FORESCOUT

Neue Funktionen in Forescout 8.1

Im Zuge der unvermindert voranschreitenden digitalen Transformation verbinden Unternehmen immer mehr intelligente Geräte mit ihren Netzwerken, um Geschäftsprozesse zu automatisieren und die Effizienz zu steigern. Diese Geräte – egal ob IoT, IIoT oder OT – bringen beispielloses Wachstum und Vielfalt in Unternehmensnetzwerke.

Um diese geschäftliche Transformation voranzubringen, müssen Unternehmen die Konnektivität und den Informationsaustausch zwischen bislang separaten Netzwerken erhöhen. Dadurch werden die Verschmelzung von IT und OT beschleunigt sowie neue Datenflüsse zwischen mit dem Campus verbundenen IT-Geräten, Cloud-basierten Anwendungen und operativen Technologiesystemen erstellt. Trotz aller damit verbundenen Vorteile steigen auch die geschäftliche Risiken, da sich Bedrohungsakteure lateral zwischen neu vernetzten Netzwerken bewegen und auf sensible Informationen zugreifen oder betriebliche Abläufe stören können.

> "Bis 2021 werden 70 % der OT-Sicherheit direkt von der CIO-, CISO- oder CSO-Abteilung verwaltet, derzeit sind es noch 35 %."[1] – *Gartner, Mai 2018*

Die Verschmelzung von IT und OT stellt CIOs und CISOs vor neue Herausforderungen, da sie nun das gesamte geschäftliche Ökosystem schützen müssen. IT-Teams sind nicht mehr nur für die Verwaltung von Benutzergeräten, Anwendungen sowie Daten verantwortlich, sondern müssen zusätzlich sichere und optimierte Geschäftsprozesse gewährleisten. Für diese Aufgabe benötigen sie vollständige Gerätetransparenz und -kontrolle.

Forescout 8.1: Vollständige Gerätetransparenz und -kontrolle für IT- und OT-Sicherheit

Forescout 8.1 ist die erste Plattform, die auch für miteinander verschmelzende IT- und OT-Netzwerke vollständige Gerätetransparenz und -kontrolle bietet. Sie liefert Unternehmen nicht nur einen Überblick über alle Geräte in der vernetzten Umgebung, sondern ermöglicht auch die Koordination von Maßnahmen zur Reduzierung von operativen sowie Cyberrisiken. Zu den neuen Funktionen gehören:

- Ausweitung des Überblicks über industrielle Switching-Umgebungen von Cisco ACI, Microsoft Azure und Belden auf Rechenzentrums-, Cloud- sowie OT-Netzwerke, sodass Unternehmen den benötigten Überblick über IT- und OT-Domänen erhalten.
- Umfangreiche Verbesserungen bei der automatischen Klassifizierung von IoT- und OT-Geräten, der Schwachstellenbewertung für Industriesteuerungssysteme sowie der Erkennung nicht autorisierter Geräte, die die Widerstandfähigkeit von IT- und OT-Netzwerken gegen Cyberbedrohungen erhöhen.
- Koordinierung der Segmentierung mit Fortinet-Firewalls und Cisco DNA Center sowie der Reaktion auf Vorfälle mit ServiceNow. Dadurch werden die Möglichkeit zur Automatisierung von Kontrollen und die Förderung der Effizienz von Sicherheitsabläufen erweitert.
- Beispiellose Skalierung auf 2 Millionen Geräte in einer einzigen Bereitstellung, die physische, virtuelle, hybride sowie Cloud-Umgebungen umfassen kann.

Unternehmensgerechte Skalierung

Verwaltung von 2 Millionen Geräten in einer einzigen Bereitstellung, die physische, virtuelle, hybride sowie Cloud-Umgebungen umfassen kann

Geräteerkennung

Neue Transparenz industrieller Switching-Umgebungen von Microsoft Azure, Cisco ACI und Belden sowie Einblick in tiefere Schichten des OT-Netzwerk-Stacks

Automatische Klassifizierung

Neue Deep Packet Inspection von mehr als 100 IT- und OT-Protokollen mit automatischer Klassifizierung von Medizin-, Industrie-, Gebäudeautomatisierungs- und IoT-Geräten

