FORESCOUT
Active Defense for the Enterprise of Things™

Segmentierung für das gesamte Unternehmensnetzwerk

Einfache und unterbrechungsfreie Zero-Trust-Segmentierung

Die Aussicht auf mehr Effizienz, Innovation und Produktivität durch die digitale Transformation hat zu flachen Netzwerken mit hoher Konnektivität geführt. Diese erlauben laterale Bewegungen von Bedrohungen und sind nicht in der Lage, die wachsende Zahl von Enterprise of Things-Geräten (EoT) im gesamten Unternehmensnetzwerk zu schützen. IT-Teams suchen nach Segmentierungsoptionen, mit denen sich Zero-Trust-Kontrollen implementieren und die Sicherheit verbessern lassen. Gleichzeitig werden jedoch auch Bedenken wegen komplizierter Bereitstellungen und teuren Unterbrechungen des Geschäftsbetriebes laut, die das Vertrauen innerhalb des Unternehmens auf die Probe stellen und dem Fortschritt im Wege stehen. Folgende Herausforderungen müssen überwunden werden:

- Fehlendes Vertrauen in die Umsetzung von Segmentierungsprojekten
- Bedrohungen und Kompromittierungsrisiken durch die digitale Transformation
- Komplexität der Betriebsabläufe aufgrund mehrerer Anbieter und uneinheitliche Segmentierungsrichtlinien in Umgebungen mit mehreren Domänen
- Fehlende Kompetenzen, Ressourcen und Tools zur effektiven Konzeption, Entwicklung und Implementierung von Segmentierung für das gesamte Unternehmensnetzwerk

> **„IoT- und netzwerkfähige Geräte haben zu neuen Kompromittierungs-möglichkeiten für Netzwerke und Unternehmen geführt. [...] Sicherheitsteams müssen jedes Gerät im Netzwerk permanent isolieren, absichern und kontrollieren.“** [1]
>
> **FORRESTER RESEARCH**
> **Juni 2020**

Gründe für Forescout: Eine erstklassige Lösung für unterbrechungsfreie Zero-Trust-Segmentierung

Wenn Ihnen diese Herausforderungen bekannt vorkommen, ist jetzt ein guter Zeitpunkt, sich die Forescout-Lösung genauer anzusehen. Sie vereinfacht die Zero-Trust-Segmentierung und optimiert das Risikomanagement für Ihre verbundenen EoT-Geräte im gesamten Unternehmensnetzwerk.

forescout.com/solutions/network-segmentation info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

Die Forescout-Plattform beschleunigt die dynamische, kontextbezogene Netzwerksegmentierung – ohne Komplexität, explodierende Kosten oder Beeinträchtigung des Geschäftsbetriebs.

So erfüllen wir Ihre Anforderungen:

- **Beschleunigte Zero-Trust-Segmentierung** im gesamten Unternehmensnetzwerk
- **Sofortiger Echtzeitüberblick über den Status der Netzwerksegmentierung** auf jedem Gerät und an jedem Ort
- **Verringerung der Angriffsfläche und Einhaltung von Konformitätsvorschriften** durch dynamische Segmentierung für IT-, IoT- und IoMT-Systeme (Internet of Medical Things), wodurch Branchenvorschriften problemlos eingehalten werden können
- **Vereinfachte Bedrohungsanalyse** mit weniger Tools, weniger Dashboards und besser umsetzbaren Warnungen
- **Weniger Konformitätsrisiken sowie geringe Kosten durch die effiziente Verwaltung der Erkennung und Abwehr von Cybersicherheitsbedrohungen**, sodass keine hochqualifizierten Mitarbeiter benötigt werden
- **Optimierung teamübergreifender Workflows** und Nutzung vorhandener Investitionen mit einer konsistenten Segmentierungsrichtlinie für das gesamte Unternehmensnetzwerk

Da es bei Netzwerksegmentierung keine universelle Lösung geben kann, trägt Forescout dem Rechnung. Alle Segmentierungstools haben eigene Stärken, Anwendungsszenarien und Netzwerkbereiche, für die sie optimal geeignet sind. Die Forescout-Plattform, einschließlich Forescout eyeSegment, verbindet diese unterschiedlichen Technologien und beschleunigt die Konzeption, Planung und Bereitstellung dynamischer Segmentierung für das gesamte Unternehmensnetzwerk. Dadurch ist die Implementierung effektiver Zero-Trust-Richtlinien, Verringerung von Richtlinienverstößen und Minimierung der Angriffsfläche möglich.

