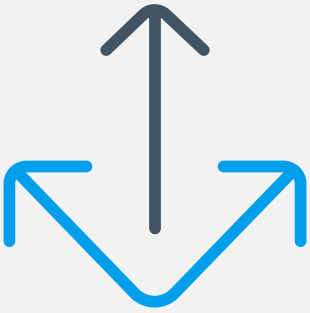


eyeSegment

Non-Disruptive Zero Trust Segmentation for Any Device, Anywhere

Help Assure Segmentation Hygiene

Gain a real-time visualization of all connected cyber assets and their communication patterns.

Enforce Least Privilege Access

Create unified Zero Trust segmentation policies that grant least privilege access and prevent the lateral movement of threats across your cyber assets.

Effective

Reduce cyber risk and limit the blast radius with flexible segmentation policies that can be run in escalating enforcement modes to avoid disrupting critical operational processes.

Reduce Operational Complexity

Enhance segmentation adoption through better collaboration between IT, security, networking and

Forescout eyeSegment removes the complexity of designing, planning and deploying dynamic segmentation across your cyber assets. Shrink the attack surface, limit the blast radius and mitigate regulatory and business risk by rapidly accelerating your segmentation projects.

A core component of the Forescout 4D Platform™ eyeSegment enables organizations to embrace Zero Trust security principles and automate security actions across their cyber assets.

Know & Visualize

- Map traffic flows to the logical taxonomy of assets, users, applications and services that make up your environment.

Design & Simulate

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

Monitor & Respond

- Monitor segmentation hygiene in real time and quickly respond to policy violations across your cyber assets.

Transforming Enterprise-wide Network Segmentation

eyeSegment leverages the Forescout comprehensive device visibility and control actions to automate policy-based segmentation across heterogeneous enforcement points throughout campus, data center and cloud networks. You're empowered to confidently design, build and deploy segmentation at scale to enable Zero Trust security.

engineering teams.

Automate Enforcement

Enhance segmentation adoption through better collaboration between IT, security, networking and engineering teams.

- Visualize and simulate policies before enforcement for proactive fine-tuning and validation
- Extend the capabilities of Forescout to address multi-domain, multi-use-case segmentation challenges
- Leverage your existing infrastructure investments in enforcement technologies

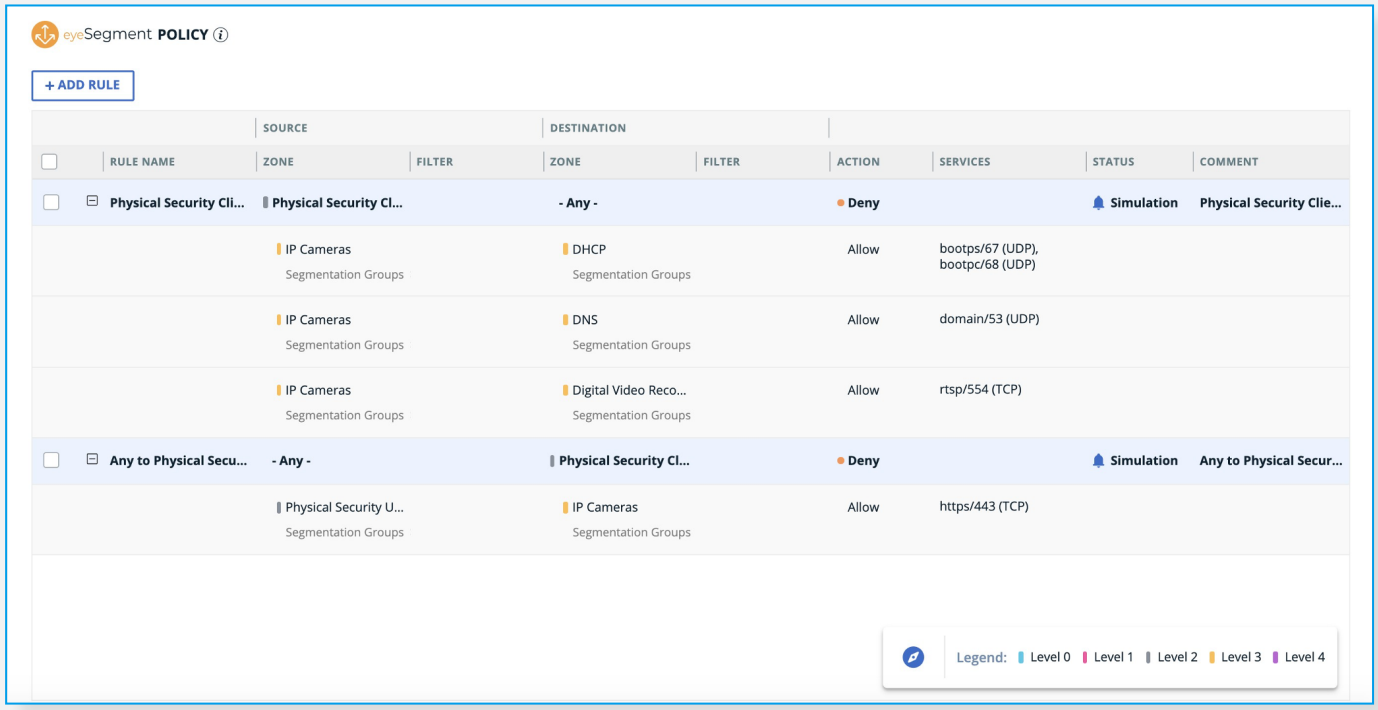
The eyeSegment Matrix allows you to focus on what is important by analyzing and investigating a particular traffic pattern in your environment, as shown below. No matter where you are in the matrix hierarchy, you can instantly create and monitor effective eyeSegment policies to segment a specific traffic pattern and protect your cyber assets while ensuring business continuity.

