Forescout eyeSegment

Konzeption, Entwicklung und Implementierung zuverlässiger Netzwerksegmentierung in großem Maßstab

Forescout eyeSegment beschleunigt die Konzeption, Planung und Implementierung dynamischer Netzwerksegmentierung im erweiterten Unternehmen. Die Lösung vereinfacht das Erstellen kontextbezogener Segmentierungsrichtlinien und ermöglicht die Darstellung und Simulation von Richtlinien vor ihrer Durchsetzung für proaktive Anpassungen und Überprüfungen.

eyeSegment erweitert den Funktionsumfang der Forescout-Plattform und ermöglicht die Lösung komplexer Segmentierungsfälle mit mehreren Domänen und mehreren Anwendungsszenarien. Dadurch können Unternehmen Zero Trust-Prinzipien für alle per IP-Adresse verbundenen Systeme implementieren, beispielsweise für IoT-Geräte (Internet of Things) und Operative Technologien (OT). Der Vorteil: Segmentierungsprojekte im erweiterten Unternehmen werden erheblich beschleunigt, sodass sich die Angriffsfläche verringert, die laterale Ausbreitung sowie der Wirkungsradius von Angriffen eingeschränkt wird und rechtliche, Compliance- und Geschäftsrisiken minimiert werden können.

Herausforderungen

- Fehlendes Vertrauen in die Umsetzung von Segmentierungsprojekten
- Gefährdungsrisiko durch potenzielle laterale Bewegung von Bedrohungen innerhalb flacher Netzwerke
- Unvollständiger Kontext zu Geräten, Anwendungen und Benutzern
- Wildwuchs bei Richtlinien und fehlende Möglichkeit zur einheitlichen Durchsetzung von Kontrollen über unterschiedliche Technologien hinweg
- Komplexität der Betriebsabläufe aufgrund mehrerer Anbieter und uneinheitliche Segmentierungskontrollen bei verschiedenen Netzwerkdomänen
- Fehlende Kompetenzen, Ressourcen und Tools zur effektiven Konzeption, Entwicklung und Implementierung von Netzwerksegmentierung im erweiterten Unternehmen

eyeSegment

Vorteile

- Zuverlässige Beschleunigung von Projekten zur Netzwerksegmentierung
- Proaktive Feststellung der Auswirkungen von Richtlinien, um Geschäftsunterbrechungen zu vermeiden
- Geringeres Risiko von Geschäftsunterbrechungen
- Einheitliche Durchsetzung von Kontrollen über unterschiedliche Durchsetzungstechnologien und Netzwerkdomänen hinweg dank eines zentralen Richtlinien-Frameworks
- Anpassung an rechtliche Vorgaben und Compliance-Vorschriften
- Geringere Komplexität von Segmentierungsprojekten
- Zero Trust-Ansatz bei der Implementierung detaillierter Sicherheitskontrollen

Kernpunkte

- Erstellung kontextbezogener Segmentierungsrichtlinien mithilfe einer logischen Geschäftstaxonomie für Benutzer, Anwendungen, Services und Geräte
- Schneller Überblick über die Auswirkungen vor der Durchsetzung von Segmentierungsrichtlinien
- Kontinuierliche Überwachung und Überprüfung des Segmentierungszustands
- Schnelle Reaktion auf Verstöße gegen Segmentierungsrichtlinien im gesamten erweiterten Unternehmen

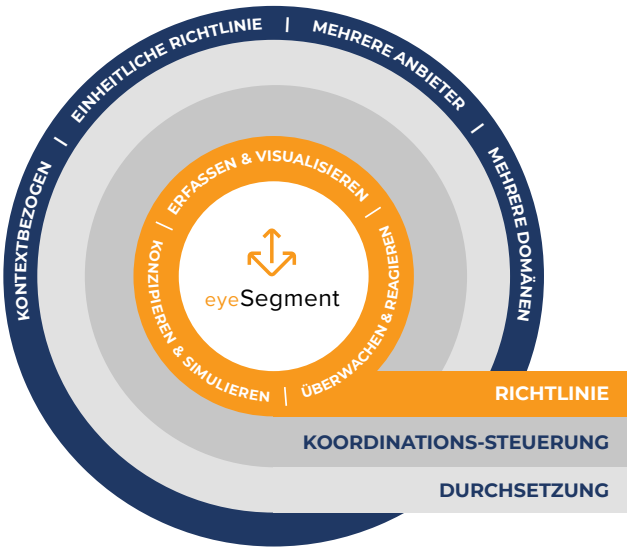

Abbildung 1. Forescout empfiehlt eine Architektur mit drei Ebenen als Best Practice für unternehmensweite Netzwerksegmentierung, beginnend mit einer „Richtlinienebene“, die von eyeSegment bereitgestellt wird.

