FORESCOUT
Active Defense for the Enterprise of Things™

Moderne Netzwerkzugriffskontrolle

Warum agentenlose Gerätetransparenz und -kontrolle für effektive Cybersicherheit unverzichtbar sind

Gerätetransparenz und -kontrolle: Warum Sie sie benötigen

Die Möglichkeit zur Erkennung, Klassifizierung, Bewertung und Kontrolle aller mit Ihrem Netzwerk verbundenen Geräte ist eine unverzichtbare Voraussetzung für Zero-Trust-Sicherheit. Nur mit Echtzeitinformationen über jedes physische und virtuelle Endgerät in jedem Segment, detaillierten Einblicken in Konfiguration und Sicherheitsstatus sowie automatisierter und richtlinienbasierter Behebung und Zugriffskontrollen können Sie zuverlässige System- und Gerätesicherheit gewährleisten sowie schnell und richtig auf Zwischenfälle reagieren.

100%

ECHTZEITTRANSPARENZ

Angreifer suchen permanent nach unverwalteten und nicht abgesicherten Geräten und werden früher oder später Ihre „blinden Flecken“ entdecken und ausnutzen. Agentenlose Transparenz und Kontrolle sind die Grundpfeiler von Sicherheit und Compliance, spielen aber auch bei der Bewältigung zahlreicher geschäftlicher Herausforderungen eine wichtige Rolle. Beispielsweise ermöglicht permanente und detaillierte Gerätetransparenz ein akkurates Echtzeit-Geräteinventar, sodass Sicherheits- und IT-Mitarbeiter die Betriebskosten senken sowie die Einhaltung von Konformitätsvorschriften gewährleisten können. Ein weiterer Vorteil: Nicht bestandene Audits gehören der Vergangenheit an.

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

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.

Die rasante Zunahme bei Anzahl und Diversität von Geräten hat den Gerätebestand fundamental verändert. Cyber-physische Systeme wie IoT-Geräte (Internet of Things) und OT-Systeme (operative Technologie) sind heute fester Bestandteil von Unternehmensnetzwerken. Viele Angestellte arbeiten im Homeoffice und ein Teil von ihnen nutzt die Cloud. Das moderne Unternehmen hat sich schnell zu einem **Enterprise of Things** gewandelt – und die meisten dieser „Dinge" unterstützen keine Verwaltungsagenten. Doch selbst bei den Geräten, die das können, ist ein agentenbasierter Ansatz problematisch:

- Agentenbasierte Systeme funktionieren nicht, sobald die Agenten fehlen, defekt sind oder deaktiviert werden.
- Agentenbasierte und 802.1X-basierte Methoden führen zu blinden Flecken in Ihrem Netzwerk und damit zu komplexen Betriebsabläufen, was unvollständige Bereitstellungen nach sich zieht.
- Isolierte Tools für Gerätekonformität bieten keine einheitliche Übersicht, was zu weiteren blinden Flecken führt.
- In vielen Netzwerken übertrifft die Zahl der nicht verwalteten Geräte die der verwalteten Geräte. Eine Authentifizierung mit herkömmlichen Methoden ist hierbei nicht möglich.
- Mobilgeräte, BYOD, Gäste und Mitarbeiter im Homeoffice machen agentenbasierte Sicherheitsmaßnahmen zeitaufwändig und ineffektiv.
- Heterogene Netzwerke mit Ressourcen von verschiedenen Anbietern sind weit verbreitet und erfordern Alternativen zu 802.1X ohne Hardware- oder Software-Upgrades.

> **NAC-Lösungen sind heute am besten für die Isolierung von Geräten und nicht genehmigten Element-en (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]**
>
> **DR. CHASE CUNNINGHAM**
> **PRINCIPAL ANALYST, FORRESTER RESEARCH**

Die Forescout-Lösung für modernes NAC

Forescout Technologies ist der erste Anbieter mit einem agentenlosen Ansatz für Netzwerkzugriffskontrollen, der den Herausforderungen in heutigen dynamischen und heterogenen Umgebungen Rechnung trägt.

