FORESCOUT®

Active Defense for the Enterprise of Things.

eyeSegment

Accelerate Zero Trust segmentation design and deployment at scale

HELP ASSURE SEGMENTATION HYGIENE

Gain an instant "current state" understanding of all connected assets and their communication patterns in real time.

BUILD UNIFIED POLICIES

Create unified Zero Trust segmentation policies to prevent lateral movement of threats across interconnected domains.

EFFECTIVE

Reduce 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.

REDUCE OPERATIONAL COMPLEXITY

Enhance segmentation adoption through better collaboration workflows between IT, Security, Networking and Engineering.teams.

AUTOMATE ENFORCEMENTS

Automate segmentation enforcement leveraging your existing network infrastructure investments.

Simple and Non-Disruptive Zero Trust Segmentation for Any Device, Anywhere

Forescout eyeSegment accelerates the design, planning and deployment of dynamic segmentation across the extended enterprise. It enables rapid acceleration of segmentation projects – to reduce the attack surface, limit blast radius, and mitigate regulatory and business risk. A core component of the Forescout platform, eyeSegment enables organizations to embrace Zero Trust principles for Enterprise of Things (EoT) security. Discover every IP-connected device.

KNOW & VISUALIZE

Map traffic flows to the logical taxonomy of devices, users, applications and services.

DESIGN & SIMULATE

Build, refine and simulate logical segmentation policies to preview impact before enforcement.

MONITOR & RESPOND

Monitor segmentation hygiene in real time and respond to policy violations across the extended enterprise.

forescout.com/platform/eyeSegment   salesdev@forescout.com   toll free 1-866-377-8771
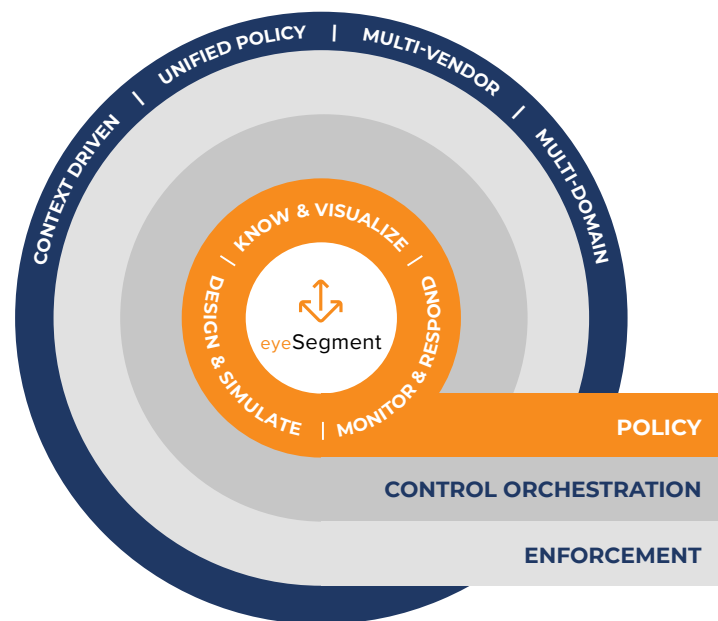
Transforming Enterprise-Wide Network Segmentation

Forescout eyeSegment leverages the Forescout platform's comprehensive device visibility and control to automate policy-based segmentation across multiple enforcement points throughout campus, data center and cloud networks. It lets you confidently design, build and deploy network segmentation at scale to enable enterprise-wide network segmentation.

- Gain an instant "current state" understanding of all connected assets and their communication patterns in real time

- Simplify the process of creating context-aware segmentation policies based on logical taxonomy of devices, users, applications and services

- Visualize and simulate policies before enforcement for proactive fine-tuning and validation

- Extend the capabilities of the Forescout platform to address multi-domain, multi-use-case segmentation challenges