Know and Visualize Traffic Flows

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

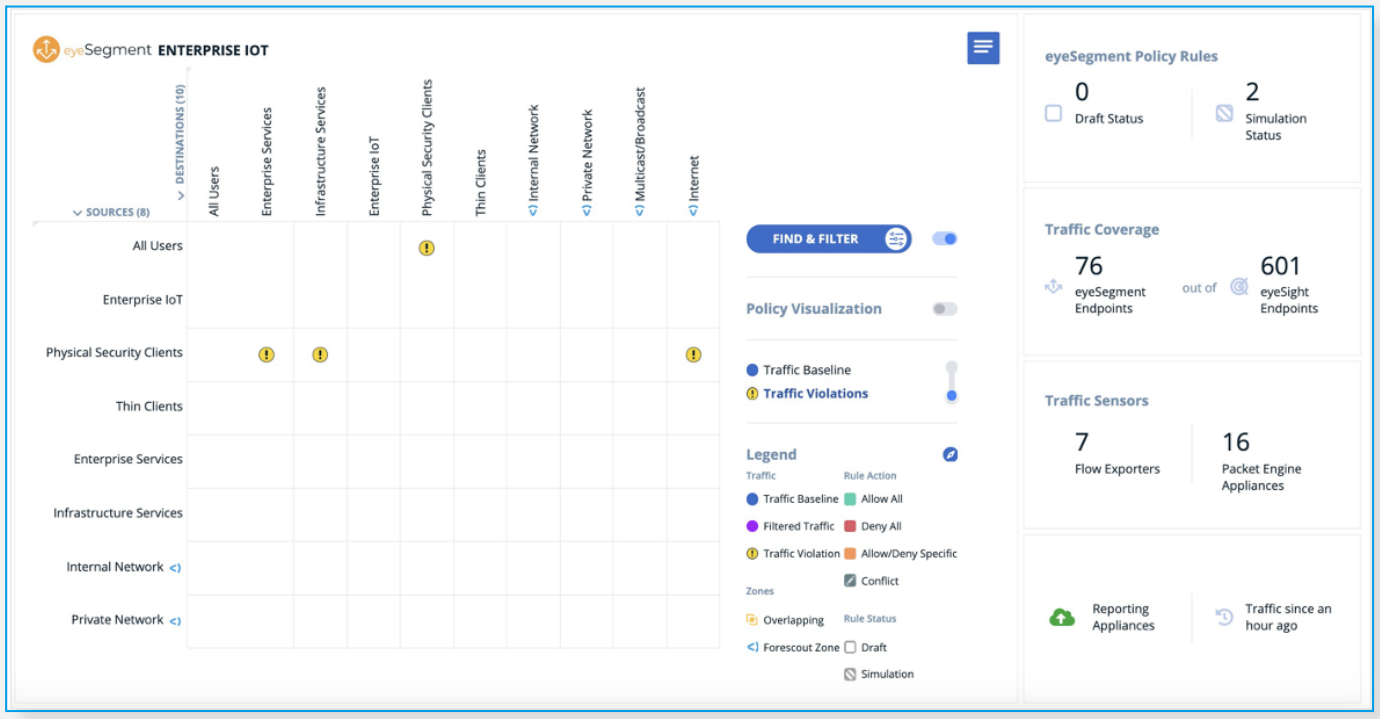
Design and Simulate Policies

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



Monitor, Automate and Respond

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



Discover, Assess, Control and Govern

The Forescout 4D Platform™ and eyeSegment provide 100% asset visibility, continuous compliance, network segmentation and a strong foundation for Zero Trust Assurance.

Visit **www.forescout.com/products** to learn more.

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