Forescout eyeExtend Connect

Einfache Integration mit der Forescout-Plattform für datenbasierende Geräte- und Benutzerinformationen sowie schnellere unternehmensübergreifende Koordination von Behebungsmaßnahmen

Um den Wert ihrer Investitionen in Sicherheits- und IT-Technologien zu steigern, nutzen Forescout-Kunden vorkonfigurierte Produktintegrationen in neun bevorzugten Kategorien für Sicherheitstechnologien. Dank dieser Integrationen können Sicherheitsprozesse koordiniert und dadurch die Effizienz Ihrer Arbeitsabläufe deutlich gesteigert werden. Zusätzlich zu vorkonfigurierten Integrationen bietet Forescout eine schnellere und einfachere Möglichkeit für Kunden, weitere vorhandene Technologien mit der Forescout-Plattform zu vernetzen. Dank eyeExtend Connect können unsere Kunden und unsere Partner eyeExtend-Apps, die die Forescout-Plattform mit anderen Technologien verknüpfen, schnell entwickeln, nutzen und teilen. Dadurch kann die Community die Vorteile vorhandener Sicherheitsprodukte mit detaillierten Informationen zu Gerätezusammenhängen von Forescout kombinieren, Sicherheitsprozesse sowie die Richtliniendurchsetzung produktübergreifend automatisieren und Behebungsmaßnahmen unternehmensweit schneller erfassen.

Die Lösung

Forescout eyeExtend Connect vereinfacht die Erstellung von Apps, die sich einfach installieren und nutzen lassen. Mit den Forescout eyeExtend-Apps können Sie die Forescout-Plattform jetzt problemlos mit Ihren IT- und Sicherheitstechnologien integrieren und die Sicherheitsprozesse über verschiedenste Cybersicherheitstechnologien hinweg koordinieren.

Durch eyeExtend Connect haben Ihre aktuellen Sicherheitstechnologien die Möglichkeit, detaillierte Daten zu Gerätezusammenhängen aus Forescout eyeSight zu nutzen, einschließlich Geräteeigenschaften, Sicherheitslage, Konformität des Geräts mit Unternehmensrichtlinien, Standort innerhalb des Netzwerks, Benutzerinformationen und vieles mehr. Andere IT- oder Sicherheitsprodukte können diese Gerätedaten automatisch abrufen oder eigene Daten an die Forescout-Plattform übertragen. Zudem lassen sich mit eyeExtend Connect systemweite, richtlinienbasierte Behebungsmaßnahmen bezüglich Bedrohungen, Vorfällen und Konformitätslücken automatisieren und so die Reaktion auf Bedrohungen beschleunigen.

eyeExtend Connect umfasst die folgenden Tools zum Koordinieren von Arbeitsabläufen und Austauschen von Gerätedaten mit anderen Produkten.

eyeExtend connect

Herausforderungen

- Firmeninterne Sicherheitslösungen und Arbeitsabläufe können nicht durch vorkonfigurierte Produktintegrationen von Forescout oder Herstellerpartnern koordiniert werden.
- Die lange Entwicklungdauer für individuell angefertigte Integrationen verzögern die Wertschöpfung für bestehende Sicherheitsinvestitionen.
- Alleinstehende Sicherheits-Tools, ohne die Möglichkeit des Austauschs von Geräte- und Benutzerdaten erfordern erheblichen manuellen Aufwand bei der Behebung von Sicherheitsvorfällen und erhöhen somit das Angriffsrisiko und den Produktivitätsverlust.

