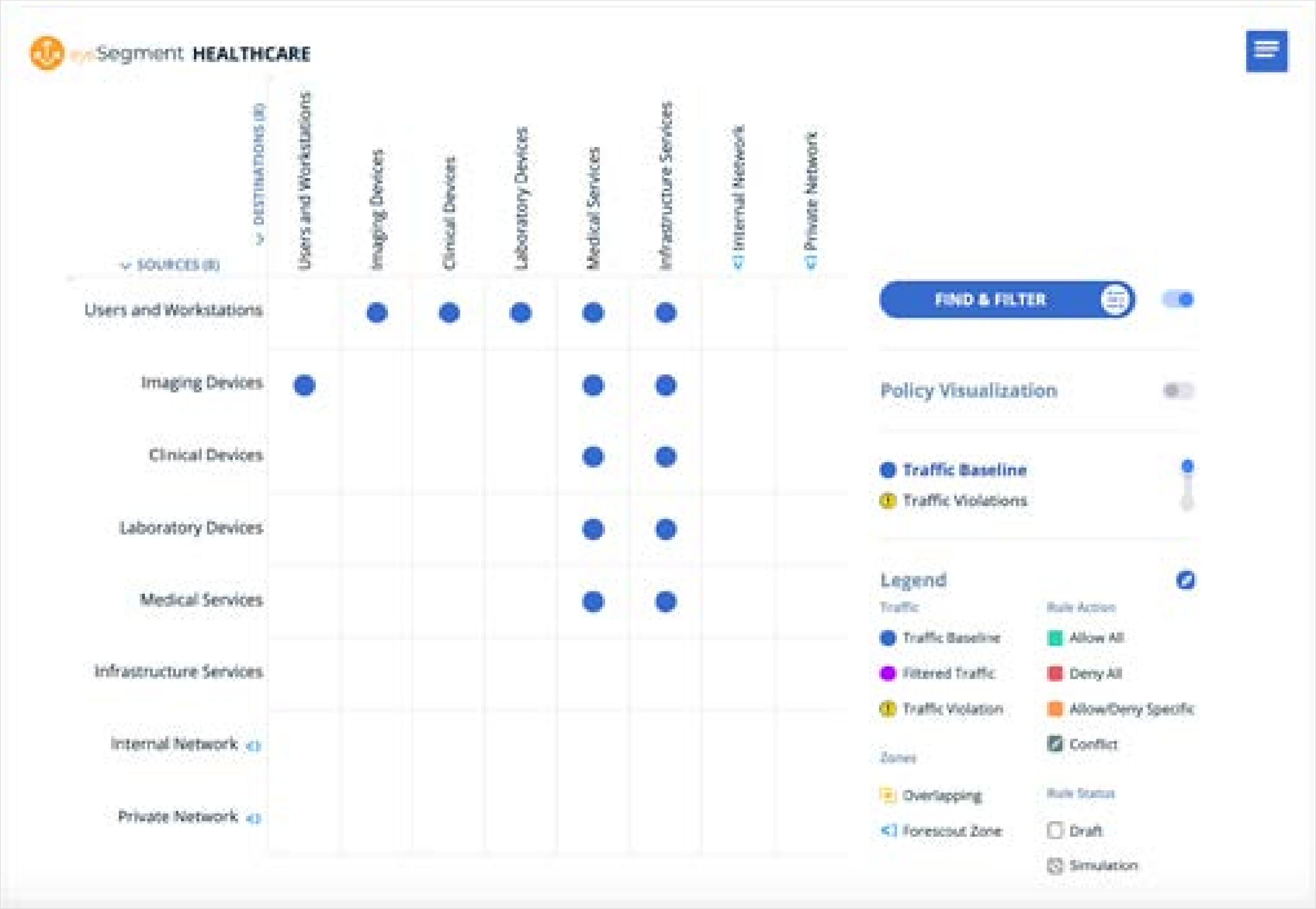
Model and apply non-disruptive network segmentation

Address your cross-domain, multi-use-case segmentation challenges across extended healthcare environments to simplify and accelerate non-disruptive Zero Trust segmentation controls. With Forescout eyeSegment as part of the solution, you can:

- Visualize and assess your network segmentation state in real time
- Build more accurate and effective segmentation policies
- Apply device access control lists (ACLs), tagging devices for NGFW rule enforcement or other methods as desired
- Enable automated response to any policy violations

Visualize traffic to understand usage, dependencies and policy design

The eyeSegment Matrix lets you focus on what is important to instantly create desired policies to segment specific traffic patterns and protect your business while ensuring patient safety and business continuity.



