FORESCOUT

Neue Funktionen in Forescout 8.2

„Bis 2023 wird die Gesamtanzahl verbundener IoT-Geräte weltweit auf über 35,2 Milliarden ansteigen."

– Weltweite IoT-Prognose, 2019–2023, IDC

Die Angriffe in den letzten zehn Jahren haben uns gelehrt, dass schon ein einziger Schwachpunkt in einem Netzwerk ausreicht, um ein Unternehmen für Kompromittierungen anfällig zu machen. Zur Förderung der digitalen Transformation werden immer mehr IoT-Geräte und andere nicht verwaltete Geräte mit Unternehmensnetzwerken verbunden. Angesichts dieser Tatsache ist es dringend erforderlich, Innovation mit dem nicht minder wichtigen Ziel in Einklang zu bringen, diese Geräte zu sichern und die Netzwerke zu schützen.

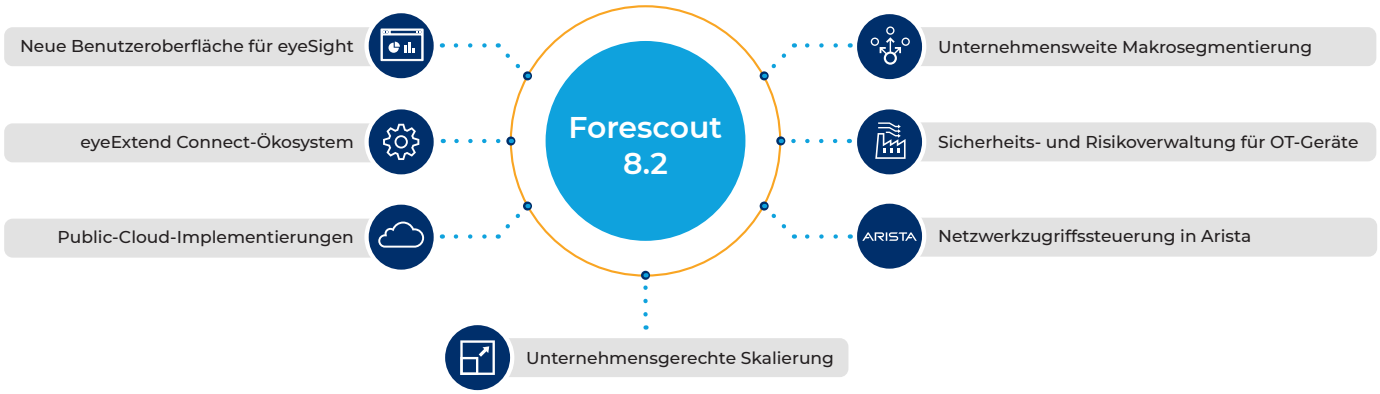
Ohne einen vollständigen Überblick über die Geräte, welche mit den verschiedenen Netzwerkdomänen verbunden sind, ist ein schnelles Handeln zur Risikominimierung praktisch nicht mehr möglich. Veraltete und anfällige Geräte, nicht konforme und falsch konfigurierte Endgeräte sowie IoT- und operative Technologien müssen ausnahmslos erkannt werden. Zudem muss eine permanente Risikoeinstufung für alle verbundenen Netzwerke und Standorte durchgeführt werden. Vollständige Transparenz ist die Grundlage, um handeln zu können – und vor allem schnell.

Forescout 8.2: Schneller erkennen und handeln

Mit Forescout 8.2 erfassen Sie alle verbundenen Geräte, Konformitätslücken und Risiken in Ihrem Netzwerk noch schneller. Sie können hierbei zuverlässig und ohne Verzögerungen Sicherheitsbedrohungen mindern und die mittlere Reaktionszeit unternehmensweit reduzieren.