Vorteile

- Erhöhen Sie die Wertschöpfung Ihrer bestehenden Investitionen durch Integration mit beliebigen Drittanbieter-Tools
- Schnellerer Einsatz durch einfache Einbindung mit der Forescout-Plattform über die eyeExtend-Apps
- Verbesserung Ihrer Sicherheit, da Ihre IT- und Sicherheits-Tools besser zusammenarbeiten, schneller verwertbare Erkenntnisse zu Geräten liefern und die Behebung von Risiken und Bedrohungen automatisieren

Highlights

- Einfache Entwicklung und Installation von eyeExtend-Apps zur Integration mit der Forescout-Plattform
- Teilen Sie Ihre Apps mit der Community, um Feedback zu erhalten und beteiligen Sie sich an den Unterhaltungen
- Entwicklung migrierbarer Apps mit Python-Skripts und JSON-Konfiguration
- Integration mit verschiedensten Drittanbieter-Webdiensten
- Erweiterung der Transparenz- und Steuerungsfunktionalität der Forescout-Plattform durch den Austausch von Gerätedaten und Kontrollfunktionen von Drittanbietern
- Unterstützung bidirektionaler Integrationen über offene standardbasierte REST-APIs
- Push & Pull-Informationsaustausch per Standard-SQL (Structured Query Language)
- Erstellung benutzerdefinierter Abfragen für Push & Pull-Informationsaustausch mit Standard-LDAP-Server
- Versand und Empfang von Informationen über Syslog an einen zweckgebundenen Server

eyeExtend Apps

Entwickeln Sie Apps, die mit Hilfe wichtiger Funktionen der Forescout-Plattform Endgeräteinformationen abrufen und weiterleiten, Netzwerkkontrollmaßnahmen anstoßen und systemweite Richtlinien durchsetzen. eyeExtend Connect bietet eine benutzerfreundliche JSON-Schnittstelle zum Definieren von Parametern, Tags und von Benutzern gesteuerten Konfigurationen. Dadurch werden Ihre eyeExtend-Apps portabel (für Migrationen von Test- zu Produktionsumgebungen, von Region A zu Region B, von IT- zu OT-Umgebungen usw.). Interaktionen mit Drittanbieter-APIs werden mit Python-Skripten definiert, was die flexible Erstellung vieler weiterer Integrationen ermöglicht. Wichtige Anwendungsszenarien und Durchsetzungsmaßnahmen wie Bedrohungseindämmung, Reaktion auf Vorfälle und Konformitätsverwaltung lassen sich über Richtlinienvorlagen, die in die Apps integriert werden können, automatisieren.

Wichtige Funktionen der eyeExtend-Apps:

- Plug-and-Play
- Erkennung neuer Geräte und deren Objekte
- Kontrollaktionen gemeinsam mit Drittanbieter-Produkten
- Anpassbare Regelwerksvorlagen
- Skriptbasierte Aktionen via API
- Anpassbare Drittanbieter-Produkticons