Neugestaltung der unternehmensweiten Netzwerksegmentierung

Forescout eyeSegment ergänzt die umfangreiche Gerätetransparenz sowie die detaillierten Echtzeit-Kontextinformationen von Forescout eyeSight. Damit können Sie die Datenflüsse und Abhängigkeiten zwischen Benutzern, Anwendungen, Services und Geräten darstellen und anschließend Richtlinien konzipieren, simulieren und überwachen, um die Auswirkungen auf Ihre Umgebung zu verstehen. Forescout eyeSegment greift auf eyeControl und eyeExtend zurück, um Richtlinien über mehrere Segmentierungsdurchsetzungspunkte in Campus-, Rechenzentrum- und Cloud-Netzwerken zu koordinieren. Mit eyeSegment können IT-Abteilungen ihre Netzwerksegmentierung in großem Maßstab unternehmensweit konzipieren, entwickeln und implementieren.

Erfassen und Visualisieren von Datenflüssen

Forescout eyeSegment ordnet die Datenflüsse automatisch einer logischen Taxonomie für Benutzer, Anwendungen, Services und Geräte im gesamten Unternehmensnetzwerk zu, ohne dass dazu Agenten notwendig sind. Dadurch können Sie Ihren Datenverkehr in Echtzeit überwachen und detaillierte kontextbezogene Segmentierungsrichtlinien erstellen. Ein typisches Anwendungsszenario besteht darin, solche Kontrollen zu konzipieren, die nur Mitarbeitern der Finanzabteilung Zugriff auf Zahlungsanwendungen in verschiedenen Domänen gewährt. Ein weiteres Szenario ist die Festlegung der gemeinsamen Services, die für medizinische Geräte mit veralteten Betriebssystemen erforderlich sind, und ihre anschließende Isolierung.

Die Konnektivitätsmatrix-Funktion von eyeSegment (Abbildung 2) erlaubt die Darstellung der Datenflüsse. Sie erstellt eine Basislinie für den Datenverkehr, erfasst Informationen zum Datenverkehr über einen längeren Zeitraum hinweg und zeigt Echtzeitdatenflüsse zwischen den Quell- und Zielzonen, die in der Segmentierungsrichtlinie definiert sind.

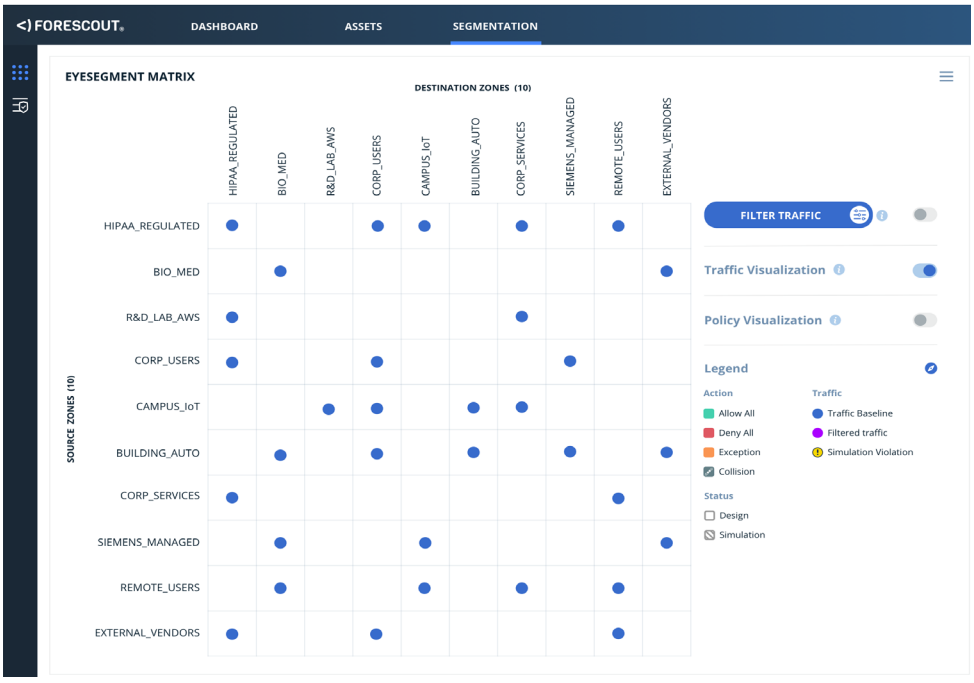

Abbildung 2. eyeSegment-Konnektivitätsmatrix, die logische Geschäftsdatenflüsse zeigt.

