FORESCOUT

Device Visibility and Control: Agentenlose Gerätetransparenz und -kontrolle

Unverzichtbare Funktionen für effektive Cybersicherheit

> "Transparenz ist für den Schutz aller wertvollen Assets unverzichtbar. Je besser Ihre Netzwerktransparenz in Ihrem geschäftlichen Ökosystem, desto größere Chancen haben Sie, die Zeichen einer aktuellen Kompromittierung zu entdecken und sie zu stoppen." [1]
>
> **– Dr. Chase Cunningham, Leitender Analyst, Forrester Research**

Device Visibility and Control: Warum Sie Gerätetransparenz und -kontrolle benötigen

Die Möglichkeit zur Erkennung, Klassifizierung, Bewertung und Kontrolle aller mit Ihrem Netzwerk verbundenen Geräte ist eine unverzichtbare Voraussetzung für die Absicherung Ihrer Systeme und Ihres Unternehmens. Zu Ihren Aufgaben als Sicherheitsverantwortlicher gehört, die System- und Gerätesicherheit zuverlässig zu gewährleisten, schnell und richtig auf Zwischenfälle zu reagieren, Compliance zu erreichen, Risiken für das Geschäft und die Infrastruktur zu kontrollieren sowie die Effizienz der Sicherheitsmaßnahmen zu optimieren. Dies können Sie nur mit Echtzeitinformationen über jedes physische und virtuelle Endgerät in jedem Segment, detaillierte Einblicke in Konfiguration und Sicherheitsstatus sowie automatisierte und richtlinienbasierte Zugriffskontrollen erreichen. Angreifer suchen permanent nach unverwalteten und nicht abgesicherten Geräten und werden früher oder später Ihre „blinden Flecken" entdecken und ausnutzen. Transparenz und Kontrolle sind die Grundpfeiler von Sicherheit und Compliance.

Schwierige Umsetzung von Transparenz und Kontrolle

Die Verwaltung von Netzwerkendgeräten wird üblicherweise mithilfe eines Software-Agenten auf jedem Gerät realisiert. Als die meisten Endgeräte noch statische, unternehmenseigene PCs oder Server waren, funktionierte diese Methode gut genug, doch angesichts von Mobilität, unterschiedlichen Gerätetypen und Virtualisierung lässt sich kontextbezogene Transparenz und Kontrolle erheblich schwieriger erreichen. In heutigen Unternehmensumgebungen sind die Cloud- und Rechenzentrum-Segmente voller dynamisch bereitgestellter Workloads, die auf virtuellen Maschinen ausgeführt und mit virtualisierten Netzwerken verbunden werden. Die Campus-Segmente sind mit benutzereigenen BYOD-Laptops, Tablets und Smartphones ohne Sicherheitsagenten bevölkert sowie mit IoT-Geräten (Internet of Things, Internet der Dinge), die diese Agenten gar nicht erst unterstützen. OT-Segmente (operative Technologie) enthalten riesige Mengen an Geräten ohne Agentenunterstützung, die zudem mit proprietären Protokollen kommunizieren, geschäftskritische Prozesse verwalten und keine internen Eingriffe zulassen. Deshalb benötigen IT-Abteilungen dringend eine agentenlose Lösung, die für diese unterschiedlichen Umgebungen umfassende Transparenz und Kontrolle bietet.

Die Lösung von Forescout: Device Visibility and Control, Agentenlose Gerätetransparenz und -kontrolle

Forescout Technologies ist Vorreiter im agentenlosen Netzwerksicherheitsansatz, der den Herausforderungen bei der Gerätetransparenz und -kontrolle in heutigen dynamischen und heterogenen Umgebungen Rechnung trägt. Die Forescout-Plattform für Device Visibility and Control, bietet durch Gerätetransparenz und -kontrolle einen kontinuierlichen und einheitlichen Überblick über alle Geräte in Ihren Campus-, Rechenzentrum-, Cloud- und OT-Netzwerken.