Besondere Highlights:

- Neue nutzerbasierte grafische Produktoberfläche für Forescout eyeSight bietet Geräteinformationen zur Erkennung, Priorisierung und proaktiven Minderung von Risiken
- Forescout eyeExtend Connect, ein neues, Community-basiertes App-Ökosystem, mit dem Kunden und Partner einfacher Apps zur Integration mit der Forescout-Plattform entwickeln, nutzen und weitergeben können
- Neue flexible Installation und schnellere Wertschöpfung für Unternehmen, die eine Cloud-First-Strategie verfolgen und Forescout-Appliances in ihren Public-Cloud-Umgebungen von AWS und Microsoft Azure verfügbar machen möchten
- Unternehmensweite Segmentierung mit Forescout eyeSegment ermöglicht Unternehmen, Richtlinien über mehrere Netzwerkdomänen und verschiedene Regelwerkdurchsetzungspunkte sicher definieren und einhalten zu können
- Integration mit Forescout SilentDefense™ sowie integrierte IT- und OT-Sensoren in derselben Appliance für einen einheitlichen Überblick über IT- und OT-Umgebungen, einschließlich Netzwerken mit sich überschneidenden IP-Adressbereichen
- Netzwerkzugriffssteuerung durch direkte Integration der Arista-Infrastruktur – ohne Agenten oder den Einsatz von 802.1X für IT- und IoT-Geräte



Neue Benutzeroberfläche

Alle Verantwortlichen profitieren von nutzerbasierten Ansichten und verwendbaren Informationen, welche über die neue webbasierte Benutzeroberfläche bereitgestellt werden. In Dashboards werden die angeschlossenen Geräte visualisiert und Mitarbeiter über die Bereiche mit den höchsten Risikofaktoren aufmerksam gemacht. Darüber hinaus wird der Fortschritt zur Erreichung der Konformitätsziele veranschaulicht. Der Echtzeit-Gerätebestand mit umfassenden Filtermöglichkeiten bietet die schnelle Suche von Geräten. Unkomplizierte Personalisierungs- und Freigabeoptionen vereinfachen das Teilen von Risikoinformationen über verschiedene IT-Funktionen hinweg und ermöglichen somit eine schnelle Reaktion auf Bedrohungen.

Schnellerer Überblick: Die vorkonfigurierten Gerätetransparenz- und Konformitäts-Dashboards bieten folgende Möglichkeiten:

- Identifizierung der Funktion, des Betriebssystems, des Anbieters und des Modells aller verbundenen Geräte
- Festlegung eines Konformitätsschwellenwerts und Überwachen dieses Werts für alle aktiven Regeln
- Erkennung stark gefährdeter Geräte, zum Beispiel:
  - IoT-Geräte mit schwachen Anmeldeinformationen, offenen Ports oder anderen Konfigurationsfehlern
  - Windows-Geräte mit fehlenden Sicherheitsupdates oder Sicherheitslücken
  - Geräte mit fehlerhaften Sicherheitsagenten oder nicht genehmigten Anwendungen
  - OT-Geräte mit kritischen, häufig auftauchenden Schwachstellen und Risiken (CVEs)
- Identifizieren von Richtlinienverstößen (einschließlich der am häufigsten vorkommenden Fehler) sowie Geräten, die gegen mehrere Richtlinien verstoßen (z. B. weil sie ohne Firewall oder Virenschutzprogramm P2P-Anwendungen ausführen)

Proaktive Schließung von Informationslücken: Die neue webbasierte Geräteübersicht bietet folgende Möglichkeiten:

- Durchsuchung des gesamten Gerätebestands im Campus, Rechenzentrum, der Cloud und OT-Infrastruktur
- Filterung nach Richtlinie, Netzwerksegment und gewünschten Geräteeigenschaften
- Erkennung des Gerätestandorts und die Verkürzung der mittleren Reaktionszeit

eyeExtend Connect-App-Ökosystem

Kunden integrieren über die Forescout-Plattform ihre vorhandenen IT- und Cybersicherheitstechnologien, um Geräteinformationen austauschen, Arbeitsabläufe koordinieren und Abhilfemaßnahmen automatisieren zu können. Die aktuell verfügbaren Forescout eyeExtend-Module bieten vorkonfigurierte Integrationen mit über 25 führenden Produkten und damit die Möglichkeit, den Wert bereits existierender Investitionen weiter zu steigern. Neben diesen von Forescout entwickelten und unterstützten Modulen bietet Forescout 8.2 ein neues, Community-basiertes App-Ökosystem, das Integrationen mit zusätzlichen Technologien ermöglicht.