Konzipieren und Simulieren von Segmentierungsrichtlinien

Forescout eyeSegment ermöglicht das Konzipieren, Erstellen und Optimieren effektiver Segmentierungsrichtlinien basierend auf einer logischen Geschäftstaxonomie, die für die zugrunde liegenden Technologien durchgesetzt werden können. Sie können die Implementierung von Richtlinien proaktiv simulieren, bevor diese in Ihrer Umgebung implementiert werden, um mögliche Unterbrechungen des Geschäftsbetriebs zu minimieren.

Aufbau einheitlicher und detaillierter Segmentierungsrichtlinien
Eine Segmentierungsrichtlinie ist ein Satz von Regeln, der den gesamten Datenverkehr zulässt, blockiert oder nur bestimmten Datenverkehr zwischen bestimmten Quell- und Zielzonen erlaubt. Diese Zonen basieren auf standardmäßigen Richtliniengruppen, die manuell oder über eine Richtlinie definiert werden können. Einzelne IP-Adressen und Forescout-Segmentobjekte, bei denen es sich um Gruppen handelt, können ebenfalls Zonen sein. Jede Segmentierungszone kann als Quellzone, Zielzone oder beides definiert werden.

Sie können Segmentierungsrichtlinien über eine zentrale Konsole erstellen, um Datenverkehr zwischen unterschiedlichen Technologien und Netzwerkdomänen zu blockieren oder explizit zuzulassen. Jede Richtlinie kann auf den Datenverkehr von einer bestimmten Quellzone zu einer bestimmten Zielzone angewendet werden. Standardmäßig wird der gesamte Datenverkehr von jeder Quellzone zu jeder Zielzone zugelassen, wobei die Richtlinie und ihre Ausnahmen bestimmen, welcher Datenverkehr zugelassen bzw. blockiert wird. Dadurch ist es möglich, unterschiedliche Aktionen für individuelle Untergruppen und Services zu definieren.

Visualisierung von Richtlinien und Datenverkehrabhängigkeiten
Die Richtlinien- und Datenverkehrvisualisierung kann erstellte Segmentierungsrichtlinien und ihren Status in der Konnektivitätsmatrix anzeigen (siehe Abbildung unten). Mithilfe von Filterfunktionen lassen sich Details zu einer bestimmten Richtlinie anzeigen, um den Datenverkehr nach Service bzw. dem Schnittpunkt der Matrixzone mit Quell- und Zielfiltern zu filtern.

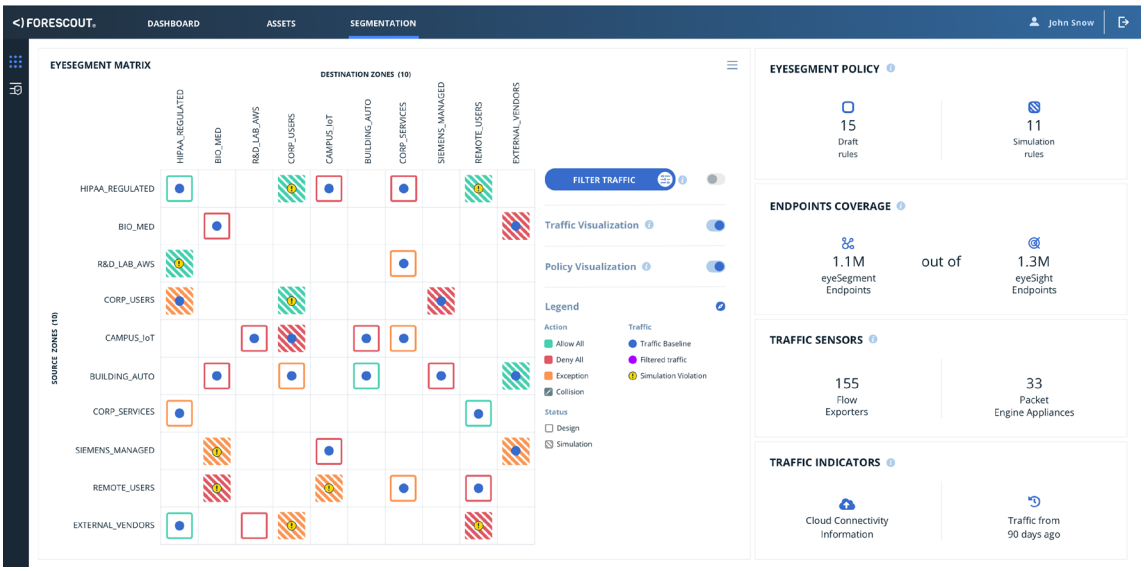

Abbildung 3. Ansicht der Richtlinienvisualisierung und Simulation.

