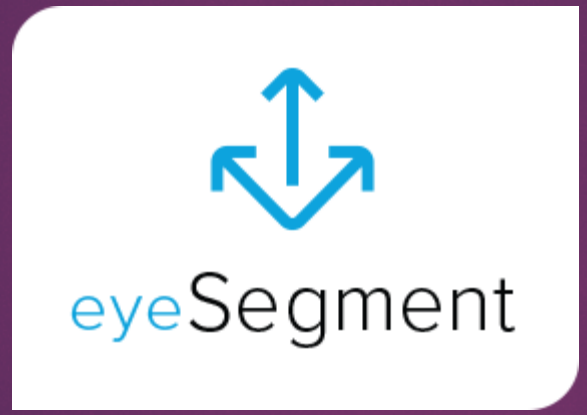
Forescout eyeSegment



BY: NIKHIL GUPTA, FSCA

Traditional Segmentation 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 resources and tools to effectively create and deploy network segmentation across the enterprise.

Forescout's Solution: eyeSegment

- **Visualization:** eyeSegment leverages device, app and user context from eyeSight to automatically map traffic flows to a logical taxonomy of users, applications, services and devices across the entire enterprise network without deploying agents. This helps customers monitor their network traffic in real time, know and visualize traffic flows with context, and create context-aware and granular segmentation policies.

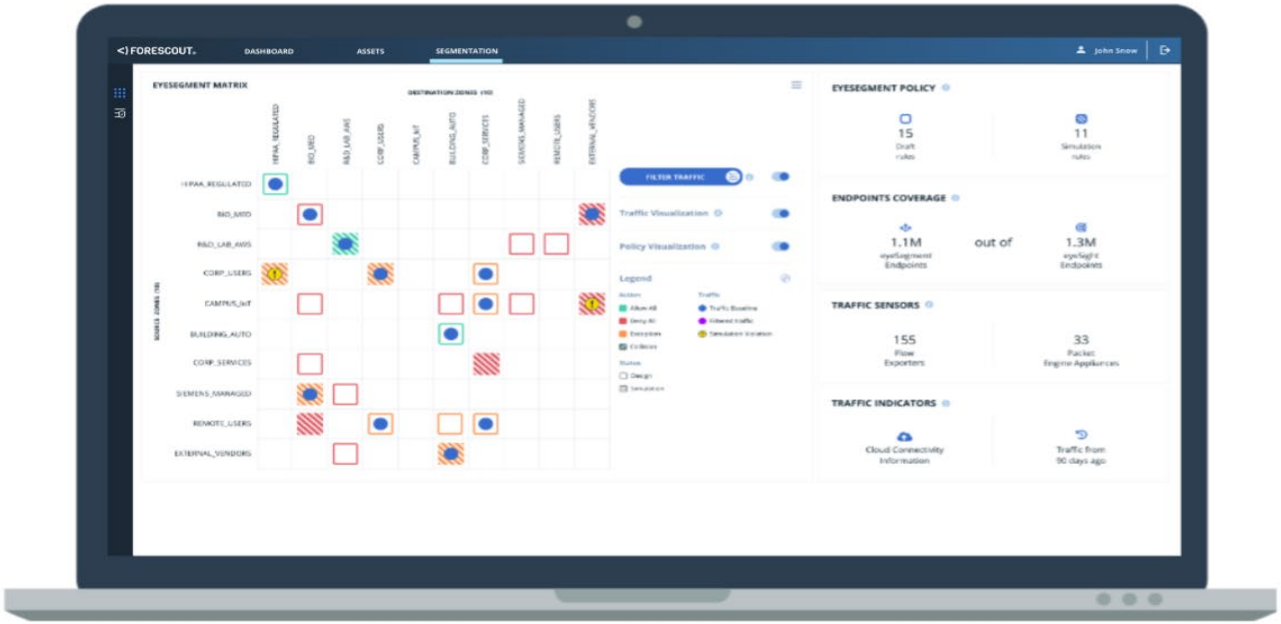
- **Simulation:** eyeSegment helps customers to design, create and fine-tune effective segmentation policies based on a logical business taxonomy, and enables them to proactively simulate policies before putting them into effect across their environment. With this capability, customers can determine how specific policies would impact the rest of their network from a single policy layer in order to minimize business disruption.

- **Monitoring and Response:** eyeSegment provides the ability to monitor and respond to segmentation policies abstracted from the underlying controls. It also helps to continuously monitor enterprise infrastructure controls and assure that segmentation controls are implemented and effectively enforcing policy across the extended enterprise.

eyeSegment Dashboard

Role Based Access For Remote Devices

Reduce risk from misbehaving devices



Know & Visualize Traffic Flows

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

Design & Simulate Policies

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

Monitor & Respond

Implement single set of policies across multi-vendor environments and multiple network domains

FORESCOUT

Three Layered Approach

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

Use Cases Continued

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

Conclusion

- eyeSegment extends the capabilities of the Forescout platform to address multi-domain, 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 policies across the extended enterprise to reduce the attack surface, limit lateral propagation and blast radius, and mitigate regulatory, compliance, and business risk.

Resources

- https://www.forescout.com/company/resources/network-segmentation-solution-brief/
- https://www.forescout.com/company/resources/forescout-eyesegment-datasheet/
- Or you can contact me at 703-871-8572 or Nikhil.Gupta@carahsoft.com