Die Forescout-Plattform erkennt:

- Campus-Netzwerkgeräte: Laptops, Tablets, Smartphones, BYOD-/Gastsysteme und IoT-Geräte
- Rechenzentrum-Infrastruktur: Virtuelle Maschinen, Hypervisoren, physische Server und physische Netzwerke
- Public- und Private-Cloud-Infrastruktur: Virtuelle Maschinen in AWS®, Microsoft® Azure® und VMware®
- OT- und Industriesteuerungssysteme (Industrial Control Systems, ICS): Medizin-, Industrie- und Gebäudeautomatisierungsgeräte
- Physische und Software-definierte Netzwerkinfrastruktur: Switches, Router, Firewalls, VPNs, drahtlose Zugriffspunkte und Controller

Abbildung 1: Forescout's Gerätetransparenz ist für das erweiterte Unternehmen skalierbar.

> "Bewertungen und der Überblick über Risiko/Vertrauenswürdigkeit sowie der Austausch von Kontextinformationen sind zum Immunsystem digitaler Unternehmen geworden." [2]
>
> **– Neil MacDonald, Vizepräsident, Analyst, Gartner**

Funktionsumfang

Dank Forescout erhalten IT-Abteilungen folgende Möglichkeiten:

- Erkennung aller per IP-Adresse verbundenen Geräte in jedem Netzwerk: physische und virtuelle Geräte in Campus-, Rechenzentrum-, Cloud- und Industrieumgebungen
- Klassifizierung unterschiedlicher IT-, IoT- und OT/ICS-Geräte sowie virtueller Maschinen (VMs) und Cloud-Instanzen in Echtzeit basierend auf Daten zu Gerätetyp und Funktion, Anbieter, Modell, Betriebssystem und Version
- Bewertung und kontinuierliches Monitoring des Gerätesicherheitsstatus für Richtlinien-Compliance
- Einhaltung von Richtlinien, Branchenvorschriften und Best Practices, z. B. zur Netzwerksegmentierung
- Sperrung, Blockierung bzw. Isolierung nicht konformer oder kompromittierter Geräte
- Automatisierung von Kontrollaktionen für Endgeräte, Netzwerk und Drittanbieter

Erkennung aller per IP-Adresse vernetzten Geräte und OT-Systeme in jedem Segment

Die Forescout-Plattform bietet mehr als 20 konfigurierbare Techniken zur Informationsgewinnung mit einer starken Integration führender IT- und OT-Netzwerk-Switches, Router, drahtloser Zugriffspunkte, Firewalls, VPN-Konzentratoren und Rechenzentrum- sowie Cloud-Lösungsanbieter. Die Plattform untersucht passiv den Netzwerkverkehr, analysiert viele unterschiedliche Protokollströme und kann direkt mit Netzwerkinfrastruktur und Endgeräten interagieren. Forescout bietet folgende Transparenztechniken:

- **Passive Methoden für das Netzwerk und das Endgerät**: Dazu gehören der Empfang von SNMP-Traps von Switches und WLAN-Controllern, die Überwachung eines SPAN-Ports und Analyse von Protokollströmen im Datenverkehr (Forescout bietet Deep Packet Inspection für mehr als 100 IT- und OT-Protokolle), die Erfassung und Analyse von Flussdaten sowie die Bewertung von DHCP-Anforderungen und HTTP-Benutzeragenten-Datenverkehr. Wenn 802.1X implementiert ist, kann Forescout einen integrierten oder externen RADIUS-Server überwachen.
- **Aktive Methoden in der Netzwerkinfrastruktur:** Dazu gehört das Abfragen von Switches, VPN-Konzentratoren, WLAN-Controllern und Private- sowie Public-Cloud-Controllern für eine Liste verbundener Geräte und VMs. Für Benutzer- und Gerätedaten fragt die Forescout-Plattform Verzeichnisdienste, Webanwendungen oder externe Datenbanken ab.
- **Aktive Methoden auf dem Endgerät:** Dazu gehören das Scannen von Netzwerksegmenten auf vernetzte Geräte mit NMAP, die Remoteuntersuchung von Windows-Geräten mit WMI bzw. Mac- und Linux-Geräten mit SSH sowie das Erstellen von Endgeräteprofilen mit SNMP-Abfragen.