Risikobewertung

Neue Schwachstellenbewertung für OT und Industriesteuerungssysteme sowie Erkennung nicht autorisierter Geräte zur Identifizierung und Abwehr von Identitätsdieben für mehr Widerstandfähigkeit gegen Cyberbedrohungen

Automatisierung der Kontrollen

Neue Koordinierung der Netzwerksegmentierung mit Fortinet-Firewalls und Cisco DNA Center sowie der Reaktion auf Vorfälle mit ITSM und Security Operations von ServiceNow

Erweiterte Geräteerkennung

Sicherheit beginnt damit, dass Sie die Daten in Ihrem Netzwerk zuverlässig kennen. Das bedeutet, dass alle Geräte sofort bei der Herstellung der Netzwerkverbindung identifiziert werden müssen. Für 2019 wird erwartet, dass sich weitere 900 Millionen physische und virtuelle Geräte in Unternehmensnetzwerken befinden. Den Großteil davon machen IoT- und OT-Geräte sowie Public- und Private-Cloud-Instanzen aus.

> "Bis 2023 wird der durchschnittliche CIO für mehr als 3 Mal so viele Endgeräte verantwortlich sein, als dies 2018 der Fall war."[2]
> *– Gartner, Septembre 2018*

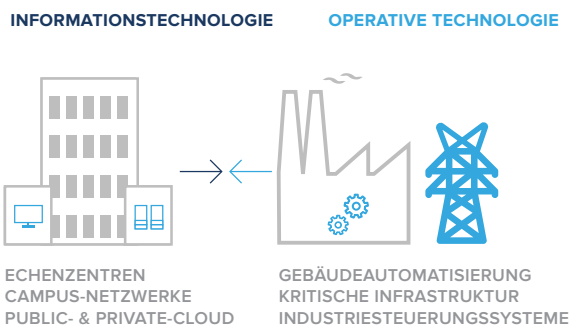
- Forescout 8.1 erweitert kontinuierlich die Transparenz dieser Bereiche, um einen einheitlichen Überblick über alle Ihre Geräte auf dem Campus, in Rechenzentren, in der Cloud und in OT-Netzwerken zu liefern.
- Die Multi-Cloud-Transparenz umfasst jetzt Microsoft Azure und dient als Ergänzung zu den bestehenden Funktionen für AWS und VMware.
- Die Integration in Cisco ACI bietet Transparenz in SDN-Umgebungen für Rechenzentren.
- Durch die Einbindung des industriellen Switching-Portfolios von Belden erhalten Sie einen erweiterten Überblick über OT-Netzwerke.
- Die passive Überwachung in tieferen Schichten des OT-Netzwerk-Stacks bietet einen Überblick über Geräte für Überwachung, Prozesskontrolle und Instrumentation.

Erstklassige automatische Klassifizierung

Durch die Vielfalt der IoT- und OT-Geräte stellt deren genaue Identifizierung und Katalogisierung für Unternehmen eine immer größere Herausforderung dar. Ohne genaue Klassifizierung ist es jedoch schwierig, gezielte Richtlinien für die Absicherung dieser Geräte zu erstellen und durchzusetzen. Forescout 8.1 enthält umfangreiche Verbesserungen, mit denen Sie eine größere Anzahl Ihrer Geräte automatisch klassifizieren und diesen Kontext dann zur Richtliniendurchsetzung mit folgenden Vorteilen nutzen können:

- Erweiterte Abdeckung zur Identifizierung von mehr als 500 Betriebssystemversionen und über 5.000 Geräteanbietern und -modellen
- Klassifizierung von medizintechnischen Geräten für mehr als 350 Medizintechnikanbieter, darunter auch Unternehmen der weltweiten Top-20-Liste
- Neue Deep Packet Inspection von mehr als 100 IT- und OT-Protokollen zur automatischen Klassifizierung industrieller Automatisierungsgeräte in Fertigungs- und Versorgungsunternehmen, im Energie-, Öl- und Gas-Sektor, im Bergbau sowie in kritischen Infrastrukturen
- Verbesserte Effizienz, Geschwindigkeit und Abdeckung bei der Klassifizierung, basierend auf der Forescout Device Cloud mit mehr als 8 Millionen IT-, IoT- und OT-Geräten

Domänenübergreifende Risikobewertung



OT-Schwachstellenbewertung

Mit der zunehmenden Konnektivität zwischen IT- und OT-Netzwerken ist es wichtig, das Risikoprofil der Geräte in beiden Domänen zu kennen. Wenn Geräte auf beiden Seiten kompromittiert werden, können sich Bedrohungen durch Domänen bewegen und Geschäftsunterbrechungen sowie finanziellen Schaden verursachen.