Wie in der Abbildung unten gezeigt, erfordert unternehmensweite Segmentierung eine kontextbezogene mehrschichtige Architektur, die der Vielfalt bei den Gerätetypen Rechnung trägt – unabhängig davon, von welchem Ort sie sich mit dem Netzwerk verbinden. Forescout bietet die Plattform, Tools und Expertise, um Sie bei der effizienten Planung und Implementierung einer solchen Lösung zu unterstützen.

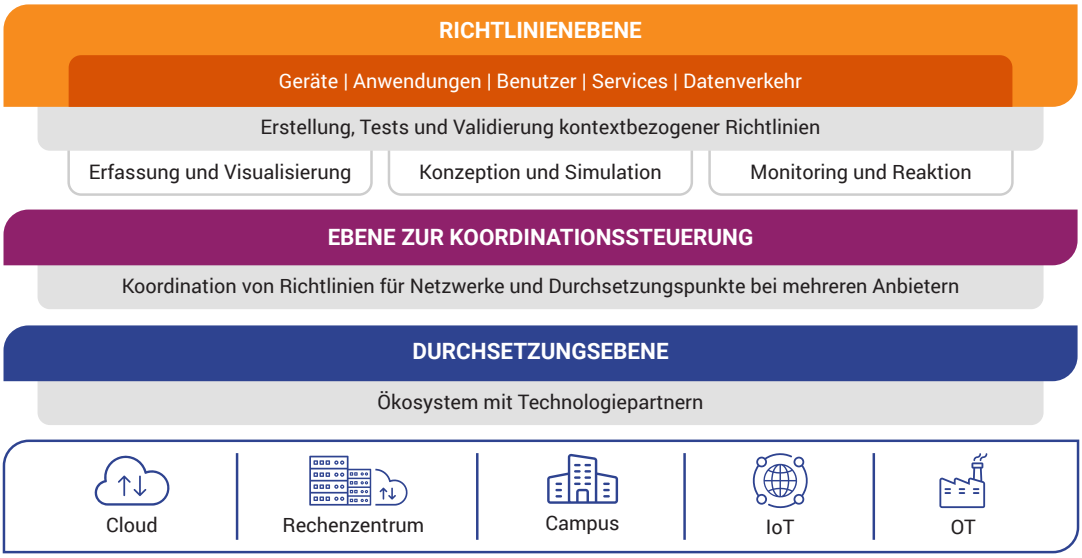
STEIGERN SIE DEN WERT IHRER SICHERHEITS- UND IT-INVESTITIONEN

- Unterbrechungsfreie und dynamische Segmentierung
- Zuverlässige Beschleunigung von Projekten zur Zero-Trust-Netzwerksegmentierung
- Geringeres Risiko von Geschäftsunterbrechungen
- Senkung der Betriebskosten
- Schnelle Anpassung an rechtliche Vorgaben und Compliance-Vorschriften
- Nutzung vorhandener Infrastrukturinvestitionen

WORKSHOP ZU NETZWERK-SEGMENTIERUNG

Möchten Sie Ihre Forescout-Bereitstellung für erweiterte Segmentierungskontrollen nutzen? Forescout-Berater bieten jetzt einen Workshop zu Netzwerksegmentierung an, damit Ihre entsprechenden Richtlinien und Implementierungen die Geschäftsstrategie unterstützen
Weitere Informationen

forescout.com/solutions/network-segmentation info-dach@forescout.com Telefon (weltweit): +1-408-213-3191



Lösungskomponenten
Die Forescout-Plattform unterstützt Unternehmen bei der Entwicklung ihrer unternehmensweiten Strategien zur Netzwerksegmentierung und Beschleunigung von Bereitstellungen. Die Plattform umfasst diese Kernprodukte:

Forescout eyeSight: Umfangreicher Kontext für jede IP-Adresse
Forescout eyeSight bietet einzigartige Einblicke und Kontext für das gesamte erweiterte Netzwerk vom Campus zum Rechenzentrum und die Cloud. Damit wird Ihr verbundenes Inventar zu einer logischen Taxonomie von Geräten, Anwendungen, Benutzern und Services, mit der Sie alle verbundenen Geräte zur Netzwerksegmentierung in eine logische Geschäftshierarchie gruppieren können. Weitere Informationen unter https://forescout.de/ressourcen/eyesight-datenblatt/.