Gerätetransparenz-Techniken

PASSIVE TECHNIKEN
SNMP-Traps
SPAN-Datenverkehr
DHCP-Anforderungen
HTTP-Benutzeragent
TCP-Fingerabdrücke
DICOM-Protokollanalysen (medizinische Bildgebungssysteme)
ICS OT-Protokollanalysen (mehr als 60 Protokolle)
Datenflussanalysen
NetFlow
Flexible NetFlow
IPFIX
sFlow
DHCP-Anforderungen (per IP-Helper)
HTTP-Benutzeragent (per URL-Umleitung)
RADIUS-Anforderungen
MAC OUI

AKTIVE INFRASTRUKTUR-ERKENNUNG
Abrufen der physischen Netzwerkinfrastruktur
Controller-basierte Netzwerkinfrastruktur-Integration
Meraki
Cisco ACI
Private-Cloud-Integration (virtuelle Infrastruktur)
VMware
Public-Cloud-Integration
AWS
Azure
Abfrage von Verzeichnisdiensten (LDAP)
Abfrage von Webanwendungen (REST)
Abfrage externer Datenbanken (SQL)
Koordinierungen (ITSM, UEM, EPP, EDR, VA)

AKTIVE ENDGERÄTE-ERKENNUNG
Agentenlose Untersuchung Windows (WMI, RPC, SMB)
Agentenlose Untersuchung macOS, Linux (SSH)
NMAP
SNMP-Abfragen an Endgeräte
Agentenbasierte Untersuchung (SecureConnector)

Abbildung 2: Forescout-Methoden zur Gerätetransparenz.

Vorteile mehrerer Gerätetransparenz-Techniken

Die Forescout-Plattform bietet viele verschiedene Erkennungsmethoden, die sich bei der Einrichtung einfach konfigurieren (und hinterher ändern) lassen. Dadurch erhalten Sie einzigartige Flexibilität, Effizient und Effektivität.

Ausschließlich passive Erkennung, Klassifizierung und Bewertung für OT-Netzwerke: OT-Netzwerke sind für aktive Test- und Scantechniken, die potenziell Prozesskontrollsysteme und Geschäftsabläufe unterbrechen können, häufig ungeeignet. Sobald Sie die Geräte genauer kennen, können Sie selektiv geeignete aktive Methoden anwenden. Die Forescout-Plattform bietet Gerätetransparenz für verschiedenste OT-Netzwerke. Erreicht wird das mithilfe einer komplett passiven Kombination aus SPAN-Datenverkehr-Spiegelung und Deep Packet Inspection für fast 100 OT-spezifische Protokolle. Forescout unterstützt Industriestandard-Protokolle wie BACnet, CIP, DNP3, Ethernet/IP, ICCP, IEC 60870-5-104, IEC 60850, IEEE C37.118, Modbus/TCP, OPC, PROFINET und Siemens S7. Wir unterstützen auch die proprietären Protokolle führender Anbieter wie ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, Schneider Electric und Yokogawa.

Kostengünstige Bereitstellung in großen Umgebungen: Durch die verfügbaren Remote-Transparenztechniken lassen sich die Gesamtbereitstellungskosten senken, da kleine Standorte ohne eine lokale Appliance überwacht werden können.

Über die Erkennung hinausgehende Einblicke – Klassifizierung und Bewertung: Dank der gleichzeitigen Nutzung passiver und aktiver Profilerstellungstechniken kann die Forescout-Plattform vernetzte Geräte nicht nur per MAC- und IP-Adresse identifizieren. Als Klassifizierung wird der Prozess des Abrufens und Korrelierens vieler Kontextebenen bezeichnet, um ein sehr detailliertes Profil jedes Geräts zu erstellen. Bewertung ist das Vergleichen von Gerätestatuseigenschaften mit Sicherheitsrichtlinien als Basis für Zugangskontrollen und Behebungsentscheidungen. Beide Prozesse erfordern genauere Betrachtung.