Die Forescout-Plattform bietet einen permanenten und einheitlichen Überblick über alle Geräte in Ihren Campus-, Rechenzentrum-, Cloud- und OT-Netzwerken. Sie gibt kontinuierlich detaillierte Einblicke in:

- Campus-Netzwerkgeräte: Laptops, Tablets, Smartphones, BYOD-/Gastsysteme und IoT-Geräte
- Rechenzentrum-Infrastruktur: virtuelle Maschinen, Hypervisoren, physische Server sowie weitere virtuelle und physische Netzwerkkomponenten
- 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, WLAN-APs und Controller

Umfassende Gerätetransparenz ohne blinde Flecken

Abbildung 1. Die Forescout-Gerätetransparenz ist für das erweiterte Unternehmen skalierbar und bietet ein detailliertes Echtzeit-Inventar aller Geräte, die mit Ihrem Netzwerk verbunden sind.

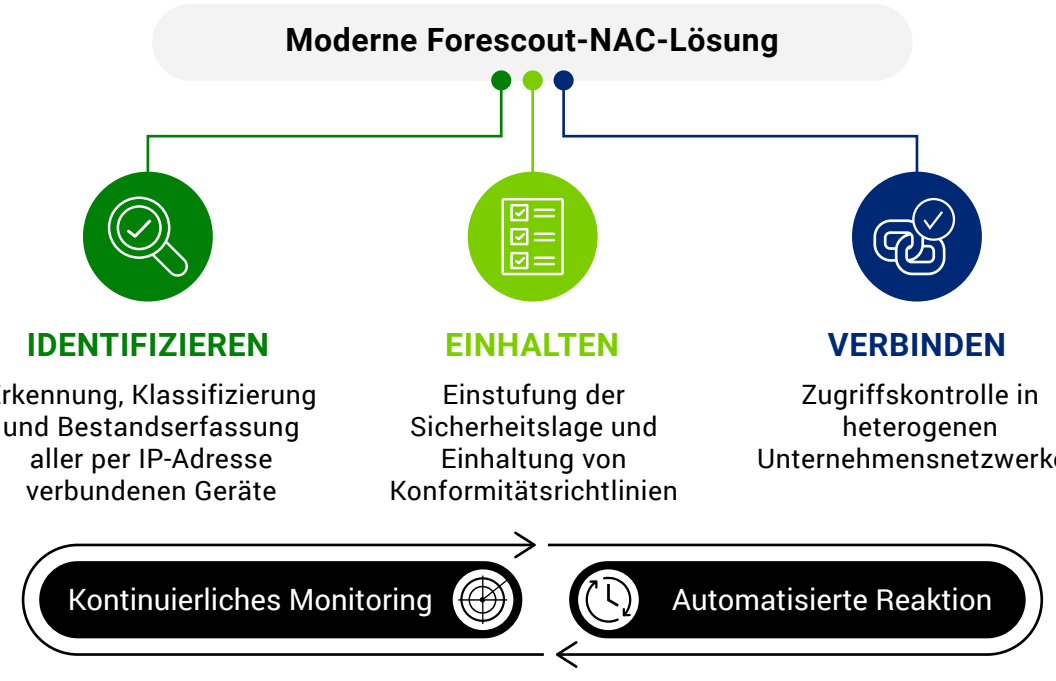


Abbildung 2. Die moderne Forescout-NAC-Lösung bietet wichtige Funktionen für beliebige heterogene Netzwerke und erfordert keine Software-Agenten oder 802.1X-Authentifizierung.