- Leverage your current infrastructure investment on enforcement technologies

Figure 2. The eyeSegment Matrix allows you to focus on what is important. For instance, you can analyze and investigate a particular traffic pattern in your environment, as shown above. No matter where you are in the matrix hierarchy, you can instantly create and monitor effective eyeSegment policies to segment a specific traffic pattern and protect the EoT while ensuring business continuity.
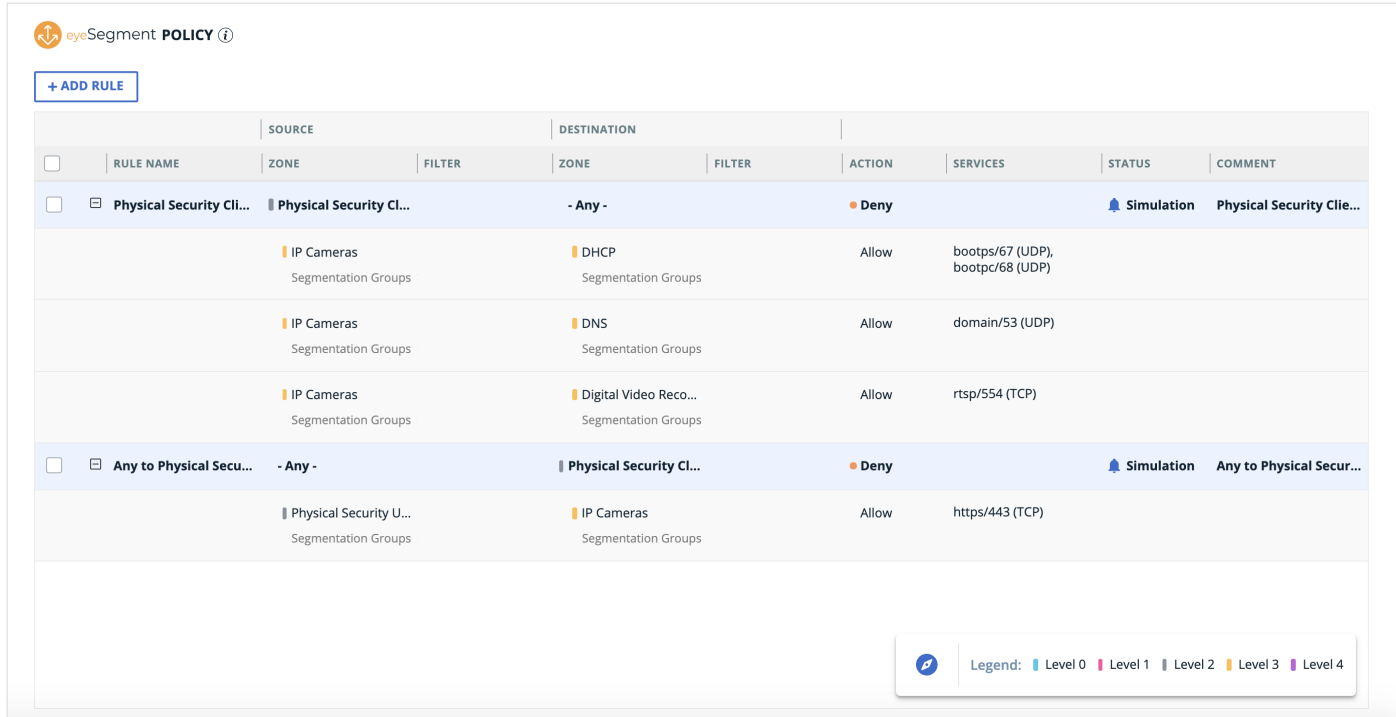
forescout.com/platform/eyeSegment   salesdev@forescout.com   toll free 1-866-377-8771