Intelligente automatische Klassifizierung

Vollständiger Kontext für jedes Gerät ist für die Erstellung detaillierter Richtlinien unverzichtbar. Sie müssen den operativen Kontext oder Zweck jedes Geräts kennen, um entscheiden zu können, wie es am besten abgesichert oder verwaltet werden kann. Aufgrund der wachsenden Zahl und Vielfalt der Geräte ist die manuelle Erfassung dieses Kontexts praktisch unmöglich. Gleichzeitig gefährdet die Erstellung von Richtlinien ohne den richtigen Kontext die betrieblichen Abläufe. Mit Forescout werden herkömmliche, IoT- und OT-Geräte automatisch klassifiziert, wobei eine mehrdimensionale Klassifizierungstaxonomie verwendet wird, um Gerätefunktion und -typ, Betriebssystem und Version sowie Anbieter und Modell zu identifizieren.

Die Plattform klassifiziert automatisch Folgendes:

- Mehr als 500 unterschiedliche Betriebssystemversionen
- Mehr als 5.000 unterschiedliche Geräteanbieterprodukte und -modelle
- Geräte im Gesundheitswesen von mehr als 350 Anbietern medizinischer Geräte
- Tausende Industriesteuerungs- und Automatisierungsgeräte, die in Fertigung, Energieversorgung, Öl- und Gas, Versorgungsunternehmen, Bergbau und anderen Bereichen zum Einsatz kommen

Forescout Device Cloud führt die automatische Klassifizierung für die Plattform durch und gewährleistet, dass diese umfangreiche Kontextquelle mit dem Wachstum und der Vielfalt bei Geräten Schritt halten kann. Das Forescout Research and Intelligent Analytics-Programm nutzt Informationen von über 8 Millionen realen Geräten* in unserer Device Cloud und veröffentlicht regelmäßig neue Profile, um die Effizienz, Abdeckung und Geschwindigkeit bei der Klassifizierung in Ihrem gesamten Gerätebestand zu verbessern.

Bewertung des Gerätezustands

Die Geräteklassifizierung liefert operativen Kontext über den Zweck eines Geräts – und informiert Sie letztendlich darüber, um was für ein Gerät es sich handelt. Für vollständigen Kontext ist jedoch eine weitere Perspektive erforderlich, um den Zustand und Patch-Status jedes Geräts zu bewerten. Deshalb überwacht Forescout kontinuierlich das Netzwerk und bewertet Konfiguration, Status sowie Sicherheitslage der verbundenen Geräte. Auf diese Weise werden ihre Risikoprofile ermittelt und festgestellt, ob sie die Sicherheits- und Compliance-Richtlinien einhalten. Forescout beantwortet beispielsweise folgende wichtige Fragen:

- Laufen die Geräte mit zugelassenen Betriebssystemen einschließlich den neuesten Betriebssystem-Patches?
- Ist Sicherheitssoftware installiert, aktiv und mit den neuesten Patches aktualisiert?
- Führen Geräte nicht autorisierte Anwendungen aus oder verletzen sie Konfigurationsstandards?
- Nutzen Geräte standardmäßige oder schwache Kennwörter (ein besonderes Risiko für IoT-Geräte)?
- Wurden nicht autorisierte Geräte entdeckt, einschließlich solcher, die sich mithilfe von Spoofing-Techniken als legitime Geräte ausgeben?
- Welche verbundenen Geräte sind für die neuesten Bedrohungen am anfälligsten?

