FORESCOUT
Active Defense for the Enterprise of Things™

Moderne Netzwerkszugriffssteuerung

Agentenlose, flexible und nicht-invasive Zero-Trust-Sicherheit für Ihr Enterprise of Things

Unternehmen müssen Zero-Trust-Zugriff für ihre verschiedenen Netzwerkarten, aber auch für die zahlreichen verbundenen „Dinge“ wie Campus-Computer, Geräte von Besuchern, im Homeoffice verwendete Laptops sowie IoT-, OT- und intelligente Geräte implementieren und verwalten können. Sie benötigen eine moderne NAC-Plattform (Netzwerkzugriffssteuerung), die folgende Möglichkeiten bietet:

- Permanente Identifizierung aller vernetzten „Dinge“
- Beurteilung ihres Sicherheitszustands
- Durchsetzung von Zugriffsrichtlinien
- Automatische Implementierung von Kontrollen für Konformitätsverstöße oder außergewöhnliches Verhalten

“Zero Trust“ ist leichter gesagt als getan

Es ist nicht leicht, alle „Dinge“ zu kontrollieren, die sich mit den Unternehmensnetzwerken verbinden. IT- und Sicherheitsarchitekten, die diese Systeme implementieren, stehen hierbei vor verschiedenen Herausforderungen:

- Der Einsatz früherer NAC-Lösungen war nicht erfolgreich, weil sie zu komplex waren oder die Gefahr bestand, dass sie sich negativ auf den Geschäftsbetrieb auswirken.
- Die IoT- und OT-Geräte, die sich in den Unternehmensnetzwerken ausbreiten, können mit herkömmlichen Agenten nicht authentifiziert oder kontrolliert werden.
- 802.1X-basierte Kontrollen sind in Netzwerken mit Produkten verschiedener Anbieter nicht realisierbar.
- Geplante Netzwerk-Scans erfassen keine Spoofing-Versuche und andere Bedrohungen, die jederzeit neu auftreten können.
- Viele Alternativen zum Zero-Trust-Zugriff sind zu kostspielig und/oder verursachen zu viel manuellen Aufwand.

> **Uns wurde gesagt, dass wir die Forescout-Plattform an einem Nachmittag implementieren könnten. Ein Teammitglied und ich schauten uns an, und wir beide rollten mit den Augen. Dann waren wir aber tatsächlich nach wenigen Stunden fertig!**
>
> **MIKE ROLING**
> **CISO, BUNDESSTAAT MISSOURI**

forescout.com/platform/eyeControl info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

Forescout: die branchenweit beste moderne NAC-Lösung

Wenn Ihnen diese Herausforderungen bekannt vorkommen, ist jetzt der richtige Zeitpunkt für einen genauen Blick auf Netzwerkzugriffssteuerung (NAC) von Forescout. Wir können Ihre Anforderungen erfüllen und Ihre Erwartungen übertreffen, und zwar durch:

Umfassendste Transparenz

Profitieren Sie dank unserer über 20 aktiven und passiven Techniken von voller Echtzeittransparenz für alle Geräte, die mit Ihren umfangreichen Netzwerken verbunden sind.

Zero Trust für alle verbundenen Geräte

Dämmen Sie die Auswirkungen von Kompromittierungen durch permanentes agentenloses Monitoring und ein einheitliches Richtlinienmodul ein, das alle mit Ihrem Unternehmen verbundenen "Dinge" dynamisch segmentiert und isoliert.

Nicht-invasive Bereitstellung mit schnellem Nutzen für Ihr Netzwerk

Dank der agentenlosen Software, für die kein Infrastruktur-Upgrade und keine 802.1X-Konfiguration erforderlich ist, verschaffen Sie sich innerhalb von Tagen volle Transparenz und haben innerhalb weniger Wochen eine automatisierte Kontrolle.

Erfolgreichen Einsatz in umfangreichen Unternehmensnetzwerken

Unsere zahlreichen zufriedenen Fortune-1000-Kunden, einige davon mit zwei Millionen Endgeräten, sind ein Beleg für die Fähigkeiten von Forescout und zeigt, dass sie Vertrauen in unseren Netzwerkschutz haben.

STEIGERN SIE DEN WERT IHRER SICHERHEITS- UND IT-INVESTITIONEN

Die meisten Sicherheitstools kennzeichnen Verstöße lediglich und informieren dann die verantwortlichen Mitarbeiter. Die Forescout-Plattform verfügt über Plug-and-Play-Module, die die Transparenz und Steuerungsmöglichkeiten erweitern, um:

- Echtzeit-Gerätekontext mit Ihren Sicherheits- und IT-Verwaltungstools auszutauschen
- Arbeitsabläufe zu koordinieren und Reaktionsmaßnahmen zu automatisieren
- Die Sicherheitslage durchgängig einzustufen und die Konformität von Geräten automatisch durchzusetze.

