FORESCOUT

Active Defense for the Enterprise of Things.

eyeSegment

What's New

OT & IT-OT SEGMENTATION

Non-disruptive Zero Trust segmentation for sensitive OT environments and IT-OT convergence.

HEALTHCARE SEGMENTATION

Non-disruptive Zero Trust segmentation for sensitive healthcare environments

HYBRID CLOUD SEGMENTATION

Implement AWS east-west and north-south segmentation

CROSS-TEAM COLLABORATION

Improve segmentation adoption through better collaboration workflows between IT, OT, clinical engineering and other business unit teams

Simplify Zero Trust Segmentation for Any Device, Anywhere

Enterprise-wide segmentation requires a context-driven, multilayered architectural approach to address today's broad diversity of use cases. Forescout's latest eyeSegment 3.0 release fits the bill. It can greatly simplify Zero Trust segmentation across IT, IoT, IoMT and OT (operational technology) devices at scale. This unique, non-disruptive approach accelerates Zero Trust adoption, reduces threat exposure and contains breach impact while minimizing business disruption.

Segmentation for OT and converging IT-OT environments

eyeSegment now integrates with eyeInspect (formerly SilentDefense™) to simplify segmentation and reduce risk in IT-OT environments and within the OT network stack. With eyeSegment, you can:

- Gain an instant, "current state" understanding of OT/ICS assets and their communication patterns in real time, powered by deep packet inspection (DPI)
- Create unified segmentation policies to address IT-OT convergence risk and prevent lateral movement of threats across interconnected domains
- Reduce OT/ICS cyber risk and the likelihood of compromise with granular segmentation policies that can be run in monitor-and-respond mode to avoid disrupting critical operational processes
- Gain segmentation assurance and identify zone violations with continuous monitoring
- Automate segmentation enforcement leveraging your existing network infrastructure investments

Segmentation for healthcare environments

eyeSegment now integrates with Medigate to simplify segmentation across medical devices and clinical equipment, as well as conventional IT and IoT devices on healthcare networks. In addition to the capabilities above, eyeSegment enables healthcare organizations to:

- Gain an instant "current state" understanding of all IP-connected devices and their communication patterns powered by deep packet inspection (DPI) of medical communication protocols
- Address compliance and zoning requirements based on the rich clinical context of devices
- Create unified segmentation policies across all device types in healthcare environments to reduce the attack surface and prevent threats from propagating across defined zones
- Mitigate risk by segmenting vulnerable or legacy medical devices that cannot be patched or require a scheduled maintenance window

Hybrid cloud segmentation

The latest eyeSegment product enhancements enable cross-domain and data center/cloud segmentation from a unified policy. They also help to continuously assure segmentation hygiene within and across AWS cloud environments. New key capabilities include:

- Unified mapping and visualization of relationships, including east-west and north-south communication patterns to, from and within AWS environments
- Dependency mapping of various assets to help with cloud migration
- Intelligence to continuously help ensure proper segmentation from external networks (e.g. the internet)

Collaboration between IT and other functional teams

Several workflow improvements allow for cross-team collaborations that can effectively reduce risk and operational costs related to designing and deploying segmentation enforcement policies across the extended environment. New key capabilities include:

Improved Baseline Traffic Filtering
In addition to the search criteria previously available in eyeSegment, you can now filter by:

Improved Baseline Traffic Filtering

In addition to the search criteria previously available in eyeSegment, you can now filter by:

- Date range
- Forescout eyeSight segment
- IP address
- Inspected protocols dynamically learned by eyeInspect and Medigate based on what they detect in the environment

Improved Export Capabilities

You can now export as many as 100,000 records to a CSV file with several new elements added, such as source and destination IPs, which provide contextual details on a particular traffic pattern.

To learn more about these and other new capabilities, please refer to eyeSegment 3.0 Release Notes.

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