Geräteklassifizierung und -bewertung

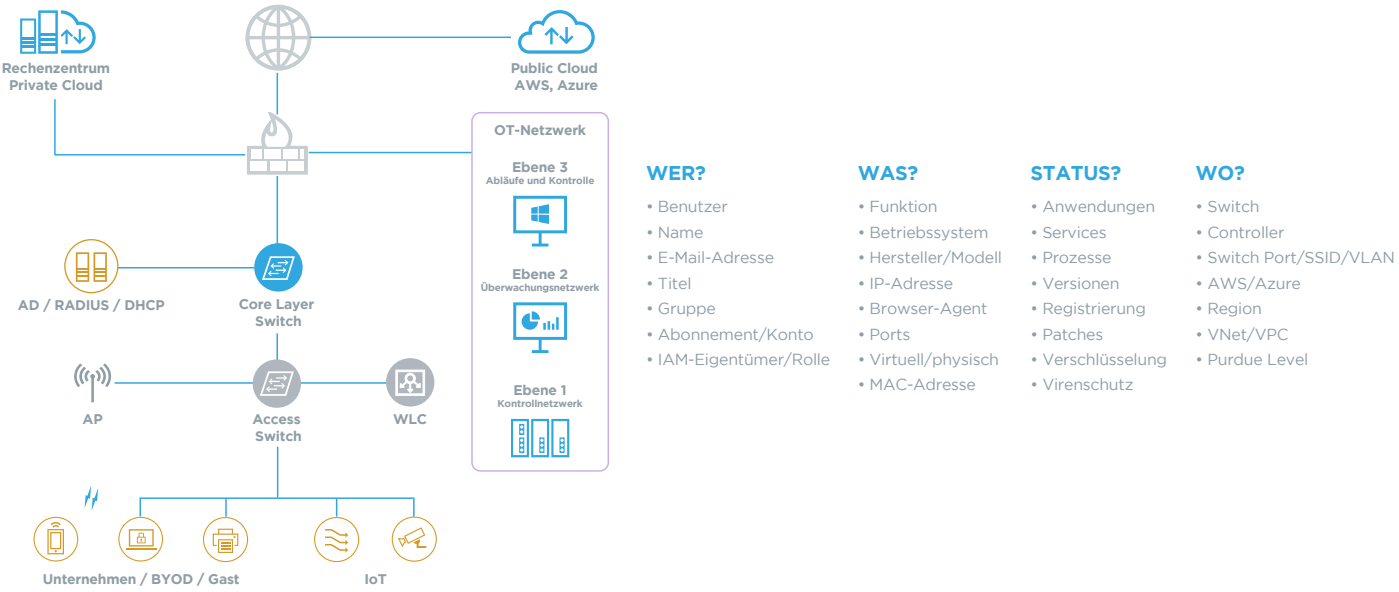

Abbildung 3: Die Forescout-Plattform kann Geräte schnell nach Typ klassifizieren, überprüft, ob sie vom Unternehmen verwaltet, unverwaltet, IoT/OT-Geräte, physisch oder virtuell sind, und unterstützt Sie bei der Bewertung ihres Compliance-Status.

Nutzung von Transparenz zur Gewährleistung von Kontrolle

Die Forescout-Plattform umfasst ein Richtlinienmodul, das kontinuierlich Geräte anhand einer Reihe anpassbarer Richtlinien überprüft, die das Geräteverhalten im Netzwerk vorschreiben und durchsetzen. Dadurch erhalten Sie eine kontinuierliche Echtzeitübersicht für bis zu 2 Millionen Geräte. Die Richtlinien werden in Echtzeit von Ereignissen ausgelöst, die entweder auf einem spezifischen Gerät oder im Netzwerk erfolgen. Dies können Netzwerkzugriffsereignisse wie der Anschluss an einen Switch-Port oder die Änderung einer IP-Adresse sein. Außerdem kann es sich um Authentifizierungsereignisse wie beispielsweise bei einem RADIUS-Server handeln. Richtlinien können auch durch Änderungen an Geräteattributen ausgelöst werden. Abbildung 4 zeigt die Bandbreite an Kontrollaktionen, die in der Forescout-Plattform möglich sind, wenn eine Richtlinie ausgelöst wird.

