FORESCOUT

Kurzvorstellung

Moderne Netzwerkszugriffssteuerung (NAC)

„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

Netzwerke benötigen heute eine moderne NAC-Lösung, also eine Netzwerkzugriffssteuerung, die sehr viel mehr leisten kann als reine Geräteauthentifizierung. Sie muss Geräte identifizieren, die Sicherheits- und Konformitätslage einstufen, die Zugriffssteuerung in heterogenen Netzwerken durchsetzen, alle verbundenen Geräte permanent überwachen und die Behebungsmaßnahmen auf auftauchende Konformitätsverstöße oder außergewöhnliches Verhalten automatisieren können.

Herausforderungen

Da sich die Geschäfts- und Sicherheitsanforderungen ständig weiterentwickeln, muss eine NAC-Lösung in Unternehmen mehr leisten können, um die folgenden Herausforderungen zu bewältigen:

- In vielen Netzwerken übertrifft die Zahl der nicht verwalteten Geräte die der verwalteten Geräte.Eine Authentifizierung mit herkömmlichen Methoden ist hierbei nicht möglich.
- Die zunehmende Zahl nicht verwalteter Geräte stellt ein zusätzliches Risiko dar und führt zu blinden Flecken.
- Heterogene Netzwerke mit Ressourcen von verschiedenen Anbietern sind weit verbreitet und erfordern Alternativen zu 802.1X.
- Remote-Unternehmenssysteme und BYOD-Systeme, die sich mit dem Netzwerk verbinden, sorgen für neue Herausforderungen in der Sicherheitsverwaltung.
- Fehlende Automatisierungsmöglichkeiten für Sicherheits-, Konformitäts- und Zugriffsrichtlinien steigern Betriebskosten und manuellen Aufwand.

Die Lösung

Wenn Ihnen diese Herausforderungen bekannt vorkommen, ist jetzt der richtige Zeitpunkt für einen genauen Blick auf eine Netzwerkzugriffssteuerung (NAC). Die Forescout-Plattform definiert neu, was NAC ist und wie sie die Geschäfts- und IT-Sicherheitsherausforderungen für Ihr Unternehmen lösen kann. Die moderne NAC-Lösung von Forescout verursacht zudem keine Unterbrechungen des Geschäftsbetriebs und lässt sich einfach implementieren. Innerhalb weniger Tage

„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

nach der Implementierung können Sie sich einen umfassenden Überblick über alle Geräte verschaffen, und die richtlinienbasierten Kontrollen funktionieren oft schon innerhalb einiger Wochen.

Unsere moderne NAC-Plattform bietet grundlegende Netzwerksicherheitsfunktionen, die weit über eine einfache Authentifizierung hinausgehen. Diese neuen Funktionen umfassen detaillierte

Geräte-/Benutzeridentifizierung, die Einstufung von Sicherheits- und Konformitätslage, permanente Geräte-Überwachung, flexible Steuerungsoptionen sowie automatisierte Behebungsmaßnahmen.

Gewöhnliche NAC-Ansätze können neuartige Systeme wie etwa IoT-Geräte (Internet of Things), die sich heute mit den Campus-Netzwerken verbinden, nicht sicher authentifizieren. Zudem können sie die Sicherheitslage und Konformität konventioneller Computer nur mit Hilfe von Agenten einstufen. Die Erkennungs- und Profilerstellungsfunktionen von Forescout identifizieren, klassifizieren und bewerten alle diese Geräte zuverlässig, sodass Sie kontextbezogene Zugriffsrichtlinien erstellen können. Die Forescout-Plattform funktioniert mit oder ohne Agenten, mit oder ohne 802.1X und überwacht alle Geräte in Ihrem Netzwerk permanent.

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 verbundenen 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 ununterbrochene 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.

„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, Sr. Information Security Analyst, Haworth International

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 installieren 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 defekten oder fehlenden Agenten vor.
- Erkennen Sie Konformitätsverstöße, Veränderungen der Sicherheitslage, Schwachstellen, schwache Anmeldeinformationen, Kompromittierungsindikatoren, Spoofing-Versuche und andere Eigenschaften, die auf ein erhöhtes Sicherheitsrisiko deuten – alles ohne Agenten.

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 durchzusetzen

Unter forescout.de erhalten Sie weitere Informationen.

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

—Forrester Research

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

Verbinden: Durchsetzen von Zugriffsrichtlinien in heterogenen Netzwerken

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

- Bereitstellung des Least-Privilege-Zugriffs auf Unternehmensressourcen anhand von Benutzerrolle, Gerätetyp und Sicherheitslage
- Verhindern der Verbindung von unberechtigten, nicht autorisierten Geräten oder Geräten mit gefälschter Identität
- Sicherer und zuverlässiger Umgang mit internen Audits und externen Vorschriften, da Ihre Sicherheitssteuerungen Konformitätsrichtlinien durchsetzen, während Ihre Benutzer produktiv weiterarbeiten können

Gründe für Forescout:

1. Schnelle, flexible Implementierung, die keine Störungen verursacht
2. Bewertung von Sicherheitslage und Risiken ohne Agenten
3. Schnelle Rendite
4. Anbieterunabhängig – nutzen Sie Ihre vorhandene Infrastruktur
5. Keine Software- oder Hardware-Upgrades
6. Integrationen mit führenden IT- und Sicherheitsprodukten
7. Vermeidung von 802.1X-Komplexität und Betriebskosten für kabelgebundene Netzwerke
8. Für große Unternehmen geeignet – Skalierung auf bis zu zwei Millionen Endgeräte
9. Robustes Richtlinienmodul automatisiert die Reaktion auf Zwischenfälle zur Verkürzung der mittleren Reaktionszeit
10. Forrester Zero-Trust-Plattform

Machen Sie den nächsten Schritt:

- Fordern Sie eine Forescout-Demo an
- Besuchen Sie unsere Webseite www.forescout.de

*** Hinweise**

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 Wave™: „Zero Trust eXtended Platform Providers, Q4 2019“ (Anbieter für Zero Trust eXtended-Plattformen, 4. Quartal 2019).

FORESCOUT

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

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

Erfahren Sie mehr unter Forescout.de