Funktionsumfang

Die moderne Forescout-NAC-Lösung bietet folgende Vorteile für die IT:

- Wahl aus mehr als 20 aktiven und passiven Techniken für die umfassendste agentenlose Geräteerkennung für alle Standorte, Netzwerke und Gerätetypen – ohne blinde Flecken
- Zuverlässige automatische Klassifizierung von Geräten anhand von Gerätefunktion, Betriebssystem und -version sowie Anbieter und Modell
- Automatische Erstellung und Pflege eines Echtzeit-Geräteinventars aller per IP-Adresse verbundenen Geräte in Ihrem erweiterten Netzwerk
- Bewertung und kontinuierliches Monitoring des Sicherheitsstatus aller Geräte – agentenlos
- Einhaltung von Sicherheitsrichtlinien und Branchenvorschriften durch die automatische Behebung von Endgeräteproblemen
- Durchsetzung flexibler Netzwerkkontrollen anhand von Authentifizierung, Benutzerrolle, Gerätetyp und Sicherheitslage für beliebige heterogene kabelgebundene, drahtlose oder VPN-Netzwerke
- Durchsetzung von Least-Privilege-Zugriffskontrollen für Zero-Trust-Sicherheit

Identifizierung aller Geräte in jedem Netzwerk

Die Forescout-Plattform bietet mehr als 20 konfigurierbare Techniken zur Informationsgewinnung mit einer tiefen Integration führender IT- und OT-Netzwerk-Switches, Router, WLAN-APs, 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 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 150 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 RADIUS-Anforderungen mithilfe eines integrierten oder externen Servers 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 verbundene 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	AKTIVE INFRASTRUKTUR-ERKENNUNG	AKTIVE ENDGERÄTE-ERKENNUNG
SNMP-Traps	Abrufen der physischen Netzwerkinfrastruktur	Agentenlose Untersuchung Windows (WMI, RPC, SMB)
SPAN-Daten • DHCP-Anforderungen • HTTP-Useragent • TCP-Fingerprints • Medizintechnik-Protokollanalysen (20 Protokolle) • ICS OT-Protokollanalysen (mehr als 70 Protokolle)	Controller-basierte Netzwerkinfrastruktur-Integration • Juniper Mist • Cisco ACI, Cisco Meraki	Agentenlose Untersuchung macOS, Linux (SSH)
Datenflussanalysen • NetFlow • Flexible NetFlow • IPFIX • sFlow	Private-Cloud-Integration (virtuelle Infrastruktur) • VMware	NMAP
DHCP-Anforderungen (per IPHelper)	Public-Cloud-Integration • AWS • Azure	SNMP-Abfragen an Endgeräte
HTTP-Benutzeragent (per URL-Umleitung)	Abfrage von Verzeichnisdiensten (LDAP)	Agentenbasierte Untersuchung (SecureConnector)
RADIUS-Anforderungen	Abfrage von Webanwendungen (REST)	
MAC OUI	Abfrage externer Datenbanken (SQL)	
	Koordinierungen (ITSM, UEM, EPP, EDR, VA)	

Figure 3: Forescout device visibility methods

Vorteile mehrerer Gerätetrans-parenz-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.

Kostengünstige einfache Bereitstellung in großen Umgebungen: Die Möglichkeit zum Auswählen aus mehr als 20 aktiven und passiven Techniken

bietet die notwendige Flexibilität, um vollständigen Gerätetransparenz in jedem heterogenen Netzwerk herzustellen – unabhängig von der Komplexität oder Größe dieses Netzwerks bzw. der Anzahl von Remote-Standorten. Dabei sind weder Infrastruktur-Upgrades (Software/Hardware) noch die Bereitstellung einer lokalen Appliance in jeder Niederlassung/Zweigstelle notwendig.

Keine blinden Flecken: Unternehmenskunden verfügen häufig über mehrere Remote-Standorte, an denen es nicht möglich ist, zusätzliche Appliances zu implementieren oder SPAN-Datenverkehr bereitzustellen. Durch den Einsatz mehrerer passiver und aktiver Techniken können wir Netzwerkbeschränkungen umgehen und 100 % Geräteabdeckung ohne blinde Flecken bieten.