- Forescout 8.1 ergänzt die bestehenden Windows-Funktionen zur Schwachstellenbewertung um Schwachstellenbewertung für OT und Industriesteuerungssysteme und liefert einen Überblick über besonders gefährdete Geräte in Ihrem Netzwerk.
- Regelmäßige Updates von Forescout liefern stets aktuelle Informationen über die neuesten häufigen Schwachstellen und Risiken (CVES) für Industriesteuerungssysteme, damit gefährdete Geräte identifiziert und Korrekturmaßnahmen koordiniert werden können.
- Für gefährdete operative und Industriegeräte, die nur innerhalb geplanter Wartungsfenster gepatcht oder korrigiert werden können, kann Forescout Eindämmungskontrollen durchsetzen, z. B. diese Geräte bis zur Problembehebung in „sichere" Netzwerkzonen segmentieren.

Erkennung nicht autorisierter Geräte

Weitere Herausforderungen, die die explosionsartige Zunahme von IoT- und OT-Geräten mit sich bringen, sind der Diebstahl von Geräteidentitäten und das MAC-Adressen-Spoofing. Bedrohungsakteure, die nach Zugriffsmöglichkeiten auf Netzwerke suchen, können einen größeren Pool an MAC-Adressen angreifen, da IoT- und OT-Geräte oft in umfangreiche Whitelists für den Netzwerkzugriff aufgenommen sind. Die Anzeigebildschirme dieser Geräte sind oft ungesichert, sodass ihre MAC-Adressen für Personen sichtbar sind, die an diesen Bildschirmen vorbei gehen. Identitätsdiebe können sich auch problemlos als legitime Geräte ausgeben, um sich Zugriff auf das Netzwerk zu verschaffen und Unterbrechungen zu verursachen oder sensible Informationen zu erhalten.

Forescout 8.1 intègre une nouvelle fonctionnalité de détection des appareils non approuvés (en attente de brevet) permettant d'identifier et de bloquer les cybercriminels qui utilisent des techniques d'usurpation des adresses MAC.

- Kontinuierliche Netzwerküberwachung erkennt vielfältige Spoofing-Szenarien in kabelgebundenen und drahtlosen Netzwerken, zum Beispiel gleichzeitige Verbindungen und Ersetzungsversuche am gleichen und unterschiedlichen Standort.
- Forescout identifiziert Geräte von Opfern sowie Identitätsdieben und kann basierend auf Richtlinien Spoofing-Versuche blockieren, um böswilligen Zugriff zu verhindern.
- Forescout ermöglicht gegenüber Prüfern den Nachweis der Widerstandsfähigkeit gegen MAC-Spoofing sowie die Verbesserung der Audit-Compliance.

Koordinierung und Automatisierung von Kontrollen

IT-Sicherheitsteams werden mit einer wachsenden Zahl von Sicherheits- und Compliance-Problemen konfrontiert, die von Sicherheitstools gemeldet werden, denen entweder der entsprechende Gerätekontext zur Priorisierung von Maßnahmen oder die Automatisierungsmöglichkeiten zur Durchsetzung von Kontrollen fehlt. Dadurch verlieren hochqualifizierte Sicherheitsteams wertvolle Zeit bei der manuellen Behebung geringfügiger Probleme und können sich nicht auf proaktive Risikominimierung oder schnelle Bedrohungsreaktionen konzentrieren. Forescout 8.1 bietet Ihnen sowohl den Gerätekontext als auch die Möglichkeit, Maßnahmen zu koordinieren und Kontrollen zu automatisieren.