Forescout eyeSegment: Einfache Zero-Trust-Segmentierung für alle Geräte an jedem Ort
OrtForescout eyeSegment beschleunigt die Konzeption, Planung und Bereitstellung dynamischer Zero-Trust-Segmentierung für das gesamte Unternehmensnetzwerk.

Dadurch lassen sich Zero-Trust-Prinzipien auch für EoT-Geräte implementieren. Dank der Beschleunigung von Segmentierungsprojekten für das gesamte Unternehmensnetzwerk können Sie mit eyeSegment die Angriffsfläche reduzieren, den Wirkungsradius von Angriffen einschränken sowie rechtliche und geschäftliche Risiken minimieren. Weitere Informationen unter https://forescout.de/ressourcen/eyesegment-datenblatt/.

eyeControl/eyeExtend: Koordinierung einheitlicher Kontrollen für Netzwerkdomänen und Umgebungen mit mehreren Anbietern
Die Forescout-Plattform erlaubt die dynamische Koordinierung von Segmentierungsrichtlinien sowie die Automatisierung von Kontrollen für heterogene Durchsetzungstechnologien mit Forescout eyeControl und eyeExtend.

- eyeControl dient zur einheitlichen Durchsetzung kontextbezogener Segmentierungsrichtlinien und -kontrollen für vorhandene Basistechnologien, sodass auf Agenten verzichtet werden kann. Weitere Informationen unter https://forescout.de/ressourcen/eyecontrol-datasheet/.
- eyeExtend koordiniert Kontrollen über standardmäßige Integrationen mit führenden NGFW-Anbietern (Next-Generation Firewall). Weitere Informationen zu Forescout-NGFW-Integrationen unter www.forescout.com/platform/eyeExtend.

Die Forescout-Segmentierungslösung erlaubt die Konzentration auf das Wesentliche, sodass Sie bestimmte Datenverkehrsmuster in Ihrer Umgebung analysieren und untersuchen können, wie in der Abbildung oben dargestellt.

Sie erfassen sofort die aktuelle Situation der Kommunikationsflüsse und können die richtigen Zero-Trust-Segmentierungsrichtlinien erstellen. Durch diese Konzentration auf den Überblick können Sie ganz einfach Mikrosegmentierungszonen erstellen sowie den Schutz Ihres Unternehmens bei störungsfreiem Geschäftsbetrieb sicherstellen.

Anwendungsszenarien

Die Forescout-Lösung für Netzwerksegmentierung deckt verschiedenste Anwendungsszenarien in Branchen wie Gesundheitswesen, OT (operative Technologie), Finanzdienstleistungen, Behörden oder Einzelhandel ab. In jedem Fall werden durch die Flexibilität der Forescout-Plattform Unterbrechungen des Geschäftsbetriebs minimiert sowie die Betriebskosten für Zero-Trust-Implementierung und Segmentierungsprojekte gesenkt. Für weitere Informationen zu Anwendungsszenarien sehen Sie sich den Überblick über die Segmentierung für das gesamte Unternehmensnetzwerk an.

Zusammenfassung

Aufgrund der Komplexität domänenübergreifender Technologien werden Segmentierungsprojekte derzeit isoliert verwaltet. Weitere Faktoren wie Zero-Trust-Sicherheit, digitale Transformation sowie die Einhaltung von Konformitätsrichtlinien erfordern einen ganzheitlichen und systematischen Ansatz. Mit der Forescout-Lösung können Sie schwierige domänenübergreifende Segmentierungen für das gesamte Unternehmensnetzwerk implementieren. Durch einen Echtzeitüberblick über Ihre aktuelle Segmentierung, kontextbezogene Richtlinien, für den Geschäftsbetrieb strukturierte Gruppen sowie proaktive Richtliniensimulationen bietet die Forescout-Plattform Zero-Trust-Segmentierungskontrollen, die unterschiedliche Durchsetzungstechnologien abdecken und Ergebnisse mit Zielen abgleichen. Das Ergebnis: schnellere Umsetzung von Zero-Trust-Segmentierungsprojekten, die detailliertere Kontrollen umfassen und Risiken im gesamten Unternehmen minimieren.

1. *„Mitigating Ransomware With Zero Trust"* (Abwehr von Ransomware mit Zero Trust), Forrester Research, Inc., 8. Juni 2020

Nicht nur alles sehen, sondern alles schützen.

Kontaktieren Sie uns noch heute, damit Sie Ihr Enterprise of Things aktiv verteidigen können.

forescout.com/solutions/network-segmentation info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

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

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

Weitere Informationen finden Sie unter Forescout.de