Forescout-Kontrollaktionen

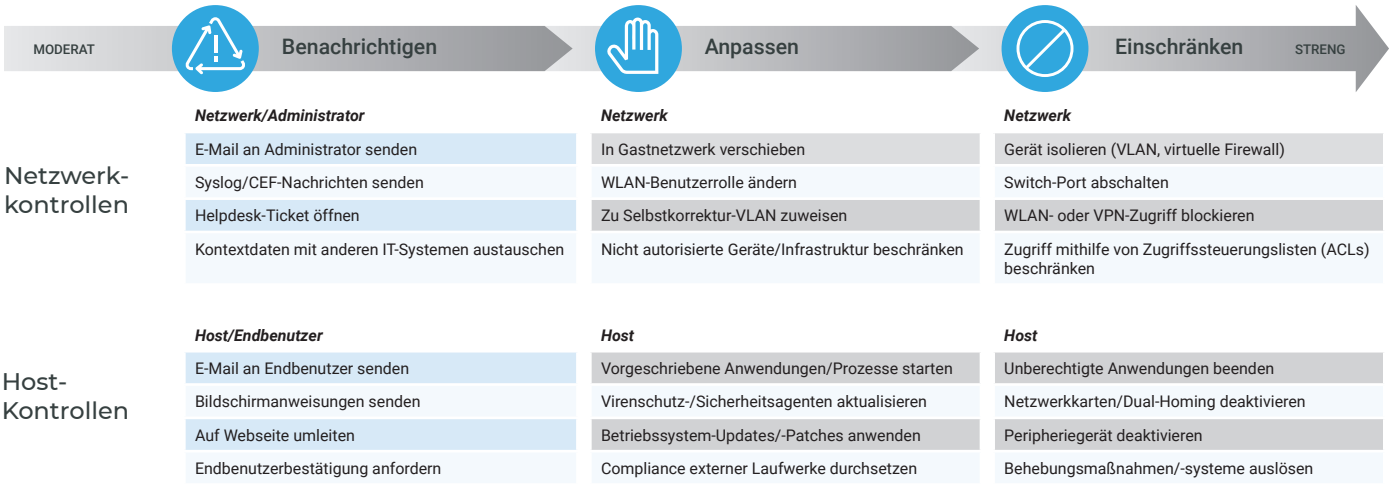

Abbildung 4: Anpassbare Kontrollaktionen ermöglichen die Durchsetzung angemessener Kontrollen – von moderat bis streng – basierend auf Ihren Sicherheitsrichtlinien.

Das Richtlinienmodul nutzt zwei Bereiche von Kontrollfunktionen. Der erste ist standardmäßig in Forescout integriert. Der zweite wird über Funktionen für Datenaustausch und Kontrollkoordinierung bereitgestellt, der mit führenden Sicherheits- und IT-Verwaltungsprodukten integriert wird.

Native Kontrollfunktionen

Die nativen Forescout-Funktionen umfassen Netzwerk- und Host-basierte Kontrollen. Die Netzwerkkontrollen bieten richtlinienbasierte Segmentierung, um den Zugriff je nach Benutzeridentität, Rolle und Gerätestatus zuzulassen oder einzuschränken. Host-basierte Kontrollen erzwingen Gerätehygienemaßnahmen. Dazu gehören das Starten und Stoppen von Anwendungen, die Aktualisierung von Virenschutz- und anderen Host-basierten Sicherheitsagenten oder die Deaktivierung von Peripheriegeräten. Das Richtlinienmodul wendet diese Richtlinien automatisch unabhängig vom Gerätestandort oder der Bewegung im Unternehmensnetzwerk und in das Rechenzentrum oder die Cloud an.

Erweiterte Kontrollfunktionen

Die Forescout-Plattform automatisiert die Richtliniendurchsetzung, beschleunigt die systemweite Reaktion und minimiert Risiken, indem sie in Echtzeit Gerätekontext austauscht und Workflows für viele verschiedene Sicherheits- und IT-Verwaltungsprodukte koordiniert. Forescout bietet Integrationen mit führenden Anbietern in den folgenden Kategorien:

- Erweiterte Bedrohungserkennung
- Client-Verwaltungstools
- Enterprise Mobility Management
- Schutz, Erkennung und Behebungsmaßnahmen für Endgeräte
- IT-Serviceverwaltung
- Firewalls der nächsten Generation
- Privilegierte Zugriffsverwaltung
- Sicherheitsinformations- und Ereignis-Management (SIEM)
- Schwachstellenbewertung

Mithilfe dieser Integrationen koordiniert die Forescout-Plattform die infrastrukturweiten Sicherheitsmaßnahmen und bietet richtliniengesteuerte Kontrollen basierend auf der Klassifizierung der Benutzer, Geräte, Anwendungen sowie des Datenverkehrs. Die Plattform erzwingt detaillierte Zugriffsrichtlinien und bietet dabei präzise und flexible Kontrolle über Ressourcen, sodass IT-Abteilungen dynamische Netzwerksegmentierung implementieren und kontextbezogene Sicherheitsrichtlinien basierend auf einem Echtzeitüberblick erstellen können.