Ausschließlich passive Erkennung, Klassifizierung und Bewertung für kritische Anwendungen im Gesundheitswesen und OT/ICS-Netzwerke: Kritische Netzwerke sind für aktive Test- und Scantechniken, die potenziell medizinische Prozesskontrollsysteme unterbrechen können, häufig ungeeignet. Die Forescout-Plattform bietet Gerätetransparenz für verschiedenste kritische Netzwerke für Gesundheitswesen- und OT-Systeme. Erreicht wird das mithilfe einer Kombination komplett passiver Techniken, beispielsweise Monitoring des SPAN-Datenverkehrs für Deep Packet Inspection für mehr als 150 IT-, Gesundheitswesen- und OT-spezifische Protokolle. Die Forescout-Lösung ist einzigartig, da sie Geräte zuverlässig identifiziert und anschließend zusätzliche aktive Bewertungsmethoden für spezifische Geräte anwenden kann, ohne eine Betriebsunterbrechung zu riskieren.

Über die Erkennung hinausgehende Einblicke für 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 Methoden erfordern genauere Betrachtung.

Intelligente automatische Klassifizierung

Für die Erstellung detaillierter Richtlinien sind vollständige Beziehungszusammenhänge für jedes Gerät unverzichtbar. Sie müssen den operativen Zweck jedes Geräts kennen, um entscheiden zu können, wie es am besten abgesichert oder verwaltet werden kann. Aufgrund der wachsenden Anzahl und Vielfalt der Geräte ist die manuelle Erfassung dieses Zusammenhangs praktisch unmöglich. Gleichzeitig gefährdet die Erstellung von Richtlinien ohne den richtigen Situationszusammenhang 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 575 unterschiedliche Betriebssystemversionen
- Mehr als 5.700 unterschiedliche Geräteanbieterprodukte und -modelle
- Geräte im Gesundheitswesen von mehr als 400 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. Als weltweit größter Crowdsourcing-Data Lake für Geräteinformationen stellt die Device Cloud eine branchenübergreifende zentrale Informationsquelle für Fingerprints sowie Verhaltens- und Risikoprofile aller individuellen Geräte in Ihrem Netzwerk dar. Dazu analysiert unsere Lösung mehr als 12 Millionen Geräte von Unternehmenskunden. Forescout Research veröffentlicht regelmäßig neue Profile, um die Effizienz, Abdeckung und Geschwindigkeit der Klassifizierung Ihres gesamten Gerätebestands zu verbessern.

Agentenlose Prüfung des Gerätezustands und automatische Korrektur

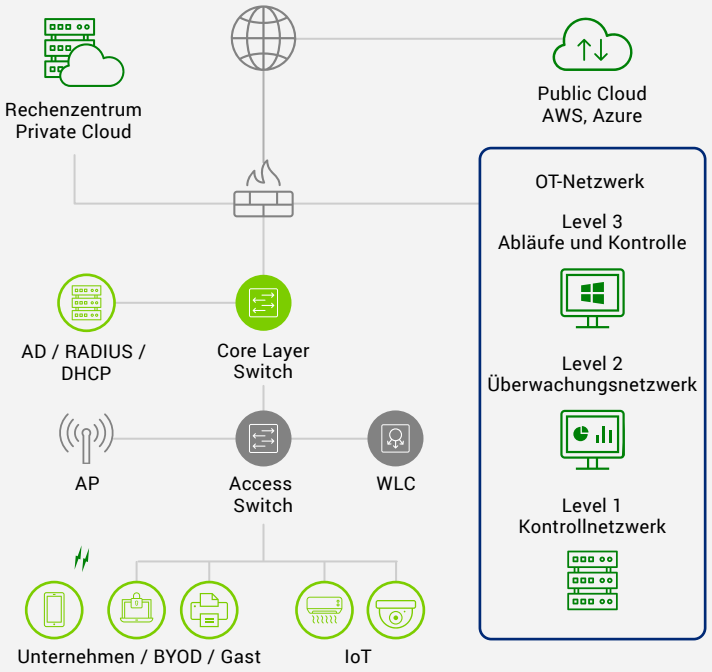
Die Geräteklassifizierung liefert betriebliche Zusammenhänge über den Zweck eines Geräts – und informiert Sie letztendlich darüber, um was für ein Gerät es sich handelt. Für vollständigen Kontext ist jedoch eine weitere Perspektive erforderlich, um den Zustand und Patch-Status jedes Geräts zu bewerten. Deshalb überwacht Forescout permanent 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 Konformitätsrichtlinien einhalten. Forescout beantwortet beispielsweise folgende wichtige Fragen:

- Laufen die Geräte mit zugelassenen Betriebssystemen einschließlich den neuesten Betriebssystem-Patches?
- Ist Sicherheitssoftware installiert, aktiv und auf dem neuesten Stand?
- 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?

