Forescout eyeSegment

Confidently design, build and deploy network segmentation at scale

Forescout eyeSegment accelerates the design, planning and deployment of dynamic network segmentation across the extended enterprise. It simplifies the process of creating context-aware segmentation policies and allows visualization and simulation of policies prior to enforcement for proactive fine-tuning and validation.

eyeSegment extends the capabilities of the Forescout platform to address multidomain, multi-use-case segmentation challenges. It enables organizations to embrace Zero Trust principles for all IP-connected systems, including Internet of Things (IoT) devices and operational technologies (OT). The result is a rapid acceleration of segmentation projects across the extended enterprise to reduce the attack surface, limit lateral propagation and blast radius, and mitigate regulatory, compliance and business risk.

Challenges

- Lack of confidence to move forward on segmentation projects
- Risk of exposure due to the potential for lateral movement of threats across flat networks
- Incomplete context on devices, applications and users
- Policy sprawl and the inability to consistently enforce controls across diverse technologies
- Multivendor operational complexity and inconsistency in segmentation controls across network domains
- Lack of skills, resources and tools to effectively design, build and deploy network segmentation across the extended enterprise

eyeSegment

Benefits

- Accelerate network segmentation projects with confidence
- Proactively determine the impact of policies to minimize business disruption
- Reduce risk of business disruption
- Uniformly enforce control across diverse enforcement technologies and network domains through a single policy framework
- Adapt to compliance and regulatory requirements
- Reduce operational complexity of segmentation projects
- Enable a Zero Trust approach to implement granular security controls

Highlights

- Create context-aware segmentation policies using a logical business taxonomy of users, apps, services and devices
- Quickly learn the impact before enforcing segmentation policies
- Continuously monitor and validate segmentation hygiene
- Rapidly respond to segmentation policy violations across the extended enterprise

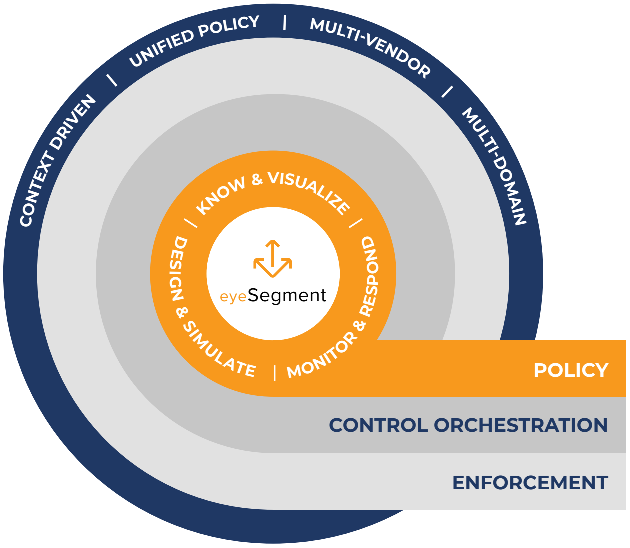

UNIFIED POLICY | MULTI-VENDOR | MULTI-DOMAIN
CONTEXT DRIVEN |
KNOW & VISUALIZE / DESIGN & SIMULATE | MONITOR & RESPOND
eyeSegment
POLICY
CONTROL ORCHESTRATION
ENFORCEMENT

Figure 1: Forescout recommends a three-layered architecture as a best practice for enterprise-wide network segmentation, starting with a “policy layer” powered by eyeSegment.