> "Bis 2021 werden 70 % der Unternehmen über automatisierte Sicherheitsfunktionen sowie Funktionen für Koordinierungs- und Reaktionsmaßnahmen verfügen. Dafür nutzen sie entweder ihre SIEM-Lösung oder eine dedizierte Plattform. Im Jahr 2018 waren es noch weniger 5 %."[3]
>
> *– Gartner, December 2018*

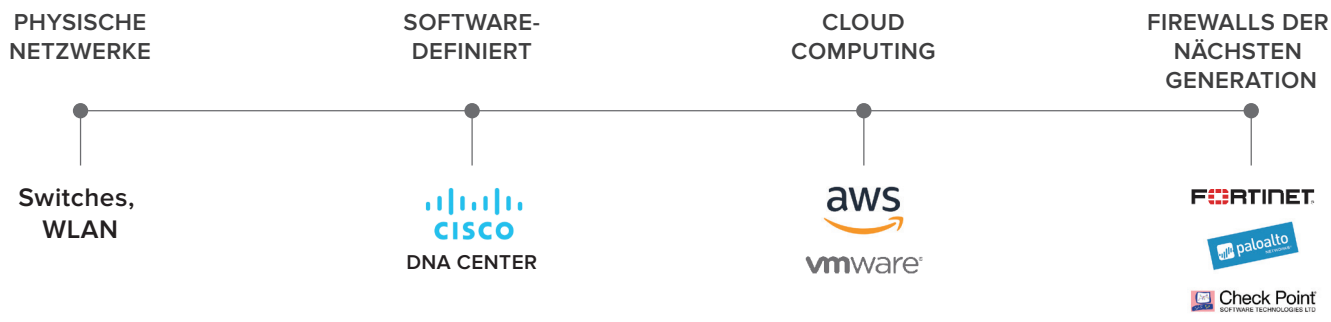
Netzwerksegmentierung

Wenn Unternehmen ihre Sicherheitsarchitekturen der nächsten Generation für IoT und OT definieren, spielt Segmentierung eine wichtige Rolle. Im Gegensatz zu herkömmlichen Geräten können IoT- und OT-Geräte nicht regelmäßig über Agenten gepatcht oder abgesichert werden. Deshalb ist die Segmentierung dieser Geräte in logische Sicherheitszonen eine unerlässliche Risikominderungsstrategie.

Mit Forescout 8.1 können Sie die Segmentierung für mehrere Durchsetzungstechnologien, einschließlich verschiedene neuer Integrationen, koordinieren:

- Automatisierung von Segmentierungskontrollen mit Fortinet-Firewalls als Ergänzung zur bestehenden Koordinierung mit Palo Alto Networks und Check Point und zur heterogenen Unterstützung von Firewalls der nächsten Generation.
- Koordinierung der Segmentierungskontrollen mit Cisco DNA Center als Ergänzung zu bestehenden Integrationen mit Software-definierten und Cloud-Netzwerktechnologien wie VMware NSX und AWS.