Nachdem sie diese wichtigen Fragen beantwortet hat, **erzwingt die Forescout-Plattform die Konformität des Geräts mithilfe automatischer Gerätekorrektur**. Dabei kommen systemeigene oder Drittanbieter-Kontrollen zum Einsatz. Zu den wichtigsten Funktionen gehören:

- Gewährleistung der korrekten Konfiguration von Endgeräten und Durchführung von Behebungsmaßnahmen bei schwerwiegenden Konfigurationsverstößen (z. B. schwachen oder standardmäßigen Kennwörtern)
- Kontinuierliche Gewährleistung, dass die Sicherheitsagenten ordnungsgemäß funktionieren (installiert, ausgeführt und aktuell)
- 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)

Geräteklassifizierung und -bewertung



WER?
- Benutzer
- Name
- E-Mail-Adresse
- Titel
- Gruppe
- Abonnement/Konto
- IAM-Eigentümer/Rolle

WAS?
- Funktion
- Betriebssystem
- Hersteller/Modell
- IP-Adresse
- Browser-Agent
- Ports
- Virtuell/physisch
- MAC-Adresse

STATUS?
- Anwendungen
- Dienste
- Prozesse
- Versionen
- Registrierung
- Patches
- Verschlüsselung
- Virenschutz

WO?
- Switch
- Controller
- Switch Port/SSID/VLAN
- AWS/Azure
- Region
- VNet/VPC
- Purdue Level

Abbildung 4. 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.

„IoT und netzwerkfähige Gerätetechnologien haben zu neuen Kompromittierungsmöglichkeiten für Netzwerke und Unternehmen geführt. Jedes Gerät führt neue Codeblöcke und Ressourcen ein, die von Sicherheitsteams aufgespürt und als nicht vertrauenswürdige Infrastruktur behandelt werden müssen. Sicherheitsteams müssen jedes Gerät im Netzwerk permanent isolieren, absichern und kontrollieren.“ [2]

FORRESTER

8. JUNI 2020

Nutzung von Transparenz zur Gewährleistung von Kontrolle

Die Netzwerke jedes Kunden sind einzigartig und dementsprechend unterscheiden sich ihre Anforderungen und Sicherheitsrichtlinien. Daher ist eine flexible Lösung notwendig, die alle kabelgebundenen, drahtlosen und VPN-Netzwerke absichern kann. Beispielsweise setzen große Unternehmenskunden in **ihren kabelgebundenen Netzwerken häufig die Forescout-Lösung ohne 802.1X** ein. Der Grund: Sie lässt sich leicht bereitstellen, erfordert keine Hardware-/Software-Infrastruktur-Upgrades oder komplexen Switch- bzw. Endgerätekonfigurationen wie bei 802.1X und funktioniert in Netzwerkinfrastrukturen mit einem oder mehreren Anbietern. Damit folgen sie der Empfehlung von Gartner zum Verzicht auf 802.1X in kabelgebundenen Netzwerken, um die Bereitstellung zu optimieren und die Betriebskosten zu senken. In drahtlosen Netzwerken ist es jedoch üblich, 802.1X zur Authentifizierung unternehmenseigener benutzergebundener IT-Geräte zu verwenden. Dank der flexiblen und hybriden Bereitstellungsoptionen von Forescout lassen sich beide empfohlenen Vorgehensweisen verbinden.