Mögliche Kontrollaktionen

Forescout besitzt langjährige Kompetenzen bei der Netzwerkzugriffssteuerung und kann daher eine Kombination aus nativen und erweiterten Kontrollfunktionen bereitstellen. Dadurch bietet die Forescout-Plattform ein außerordentlich breites Spektrum an Gerätekontrollmöglichkeiten, die wiederum IT-Abteilungen ein leistungsstarkes Arsenal an Netzwerksicherheits-Tools in die Hand geben.

The Forescout platform enforces network access to enterprise resources based on user profile (guest, employee, contractor), device classification and security posture by:

- Differenzierter Zugriff für Gast- und BYOD-Geräte
- Durchsetzung von Netzwerkzugriffsrichtlinien mit oder ohne 802.1X-Authentifizierung
- Durchführung von Maßnahmen bei verdächtigen, nicht autorisierten oder Schatten-IT-Geräten im Netzwerk
- Einschränkung oder Blockierung des Netzwerkzugriffs für kompromittierte oder böswillige Geräte
- Quarantäne oder Isolierung nicht konformer Geräte, bis die Compliance-Verstöße beseitigt wurden

Die Forescout-Plattform verbessert die Geräte-Compliance durch die Automatisierung der Compliance-Bewertung und Durchsetzung von Behebungsmaßnahmen und gewährleistet so die kontinuierliche Einhaltung interner Sicherheitsrichtlinien, externer Standards und branchenspezifischer Vorschriften. Zu den wichtigsten Funktionen gehören:

- Gewährleistung der korrekten Konfiguration von Endgeräten und Durchführung von Behebungsmaßnahmen bei schwerwiegenden Konfigurationsverstößen (z. B. schwachen oder standardmäßigen Kennwörtern)
- Überprüfung der Installation, Ausführung und Aktualisierung aller erforderlichen Anwendungen und Sicherheitsagenten
- Deaktivierung oder Blockierung aller nicht autorisierten Anwendungen, die zu Risiken führen bzw. Netzwerkbandbreite oder Mitarbeiterproduktivität unnötig beeinträchtigen könnten
- Erkennung gefährlicher Schwachstellen und fehlender kritischer Patches sowie Durchführung von Korrekturmaßnahmen
- Durchführung proaktiver gezielter Korrekturmaßnahmen wie Installation erforderlicher Sicherheitssoftware, Aktualisierung von Agenten oder Anwendung von Sicherheits-Patches
- Implementierung von Richtlinien und Automatisierung von Kontrollen zur Einhaltung von Konfigurationsvorschriften in Cloud-Bereitstellungen (z. B. AWS, Azure und VMware)

Die Forescout-Plattform implementiert dynamische Netzwerksegmentierung mithilfe eines einheitlichen Richtlinien-Frameworks, das die Anwendung von Segmentierungsrichtlinien für unterschiedliche Durchsetzungstechnologien in Ihrer erweiterten Unternehmensumgebung erlaubt. Die Forescout-Plattform bietet folgende Möglichkeiten:

- Dynamische Zuweisung von Geräten in Segmentierungsgruppen basierend auf Geräteeigenschaften, Klassifizierung und Sicherheitsstatus
- Durchsetzung der Segmentierung für VLANs, ACLs, WLAN-Kontrollen und Tagging in Campus- und OT-Netzwerken
- Anwendung von Segmentierungskontrollen über Sicherheitsgruppen/Tags in Public- und Private-Cloud-Umgebungen wie AWS und VMware NSX®
- Segmentierung nicht konformer und anfälliger Geräte in verschiedene Zonen (insbesondere für Geräte, die nur innerhalb geplanter Wartungsfenster gepatcht oder korrigiert werden können), damit störungsfreier Geschäftsbetrieb mit minimaler Angriffsfläche gewährleistet ist