„NAC-Lösungen sind heute am besten für die Isolierung von Geräten und nicht genehmigten Elementen (Benutzer, Segmente, Geräte usw.) geeignet, sodass diese nicht mit dem Netzwerk ‚in Berührung' kommen. Verwenden Sie diese moderneren NAC-Technologien von Anbietern wie Forescout dafür, unbekannte und wahrscheinlich ungepatchte Objekte von Ihren Zero-Trust-Netzwerken fernzuhalten."[1]

CHASE CUNNINGHAM
PRINCIPAL ANALYST, FORRESTER RESEARCH

IDENTIFIZIEREN

Erkennung, Klassifizierung und Bestandserfassung aller verbundenen Geräte

Mit der Forescout-Plattform verschaffen sich Sicherheits- und IT-Teams einen umfassenden Echtzeitüberblick über alle per IP-Adresse vernetzten Geräte, sobald diese auf das Netzwerk zugreifen. Dadurch erhalten die Mitarbeiter in Echtzeit ein akkurates Ressourceninventar.

- Wählen Sie aus den über 20 aktiven und passiven Erkennungs- und Profilerstellungsmethoden die passenden für Ihre Geschäftsumgebung aus und stellen Sie die unterbrechungslose Verfügbarkeit Ihres Netzwerks sicher.
- Die über 12 Millionen Geräte-Fingerprints in der Forescout Device Cloud bieten Ihnen hochpräzise dreidimensionale Funktionen zur Geräteklassifizierung, um Gerätefunktion, Betriebssystem, Anbieter und Modell sowie weitere Informationen zu bestimmen.
- Verschaffen Sie sich einen kompletten Überblick über alle Standorte, Netzwerke und Gerätetypen – ganz ohne blinde Flecken – mit oder ohne 802.1X-Authentifizierung.

EINHALTEN

Einstufung der Sicherheitslage und Konformität

Agentenbasierte Sicherheitstools sind blind, wenn es um verwaltete Geräte mit fehlenden, defekten oder funktionsunfähigen Agenten geht. Da IoT-Geräte zudem keine Sicherheitsagenten unterstützen können, haben diese Tools auch keine Möglichkeit, sie einzustufen, wodurch die Angriffsfläche sich weiter vergrößert. Mit der Forescout-Plattform können Sie jedoch die fortgehende Einstufung der Sicherheitslage und die Behebungsmaßnahmen für alle IP-basierten Geräte automatisieren, sobald diese eine Verbindung hergestellt haben.

- Finden Sie verwaltete Geräte und nehmen Sie mit Ihren vorhandenen Sicherheitstools Korrekturen bei fehlenden, defekten oder nicht funktionierenden Agenten vor.
- Erkennen Sie Konformitätsverstöße, Veränderungen der Sicherheitslage, Schwachstellen, schwache Anmeldeinformationen, Kompromittierungsindikatoren, Spoofing-Versuche und andere Eigenschaften, die auf ein erhöhtes Sicherheitsrisiko hindeuten – alles ohne Agenten.

> **Der Umfang der Daten, die wir von der Forescout-Plattform erhalten, ist einfach unglaublich. Sie ist das mit Abstand beste Tool, das ich jemals verwendet habe, um Systeme zuverlässig zu finden, zu identifizieren und zu steuern. Sie hat ihren Mehrwert für uns deutlich bewiesen.**
>
> **JOSEPH CARDAMONE**
> **SENIOR INFORMATION SECURITY ANALYST, HAWORTH INTERNATIONAL**

forescout.com/platform/eyeControl info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

- Bewerten und überwachen Sie nicht verwaltete Geräte permanent, selbst die Geräte, die keine Agenten haben, um deren Sicherheitskonformität durchsetzen zu können.

VERBINDEN

Durchsetzung von Zugriffsrichtlinien in heterogenen Netzwerken

Die Forescout-Plattform setzt Zero-Trust-Sicherheit auf Basis der Geräte- und Benutzeridentität, des Gerätezustands und des aktuellen Konformitätsstatus durch, ohne dass Hardware- oder Software-Upgrades für die Infrastruktur erforderlich sind.

- Stellen Sie Least-Privilege-Zugriff auf Unternehmensressourcen anhand von Benutzerrolle, Gerätetyp und Sicherheitslage bereit.
- Verhindern Sie die Verbindung von unberechtigten, nicht autorisierten Geräten oder Geräten mit gefälschter Identität.
- Setzen Sie flexible Kontrollen durch für drahtgebundene, drahtlose und VPN-Infrastruktur – mit oder ohne 802.1X.

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook" (Das Zero Trust eXtended-Ökosystem: Strategischer Netzwerkplan: Playbook zu Sicherheitsarchitektur und Operation), Forrester Research, 2. Januar 2019.
2. Forrester WaveTM: „Zero Trust eXtended Platform Providers, Q4 2019" (Anbieter für Zero Trust eXtended-Plattformen, 4. Quartal 2019).

Die Plattform und die Fähigkeiten [von Forescout] für IoT/OT-Sicherheit übertreffen die der Mitbewerber. Maximaler Überblick führt zu maximaler operativer Kontrolle und letztendlich Sicherheit. Das ist der Kernpunkt des Zero-Trust-Ansatzes von Forescout.[2]

FORRESTER RESEARCH

Nicht nur alles sehen, sondern alles schützen.

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

forescout.com/platform/eyeControl 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

© 2020 Forescout Technologies, Inc. Alle Rechte vorbehalten. Forescout Technologies, Inc. ist ein Unternehmen aus Delaware. Eine Liste unserer Marken und Patente finden Sie unter https://www.forescout.com/ company/legal/intellectual-property-patents-trademarks. Andere genannte Marken, Produkte oder Servicenamen können Marken oder Servicemarken ihrer jeweiligen Eigentümer sein.
Version 08_20