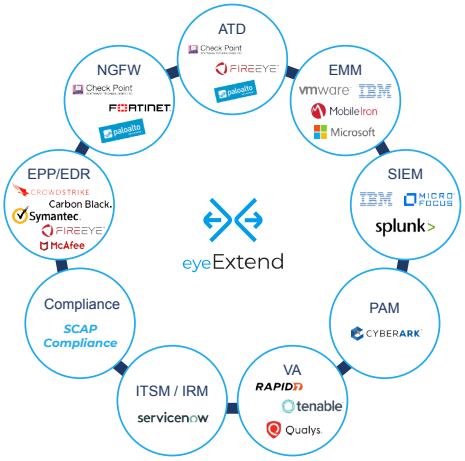
eyeExtend Connect nutzt das Crowdsourcing-Konzept, um Kunden sowie Partnern die Möglichkeit zur schnellen Entwicklung, Nutzung und Weitergabe von Apps zu geben, über die eine Verbindung zur Forescout-Plattform hergestellt werden kann. Dadurch können Sie Gerätezusammenhänge problemlos mit anderen Tools austauschen, Arbeitsabläufe automatisieren und Maßnahmen ergreifen, um systemweit reagieren zu können und so die mittlere Reaktionszeit zu verkürzen.

Einfache Entwicklung: Sie können flexible eigeneApps erstellen, welche dank universeller Python-Skripts und JSON einen schnellen Einsatz ermöglichen.

Einfache Nutzung: Sie haben die Wahl zwischen zahlreichen in der Community erstellten Apps, welche sich leicht implementieren und anpassen lassen und in Ihre gesamte Netzwerkumgebung übernommen werden können.

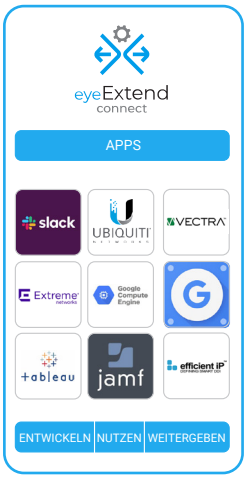
Einfache Weitergabe: Sie können aus den Anwendungsbeispielen der Community lernen und eigene Beiträge hinzufügen, Apps an Ihre Kollegen weitergeben und Crowdsourcing nutzen, um den Wert Ihrer vorhandenen IT-Investitionen weiter zu steigern.

eyeExtend-Module



Von Forescout erstellt

eyeExtend-Apps



NEU

Von der Community erstellt

Unternehmensweite Makrosegmentierung

Forescout 8.2 ergänzt eyeSegment durch die neuesten Innovationen in eyeSight und eyeControl zur unternehmensweiten Segmentierung für mehrere Netzwerkumgebungen und verschiedene Regelwerkdurchsetzungspunkte. Dank der reibungslosen Abläufe können Sie mit bestem Wissen Ihre Netzwerksegmentierung und Zero Trust-Sicherheitsstrategie konzipieren und unternehmensweit implementieren.

- Zuordnung und Visualisierung von Datenflüssen in einem logischen Schema für Benutzer, Geräte, Applikationen und Anwendungsdienste
- Entwurf, Simulation und Verfeinerung logischer Segmentierungsrichtlinien, um vor deren Aktivierung die Auswirkungen auf das Netzwerk zu verstehen
- Echtzeit-Überwachung des Segmentierungszustands und Gegenmaßnahmen bei Richtlinienverstößen
- Datenbasierte Entscheidungen zur Durchsetzung von Segmentierungskontrollen für mehrere Netzwerkumgebungen und verschiedene Regelwerkdurchsetzungspunkte

Sicherheits- und Risikoverwaltung in OT-Umgebungen

Dank der Integration zwischen SilentDefense und Forescout 8.2 können Sie vielfältige Anwendungsszenarien für die Sicherheits- und Risikoverwaltung in OT- und verschmelzenden Umgebungen abdecken.