Know & Visualize Traffic Flows

Translate IP addresses into a logical taxonomy of devices, applications, users, and services.
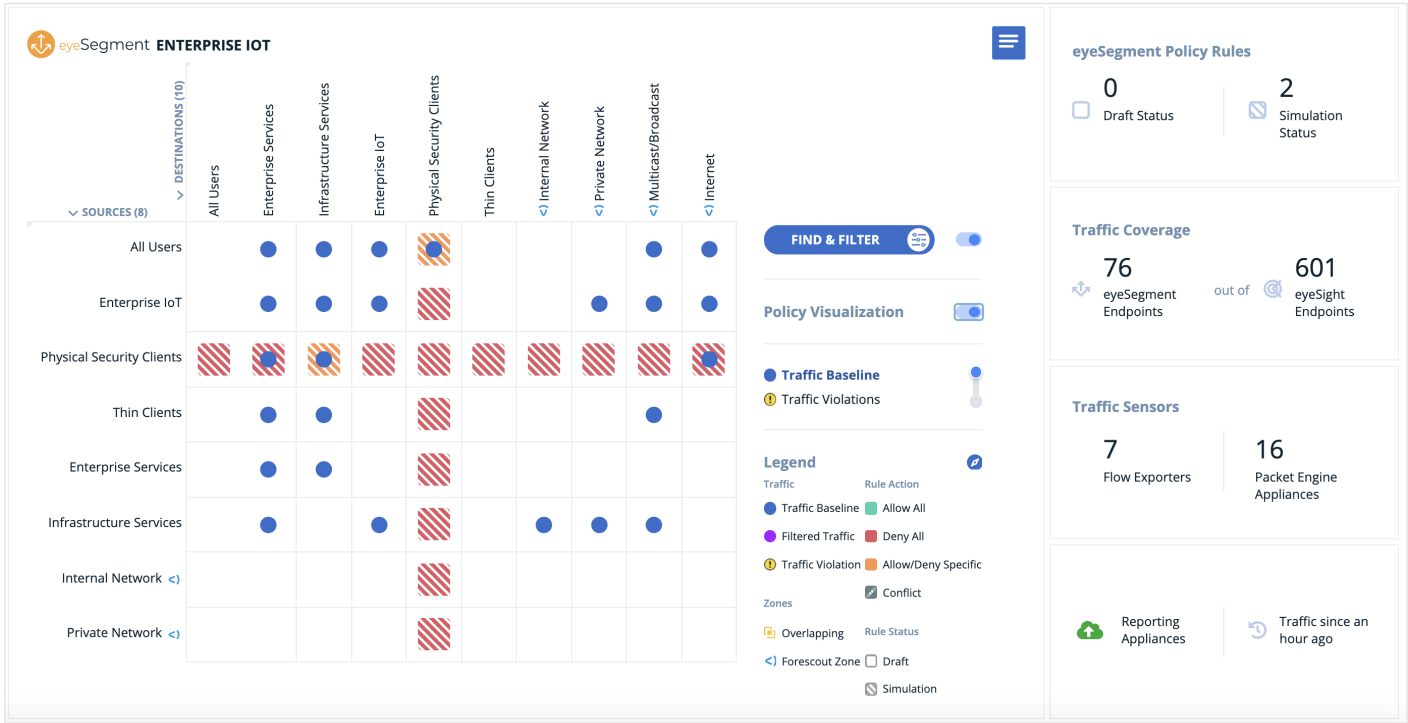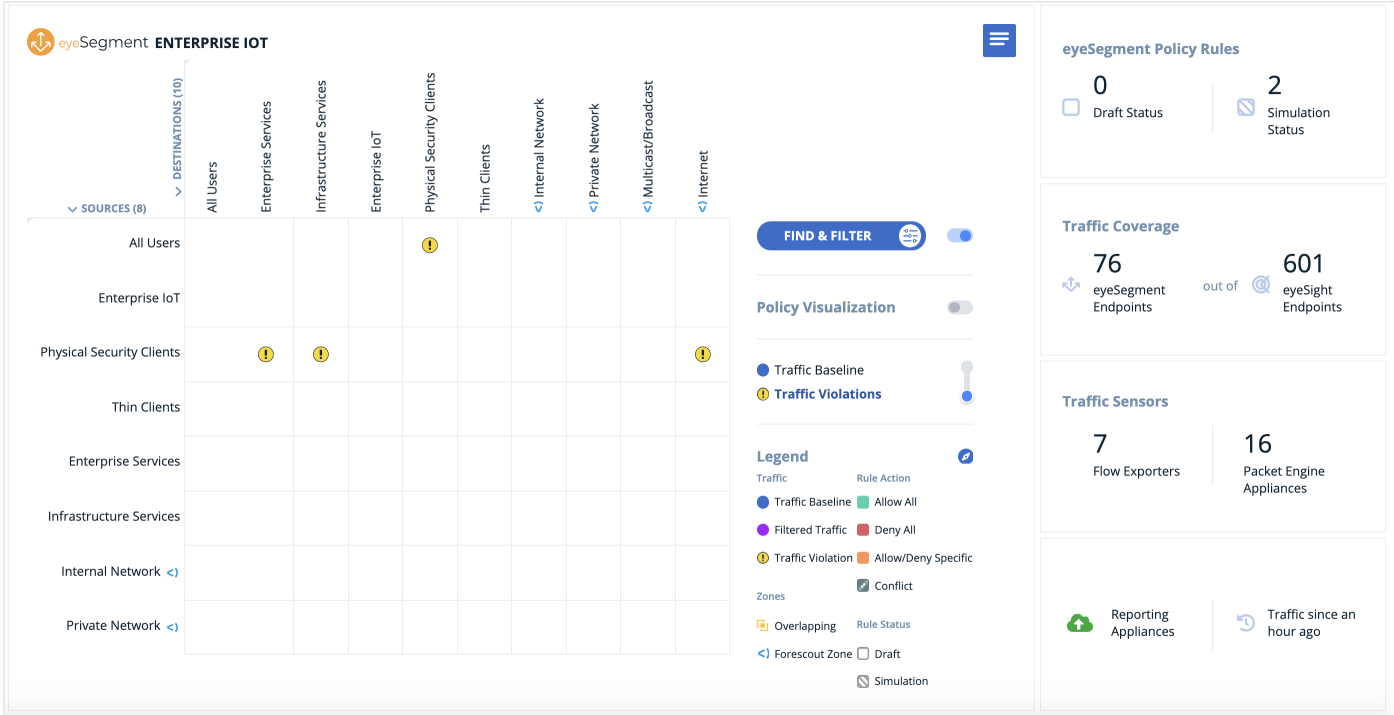

Design & Simulate Policies

Design, create and fine-tune effective segmentation policies based on a logical business taxonomy.

3

Monitor, Automate & Respond

Implement and monitor unified policies to identify policy violations in real time across multivendor environments and multiple network domains without disrupting business.

Don't just see it.
Secure it.

Contact us today to actively
defend your Enterprise of Things.

FORESCOUT.
Active Defense for the Enterprise of Things.

Learn more at Forescout.com