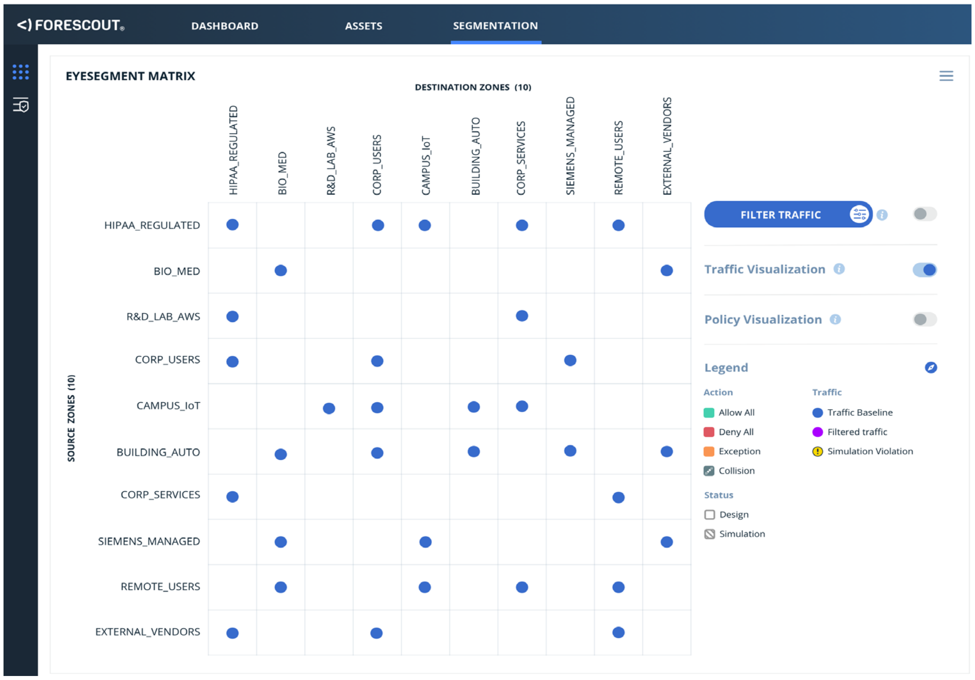
Transforming Enterprise-Wide Network Segmentation

Forescout eyeSegment builds on the comprehensive device visibility and in-depth, real-time context provided by Forescout eyeSight. It lets you visualize traffic flows and dependencies between users, applications, services and devices, and then design, simulate and monitor policies to understand the impact to your environment. Leveraging Forescout eyeControl and eyeExtend, policies are orchestrated across multiple segmentation enforcement points in campus, data center and cloud networks. eyeSegment helps organizations to confidently design, build and deploy network segmentation at scale to enable enterprise-wide network segmentation.

Know and visualize traffic flows

Forescout eyeSegment automatically maps traffic flows to a logical taxonomy of users, applications, services and devices across the entire enterprise network without deploying agents. This helps you monitor your network traffic in real time and create granular segmentation policies that are context-aware. A typical use case would be to design controls to ensure that only Finance Department employees have access to payment applications running across different domains. Another would be to determine the common services required by medical devices with legacy operating systems, and then segregating them.

The eyeSegment connectivity matrix feature (Figure 2) helps you visualize traffic flows. It creates a traffic baseline, maintains traffic data over time and shows real-time flows between source and destination zones as defined in the segmentation policy.



EYESEGMENT MATRIX

DESTINATION ZONES (10)

SOURCE ZONES (10)

	HIPAA_REGULATED	BIO_MED	R&D_LAB_AWS	CORP_USERS	CAMPUS_IoT	BUILDING_AUTO	CORP_SERVICES	SIEMENS_MANAGED	REMOTE_USERS	EXTERNAL_VENDORS
HIPAA_REGULATED	●			●	●		●		●	
BIO_MED		●								●
R&D_LAB_AWS	●						●			
CORP_USERS	●			●				●		
CAMPUS_IoT			●	●		●	●			
BUILDING_AUTO		●		●		●		●		●
CORP_SERVICES	●								●	
SIEMENS_MANAGED		●			●					●
REMOTE_USERS		●			●		●		●	
EXTERNAL_VENDORS	●			●					●	

FILTER TRAFFIC

Traffic Visualization ●

Policy Visualization ○

Legend

Action	Traffic
🟩 Allow All	● Traffic Baseline
🟥 Deny All	● Filtered traffic
🟧 Exception	⚠ Simulation Violation
▨ Collision	

Status
□ Design
▨ Simulation

Figure 2: eyeSegment connectivity matrix view showing logical business traffic flows.

Design and simulate segmentation policies

Forescout eyeSegment helps you design, create and fine-tune effective segmentation policies based on a logical business taxonomy that can be enforced across existing underlying technologies. You can proactively simulate the implementation of policies before putting them into effect across your environment, thus minimizing the possibility of business disruption.

Build unified and granular segmentation policies

A segmentation policy is a set of rules to allow all traffic, deny all traffic or allow only specific traffic between specific source and destination zones. Zones are based on standard policy groups that can be populated manually or via a policy. Single IP addresses and Forescout segment objects that are groups can also be zones. Each segmentation zone can be designated as a source zone, a destination zone or both.

You can create segmentation policies from a single console to deny or to explicitly allow specific traffic across different technologies and network domains. Each policy can be applied to traffic from a specific source zone to a specific destination zone. By default, all traffic from any source zone to any destination zone is allowed. The policy and its exceptions determine which traffic is allowed and which is denied. This allows you to define different actions for individual sub-groups and services.