Domänenübergreifende Netzwerksegmentierung



Automatisierung der Reaktion auf Vorfälle

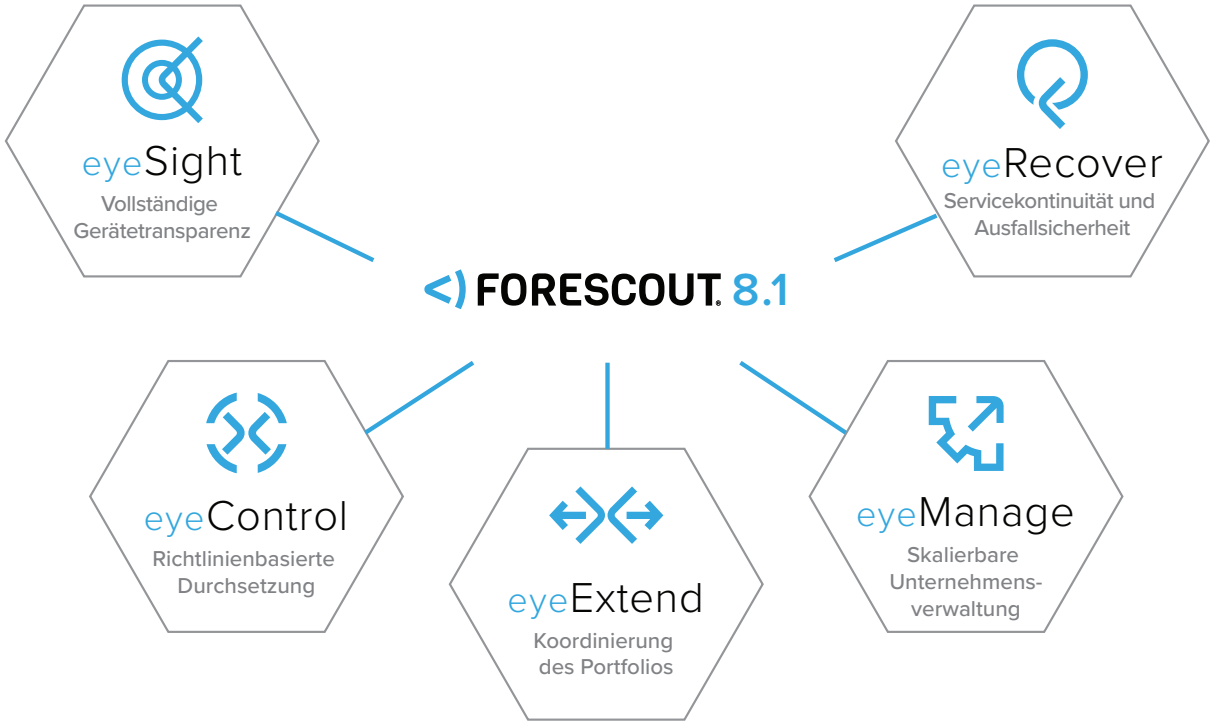
IT- und Sicherheitsteams sehen in der Automatisierung von Reaktionen zunehmend eine Möglichkeit, Probleme mit geringem Risiko zu beheben, damit sich ihre hochqualifizierten Experten auf die Risikominderung sowie andere geschäftskritische Aufgaben konzentrieren können. Forescout 8.1 lässt sich in ITSM- und Security Operations-Produkte von ServiceNow integrieren, um die Reaktion auf Vorfälle zu automatisieren und zu beschleunigen.

- Die neue Koordinierung mit ServiceNow ITSM automatisiert die Erstellung von Servicevorfällen und die richtlinienbasierte Reaktionen zur Einhaltung von Konfigurationsvorschriften.
- Die neue Koordinierung mit ServiceNow Security Operations automatisiert die Erstellung von Sicherheitsvorfällen sowie die Reaktion auf Bedrohungen für hochriskante oder kompromittierte Geräte.
- Die verbesserte Koordinierung mit ServiceNow CMDB aktualisiert Konfigurationselemente, nachdem der Vorfall vollständig behoben ist, um Services innerhalb eines geschlossenen Kreislaufs und Sicherheitsverwaltungs-Workflows zu unterstützen.

Skalierbare und flexible Plattform

Forescout 8.1 bietet beispiellose Skalierungs- und Bereitstellungsflexibilität, um die strikten Anforderungen großer Unternehmensumgebungen zu erfüllen:

- Mit einer Installation können bis zu 2 Millionen physische oder virtuelle Geräte auf dem Campus, in Rechenzentren, in der Cloud und in OT-Netzwerken verwaltet werden.
- Eine modulare Produkt-Suite bietet Flexibilität auf Basis Ihrer sich verändernden Unternehmensanforderungen. Das beginnt mit Forescout eyeSight für Gerätetransparenz, und jedes weitere Produkt bringt weitere leistungsstarke Funktionen zur Automatisierung von Kontrollen, Koordinierung von Sicherheitsmaßnahmen sowie operative Widerstandsfähigkeit und OT-Sicherheit.
- Alle Forescout-Softwareprodukte sind jetzt als Dauerlizenz sowie als zeitlich gebundenes Abonnement verfügbar.



1 "*2018 Strategic Roadmap for Integrated IT Security*" (Strategische Roadmap für integrierte IT-Sicherheit 2018), Gartner, Mai 2018
2 Gartner: "*Top Strategic IoT Trends and Technologies Through 2023*" (Wichtigste strategische IoT-Trends und -Technologien von Gartner bis 2023), September, 2018
3 Gartner: "*Emerging Technology Analysis: SOAR Solutions*" (Analyse neuer Technologien: SOAR-Lösungen) 7. Dezember 2018, Eric Ahlm

FORESCOUT

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

Gebührenfreie Rufnummer (USA):
1-866-377-8771
Telefon (International):
+1-408-213-3191
Support +1-708-237-6591

Weitere Informationen unter Forescout.com