Überwachung und Reaktion

Dank der zentralen Richtlinienverwaltung und dem Dashboard von eyeSegment können Sie sämtliche Datenflüsse zwischen unterschiedlichen Quell- und Zielzonen an einem Ort überwachen. Die Möglichkeit zur kontinuierlichen Überwachung und Reaktion auf Segmentierungsrichtlinien, die von den zugrunde liegenden Kontrollen abstrahiert sind, bietet Vorteile als schrittweise Kontrollmaßnahme oder wenn eine Infrastrukturkontrolle nicht verfügbar ist. Außerdem ermöglicht eyeSegment die kontinuierliche Überwachung der unternehmenseigenen Infrastrukturkontrollen und bietet die Sicherheit, dass die Segmentierungskontrollen nach ihrer Durchsetzung im erweiterten Unternehmen implementiert sind und effektiv funktionieren.

Anwendung

Die Forescout-Plattform deckt ein breites Spektrum an Anwendungsszenarien für Netzwerksegmentierung ab. In jedem Fall erleichtert die Forescout-Plattform das Minimieren von Unterbrechungen des Geschäftsbetriebs sowie die Senkung von Betriebskosten für Segmentierungsprojekte.

Dies sind einige gängige Anwendungsszenarien:

Schutz wichtiger geschäftlicher Anwendungen	• Schutz geschäftskritischer Anwendungen, Gewährleistung der effektiven Durchsetzung von Kontrollen und kontinuierliche Überwachung für kontinuierlichen Schutz. Gewährleistung adäquater geschäftsinterner sowie -übergreifender Servicekontrollen über unterschiedliche Services, Anwendungen und Domänen hinweg • Kontrolle des Benutzerzugangs zu geschäftskritischen Services in unterschiedlichen Domänen. Schutz geschäftskritischer Anwendungen vor Missbrauch durch Benutzer, Gewährleistung der effektiven Durchsetzung von Kontrollen und kontinuierliche Überwachung der dauerhaften Schutzmaßnahmen
Durchsetzung von Zugriffsbeschränkungen für kritische IT-Infrastruktur	• Einschränkung des IT-Administratorzugriffs auf wichtige Netzwerkgeräte (z. B. Switch oder NGFW) und Rechenzentrum-/Cloud-Workloads (Active Directory/ LDAP, Domain Name System oder Oracle Cluster) basierend auf festgelegten Administratoren (rollenbasiert), Status des IT-Administrator-Endgeräts (z. B. verschlüsselt oder Mitglied der gleichen Domäne) und sicherer Kommunikation (spezifischer Port/Service)
Schutz unternehmenseigener IoT-/OT-Geräte (z. B. Drucker, Kameras, VoIP, Kartenleser, Klimaanlagen)	• Schutz des IT-Netzwerks vor IoT-/OT-Geräten • Schutz von IoT-/OT-Geräten vor Angriffen
Zuverlässige unternehmensweite Segmentierung	• Gewährleistung, dass alle Durchsetzungspunkte über unterschiedliche Domänen hinweg (Campus, Rechenzentrum und IoT), die von anderen Teams verwaltet werden, die Anforderungen der Segmentierungsrichtlinie einhalten und ordnungsgemäß konfiguriert sind
Isolierung anfälliger Geräte	• Einschränkung des Zugriffs von/auf anfälligen Geräten (WannaCry, ungepatcht, Ende des Lebenszyklus usw.) auf den Rest des Netzwerks
Schutz veralteter Anwendungen/Geräte-Betriebssysteme	• Verringerung der Angriffsfläche durch Isolierung von Geräten mit darauf installierten veralteten Betriebssystemen und Anwendungen • Minimierung von Bedrohungen für Geräte mit Betriebssystemen am Ende des Lebenszyklus

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Telefon (International): +1-408-213-3191
Support: +1-708-237-6591

Weitere Informationen
finden Sie unter Forescout.de