Visualize policies and traffic dependencies

Policy and traffic visualization can be enabled to visualize created segmentation policies and their status in the connectivity matrix as shown below. Filtering capabilities allow you to drill down on a particular policy in order to filter traffic by service and/or the intersection of matrix zones with source and destination filters.

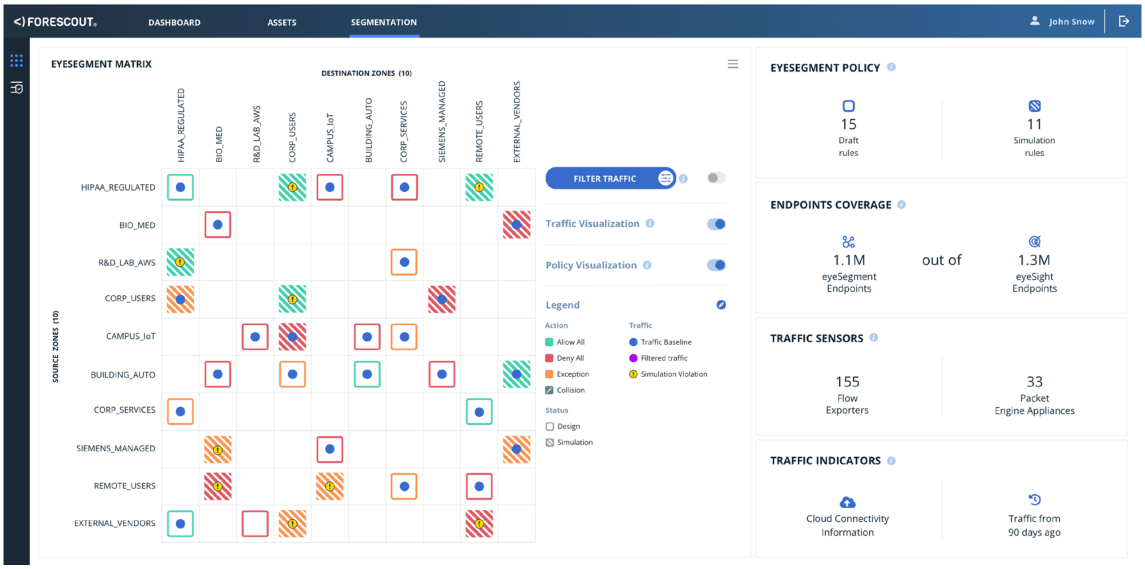


Figure 3: Policy visualization and simulation view.

Monitor and respond

eyeSegment's single-pane-of-glass policy management and dashboard let you centrally monitor traffic flows between different source and destination zones. The ability to continuously monitor and respond to segmentation policies abstracted from the underlying controls can be valuable as a gradual step to control, or when an infrastructure control is not available. eyeSegment also helps to continuously monitor enterprise infrastructure controls and assure the segmentation controls are implemented and working effectively after enforcing controls across the extended enterprise.

Use Cases

The Forescout platform addresses a wide array of network segmentation 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.

Here are a few common use cases:

Protecting critical business applications	• Protect business-critical applications, ensure controls are effectively enforced and continuously monitor to ensure continuous protection. Maintain appropriate intra- and inter-business service controls across different services, applications and domains. • Control user access to critical business services across different domains. Protect business-critical applications from misuse by users, ensure controls are effectively enforced and continuously monitor ongoing protection.
Enforce privileged access to critical IT infrastructure	• Restrict IT admin access to sensitive network devices (switch, NGFW, etc.) and data center/cloud workloads (Active Directory/LDAP, Domain Name System, Oracle Cluster, etc.) based on designated admins (role-based), IT admin endpoint state (encrypted, domain-joined, etc.) and secure communication (specific port/service)
Protecting enterprise IoT/OT devices (printers, cameras, VoIP, card reader, HVAC, etc.)	• Protect the IT network from IoT/OT devices • Protect IoT/OT devices from attacks
Enterprise-wide segmentation assurance	• Ensure all enforcement points across different domains (campus, data center and IoT), managed by other teams, are meeting segmentation policy requirements and configured as intended
Containment of vulnerable devices	• Limit access from/to vulnerable devices (WannaCry, unpatched, end of life, etc.) to the rest of the network
Protecting legacy applications/ OS devices	• Reduce the attack surface by segregating devices with legacy operating systems and applications installed on them • Mitigate risk of threats to devices running end-of-life operating systems

FORESCOUT

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