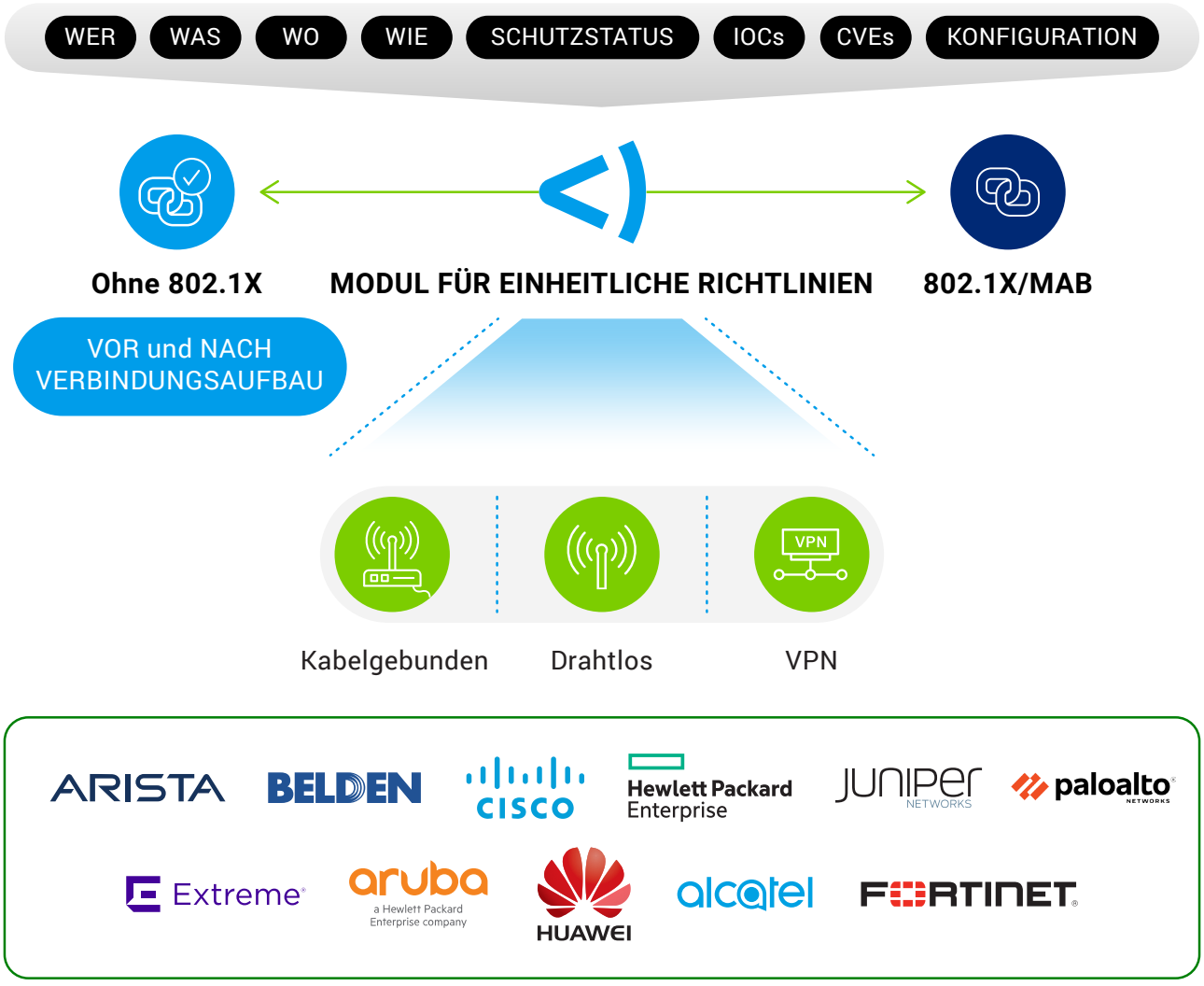


Abbildung 5. Forescout bietet Optionen mit oder ohne 802.1X zur Absicherung von Endgeräten in kabelgebundenen, drahtlosen und VPN-Netzwerken mit mehreren Anbietern.