- Durchsetzung von Segmentierungsrichtlinien zur Isolierung bestimmter Geräte und kritischer Datenflüsse vom Rest des Netzwerks, wie von HIPAA, DSGVO, PCI, SWIFT CSP und anderen Vorschriften gefordert

Die Forescout-Plattform beschleunigt Vorfallreaktionen durch die schnelle und effektive Eindämmung von Bedrohungen und Reaktion auf Zwischenfälle, sodass Unterbrechungen der Geschäftsabläufe sowie Schäden für das Unternehmen minimiert werden können. Diese Lösung für Device Visibility and Control bietet Gerätetransparenz und -kontrolle mit folgenden Vorteile:

- Erkennung besonders gefährdeter Geräte, die nicht eingedämmt oder korrigiert wurden
- Integration mit ATD-Lösungen zur Erkennung von Kompromittierungsindikatoren auf Geräten sofort beim Verbindungsaufbau, um die durchschnittliche Reaktionszeit zu verkürzen
- Schnelle Isolierung und Eindämmung kompromittierter oder böswilliger Geräte, um die Ausbreitung von Malware innerhalb des Netzwerks zu vermeiden
- Automatisierung der Reaktion auf Zwischenfälle und Initiierung von Korrektur-Workflows auf kompromittierten Geräten
- Kürzere mittlere Reaktionszeit durch Bereitstellung von wertvollem Gerätekontext (Geräteverbindung, Standort, Klassifizierung und Sicherheitsstatus) für funktionsübergreifende Vorfallreaktionsteams und isolierte Technologien

Sicherheit beginnt mit Transparenz

Es gibt einen guten Grund dafür, dass militärische Befehlshaber stets alles daran setzen, eine erhöhte Position zu erlangen und zu halten. Hier sind anrückende Gegner schon von weitem sichtbar, sodass die Verteidiger schon vor Beginn des Angriffs reagieren können. Die Forescout-Plattform bietet IT-Abteilungen einen solchen vollständigen Überblick über die zu schützende Netzwerkumgebung. Durch die kontinuierliche Erkennung, Klassifizierung, Bewertung und Kontrolle jedes Geräts unabhängig davon, wo es verbunden ist, macht Forescout das IT-Schlachtfeld sichtbar, verständlich und kontrollierbar.

Testen Sie die Forescout-Plattform selbst

Die beste Möglichkeit, ein besseres Verständnis der agentenlosen Gerätetransparenz und -kontrollfunktionen der Device Visibility and Control-Plattform von Forescout zu erhalten, ist es dies aus erster Hand zu erleben. Forescout bietet verschiedene Möglichkeiten, um die Device Visiblity and ControlPlattform besser kennenzulernen, darunter:

Test Drive starten: Erleben Sie den Vorher-Nachher-Effekt der Forescout-Plattform mit einem praktischen Testlauf, der Sie durch sechs überzeugende Anwendungsszenarien führt.

Ihren Forescout Absolute Visibility and Risk Report abrufen: Hier erhalten Sie eine detaillierte Geräteübersicht und Risikobewertung. Weitere Informationen erhalten Sie von Ihrem örtlichen Forescout-Vertreter.

Demo anfordern: Besuchen Sie die Forescout-Webseite um eine persönliche Demo anzufordern und weitere Informationen zu erhalten.

Verwenden Sie das Forescout Business Value ROI Tool (in englisch): Hier können Sie in nur 10 Minuten den geschäftlichen Mehrwert der Forescout-Plattform für Ihr Unternehmen ermitteln (berechnet nach dem IDC Business Value Model)

* Stand: 31. März 2019

[1] „The Zero Trust eXtended (ZTX) Ecosystem" (Das ZTX-Ökosystem), Forrester Research, Januar 2018

[2] „Zero Trust Is an Initial Step on the Roadmap to CARTA" (Zero Trust ist ein erster Schritt auf dem Weg zu CARTA), Gartner, Dezember 2018

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 www.forescout.de