eyeSegment **HEALTHCARE**

SOURCES (8) \ DESTINATIONS (8)	Users and Workstations	Imaging Devices	Clinical Devices	Laboratory Devices	Medical Services	Infrastructure Services	Internal Network	Private Network
Users and Workstations		●	●	●	●	●		
Imaging Devices	●				●	●		
Clinical Devices					●	●		
Laboratory Devices					●	●		
Medical Services					●	●		
Infrastructure Services								
Internal Network								
Private Network								

FIND & FILTER

Policy Visualization

● Traffic Baseline

● Traffic Violations

Legend

Traffic
- ● Traffic Baseline
- ● Filtered Traffic
- ● Traffic Violation

Zones
- Overlapping
- Forescout Zone

Rule Action
- 🟩 Allow All
- 🟥 Deny All
- 🟧 Allow/Deny Specific
- ▨ Conflict

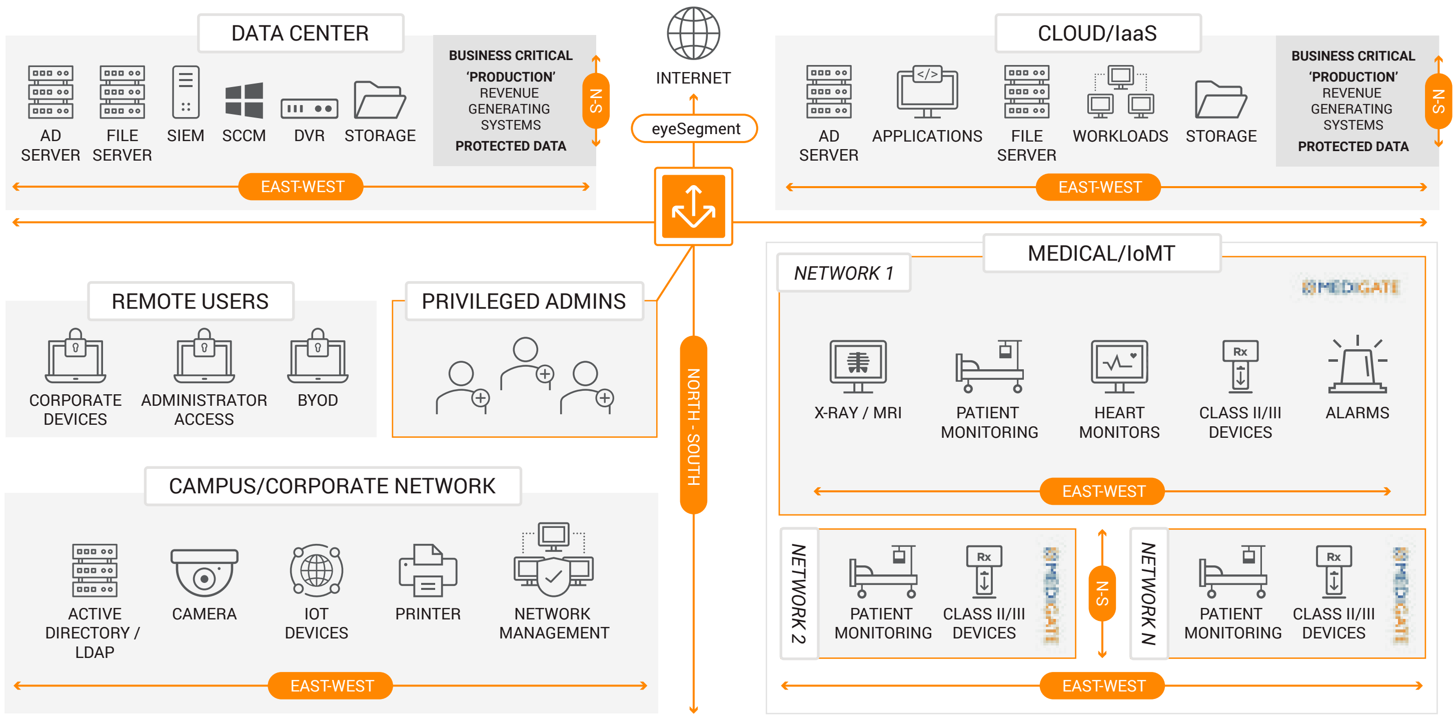
Rule Status
- □ Draft
- Simulation

The Forescout network segmentation solution addresses a wide array of use cases. In every case, the flexibility of the Forescout platform helps to reduce the risk of business disruption and minimize operating costs related to segmentation projects. Key use cases include:

- Gain instant visibility into your extended environment in real time to proactively model non-disruptive segmentation policies
- Mitigate risk, maintain compliance and reduce operational costs
- Simplify Zero Trust segmentation for clinical, IT and OT devices

Monitor and enforce Zero Trust segmentation between zones

Forescout eyeSegment reduces risk and helps ensure compliance by keeping connected devices from crossing healthcare and IT-OT domains.



[1] Mitigating Ransomware With Zero Trust, Forrester Research, Inc., June 8, 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

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