Bei der Absicherung des Netzwerkzugriffs bietet die Forescout-Plattform folgende wichtige Vorteile:

Größere Flexibilität

- Vielfältige Methoden zur Zugriffskontrolle – mit oder ohne 802.1X
- Zuverlässige kabelgebundene Architektur ohne 802.1X – unterbrechungsfrei, leicht zu implementieren, minimale Konfigurationsanforderungen, ohne Infrastruktur-Upgrades, Optionen für vor und nach dem Verbindungsaufbau, kürzere Amortisationszeit und schnellere Rendite
- Modul für einheitliche Richtlinien zur Implementierung differenzierter (Gast, BYOD, Unternehmen, IoT) und Zero-Trust-Zugriffe

Keine Upgrades

- Funktioniert in vorhandener Infrastruktur ohne Software-/Hardware-Upgrades
- Funktioniert mit Ihren aktuellen Netzwerkinfrastruktur-Anbietern (z. B. für Switches, WLAN-Controller, IaaS) und vermeidet Anbieterbindung
- Kürzere Amortisationszeit und schnellere Rendite

Heterogen

- Direkte Integration (per SNMP, SSH, Telnet, RADIUS) mit hunderten Switches und WLAN-Controllern mit jeweils unterschiedlichen Betriebssystem-Versionen von mehr als 30 Netzwerkinfrastruktur-Anbietern, sodass die Durchsetzung von Zugangskontrollen in jedem beliebigen Netzwerk mit mehreren Anbietern möglich ist
- Flexible und unterbrechungsfreie Lösung, die die Kosten für Bereitstellung, Wartung und Betrieb senkt
- Unterstützung für heterogene Umgebungen, sodass Unternehmen nach Fusionen und Übernahmen schnell Transparenz und Kontrolle über Ressourcen erhalten

Unternehmensweite Segmentierung

- Nutzung der Erkenntnisse, die sich aus den Transparenzinformationen der Forescout-Plattform ziehen lassen, für die Echtzeit-Bewertung des Segmentierungsstatus – für jedes Gerät und an jedem Ort
- Entwicklung und Simulation logischer Segmentierungsrichtlinien, um noch vor der Durchsetzung die Auswirkungen abzuschätzen
- Monitoring des Segmentierungszustands in Echtzeit und Gegenmaßnahmen bei Richtlinienverstößen im gesamten Unternehmensnetzwerk

Weitere Informationen zur Forescout-Lösung für unternehmensweite Segmentierung erhalten Sie hier.

EMPFEHLUNGEN FÜR DIE NAC-BEREITSTELLUNG

Forescout empfiehlt diese Vorgehensweise bei der Bereitstellung von NAC:

WLAN: 802.1X ist die Standardoption zur Authentifizierung unternehmenseigener benutzergebundener IT-Geräte in WLANs. Nach der Authentifizierung identifiziert und bewertet Forescout agentenlos die Konformität von Computern mit Windows, macOS und Linux. Das Forescout-Richtlinienmodul erlaubt die automatische Behebung und Durchsetzung entsprechender Netzwerkkontrollen, um Sicherheitsrichtlinien einzuhalten (z. B. Benutzer benachrichtigen, beheben, blockieren bzw. Kontext mit Drittanbieter-Tools austauschen).

Kabelgebundenes Netzwerk: In Kabelnetzwerken empfiehlt Forescout eine Architektur ohne 802.1X. Da Bereitstellung und Verwaltung von 802.1X und MAB in Kabelnetzwerken komplex ist, wählen die meisten Kunden eine Option ohne 802.1X. Kunden mit heterogenen Netzwerken beginnen mit Geräteerkennung, Identifizierung sowie Einstufung der Sicherheits- und Konformitätslage und setzen dann die entsprechenden Netzwerkzugriffsrichtlinien mit Kontrollen ohne 802.1X durch. Hinweis: Forescout unterstützt 802.1X auch in kabelgebundenen Netzwerken.