- Weitergabe von OT-Geräteklassifikation und -schwachstellen aus SilentDefense zu eyeSight sowie Nutzung der neuen eyeSight-Benutzeroberfläche, um einen einheitlichen Überblick über IT- und OT-Netzwerke zu erhalten
- Installation von IT- und OT-Sensoren in derselben Appliance, um Geräte in verschmelzenden Umgebungen zu erkennen und zu klassifizieren

- Eindeutige Identifizierung von Geräten und Durchsetzung von Richtlinien in Netzwerkumgebungen mit identischen IP-Adressbereichen für mehrere Websites, Produktionslinien oder Betrieb
- Anwendung der neuesten Funktionen von SilentDefense in OT-Umgebungen, einschließlich erweiterter Berichterstellung zur CIP-Konformität gemäß NERC, selektiver und nicht-intrusiver, aktiver Untersuchung der Gerätetransparenz und Bewertung des Risiko-Frameworks, in dem mehrere Risikofaktoren zusammengelegt werden, um auswirkungsbasierte Bewertungen zu erhalten

Netzwerkzugriffssteuerung in Arista-Umgebungen

Forescout 8.2 integriert sich direkt mit der Arista-Infrastruktur, sodass Sie die Netzwerkzugriffssteuerungen in Arista und in heterogenen Umgebungen durchsetzen können. Das ermöglicht die Identifizierung und Kontrolle von IT- und IoT-Geräten, ohne Agenten oder den Einsatz von 802.1X.

- Identifizierung und Einstufung aller IoT- und IT-Geräte in Echtzeit, sobald diese an das Netzwerk angeschlossen werden
- Implementierung von dynamischen Netzwerkzugriffen, basierend auf Kontextinformationen von eyeSight und Drittanbietern, einschließlich Gerätetyp, Geräteeigentümer, Benutzerrolle, Konformitäts- und Sicherheitsstatus
- Risikominderung durch Automatisierung verschiedener situationsbedingter Netzwerksicherungsmaßnahmen, z. B. Rechteeinschränkung, Segmentierung, Isolierung oder Blockierung von Geräten

Public-Cloud-Implementierungen

Unternehmen, die einen Cloud-First-Technologieansatz verfolgen, konnten Gerätesichtbarkeit und -kontrolle bislang nur in lokalen physischen oder virtuellen Umgebungen umsetzen. Mit Forescout 8.2 können Sie Forescout-Appliances und die Unternehmensverwaltung in Ihren Amazon Web Services- oder Microsoft Azure-Cloud-Umgebungen implementieren, ohne dass lokale Ressourcen erforderlich sind. Darüber hinaus können Sie Public-Cloud-Implementierungen flexibel mit physischen und virtuellen Instanzen in der Private-Cloud-Infrastruktur von VMware, Hyper-V oder KVM kombinieren.

Physisch | Virtuell | Public Cloud | Hybrid
Kombination mehrerer oder aller Umgebungen

Unternehmensgerechte Skalierung

Forescout 8.2 bietet unübertroffene Skalierbarkeit, um die strikten Anforderungen großer Unternehmen zu erfüllen und mit der explosionsartig wachsenden Anzahl verbundener Geräte in Campus-, Rechenzentrum-, Cloud-, IoT- und OT-Umgebungen Schritt halten zu können.

- Klassifikation von Geräten anhand der größten Cloud-basierten Gerätedatenbank mit über 11 Millionen Unternehmensgeräten für eine genauere und schnellere Identifizierung an das Netzwerk angeschlossener IoT-, OT- und IT-Geräte
- Verwaltung von 2 Millionen Geräten in physischen, virtuellen, Hybrid- und Cloud-Umgebungen in einer einzigen Instanz

FORESCOUT

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

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

Weitere Informationen unter Forescout.de