Koordinierung mit IT- und Sicherheitsprodukten
Während des gesamten Prozesses der Netzwerkzugriffskontrolle kann Forescout mit Ihren vorhandenen Tools Echtzeit-Gerätezusammenhänge austauschen und Reaktionsabläufe automatisieren. Das beschleunigt nicht nur die Risikobehebung, sondern verbessert zudem die Rendite vorhandener Sicherheits- und IT-Verwaltungslösungen. Dank unserer standardmäßigen eyeExtend-Integrationen sowie der eyeExtend Connect-App können unsere Kunden aus ihren isolierten Sicherheitsverwaltungsprodukten schnell ein automatisiertes, unternehmensweites Reaktionssystem machen, das Ihr Enterprise of Things aktiv schützt.

Die Koordinierung mit vorhandenen Sicherheitstools während des NAC-Prozesses bietet folgende Vorteile:

Austausch der Gerätezusammenhänge

- Durch den Austausch der Gerätezusammenhänge gewährleisten Sie, dass Ihre Inventardatenbank (CMDB) stets aktuell und vollständig ist.
- Echtzeit-Bereitstellung der Kontextdaten an Sicherheitsteams und -anwendungen zum Korrelieren und Priorisieren von Zwischenfällen.

Starten von Workflows beim Verbinden

- Vorhandene Tools führen aufgrund zeitlich festgelegter Scans möglicherweise keine Schwachstelleneinstufung sich an- und abmeldender Geräte durch. Forescout integriert sich mit Sicherheitstools, um Schwachstellen-Scans nach dem Verbindungsaufbau auszulösen.
- Auslösen von Patch-Vorgängen und Sicherheits-Updates sofort nach dem Verbindungsaufbau, um die Angriffsfläche zu verringern.

Beurteilung des Sicherheitszustands

- Überprüfung der Funktion vorhandener Sicherheitsagenten und Identifizierung riskanter Geräte und Kompromittierungsindikatoren.
- Erkennung veralteter oder unzulässiger berechtigter Konten auf verbundenen Geräten.

Automatisierte Reaktionsmaßnahmen

- Eindämmung, Isolierung oder Blockierung anfälliger, kompromittierter und riskanter Geräte.
- Initiieren richtlinienbasierter Behebungsmaßnahmen zur Reaktion auf Vorfälle.

Forescout dominiert derzeit das agentenlose Segment des NAC-Marktes mit einem Anteil von 64,7 % und besitzt wohl den größten Anteil bei hybriden NAC-Bereitstellungen in der Branche. Dieses Wachstum ist in erster Linie auf den starken Funktionsumfang von Forescout zurückzuführen, der dank des agentenlosen Ansatzes den zunehmenden Anteil nicht verwalteter und nicht agentenfähiger Geräte berücksichtigt.

IDC
MAI 2020[3]

Nicht nur alles sehen, sondern alles schützen.

Die moderne Forescout-NAC-Lösung bietet einen agentenlosen, flexiblen und unterbrechungsfreien Weg zu Zero-Trust-Sicherheit. In diesen Ressourcen erfahren Sie mehr darüber, wie Forescout das Enterprise of Things aktiv schützt:

Lesen Sie den Gartner-Marktleitfaden für NAC: Hier erfahren Sie, warum Forescout von Gartner als „eine der am häufigsten eingesetzten NAC-Lösungen“ bezeichnet wird.

Besuchen Sie die Forescout-Website: Hier erfahren Sie mehr über die moderne Forescout-NAC-Lösung und lernen Anwendungsszenarien, die Gewährleistung von Gerätekonformität sowie Rückmeldungen von Forescout-Kunden kennen.

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

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

1. Forrester Research: „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 Operations), 2. Januar 2019.
2. Forrester Research: „Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles And Techniques“ (Abwehr von Ransomware mit Zero Trust: Stärkung des Schutzes mit Zero-Trust-Prinzipien und -Techniken), 8. Juni 2020.
3. IDC: „Worldwide NAC Market Shares, 2019: Diverse Market Demands Expand NAC's Addressable Market“ (Weltweite NAC-Marktanteile: Unterschiedliche Marktnachfragen erweitern NAC-Absatzmarkt), Mai 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-access-control 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