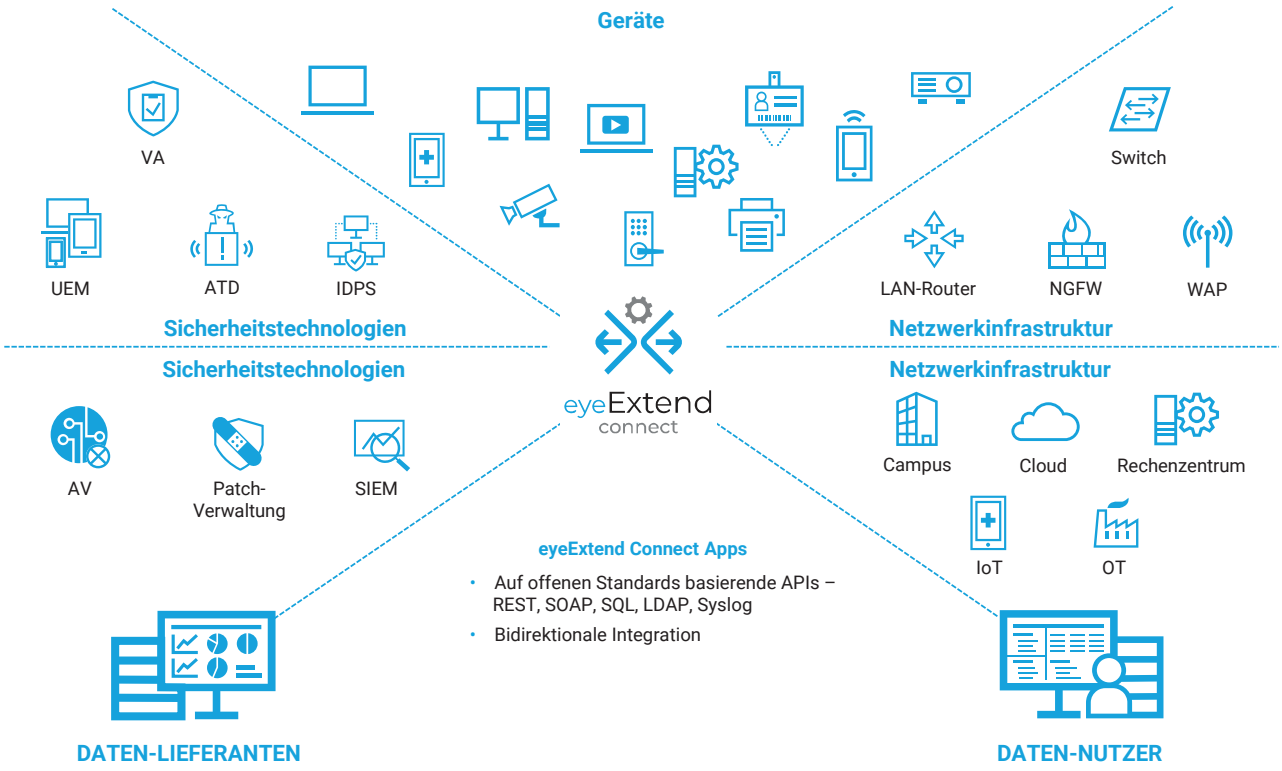
Web-API & Data Exchange (DEX)
Die Forescout-Plattform bietet eine Reihe von REST-APIs, über die externe Anwendungen von Forescout Informationen zu Geräteeigenschaften und Richtlinien abrufen können. Das DEX-Plug-In (Data Exchange) ermöglicht die bidirektionale Kommunikation zwischen der Forescout-Plattform und externen REST-APIs und damit den Austausch von Echtzeit-Geräteinformationen.

SQL
Das DEX-Plug-In ermöglicht den Push & Pull-Informationsaustausch mit einer Standard-SQL-Datenbank. Dank dieser Integration können unternehmenseigene Anwendungen Informationen mit Drittanbieter-Produkten austauschen, sofern diese über eine Schnittstelle zu einer externen oder internen Datenbank verfügen. Sie haben die Möglichkeit, bei externen Datenbanken Informationen abzufragen und Geräteeigenschaften zu erstellen, um die von der Forescout-Plattform erfassten Daten zu speichern. Diese Geräteeigenschaften lassen sich im Forescout-Regelwerk verwenden und in Netzwerksystemstatus- und Bestandsansichten anzeigen. Die von der Forescout-Plattform erfassten Informationen können auch zum Aktualisieren externer Datenbanken verwendet werden, damit ein Drittanbieter-Produkt diese als Grundlage für Aktivitäten nutzen kann.

LDAP
Generieren Sie mit dem DEX-Plug-In benutzerdefinierte Abfragen, um Informationen per Push & Pull mit einem Standard-LDAP-Server auszutauschen. Sie können zum Beispiel LDAP-Server-Informationen abfragen und diese erfassten Daten in den Forescout-Geräteeigenschaften speichern. Diese Geräteeigenschaften lassen sich in Forescout-Regelwerk verwenden und in Netzwerksystemstatus- und Bestandsansichten anzeigen.

Syslog
Das DEX-Plug-In kann so konfiguriert werden, dass Informationen über Syslog an einen definierten Server gesendet und empfangen werden. Diese Art von Schnittstelle wird für verschiedenste Produktintegrationen verwendet, welche diese Protokolle aggregieren und Protokollanalysen unterstützen, z. B. SIEM-Produkte (Sicherheitsinformations- und Ereignis-Management). Diese Schnittstelle ist auch für Lösungen geeignet, welche auf diese Weise Warnmeldungen senden und empfangen. Das Nachrichtenformat ist anpassbar.

Abbildung 1. Koordinierung der Arbeitsabläufe über Geräte, Umgebungen und Sicherheitstechnologien hinweg



VA: Schwachstelleneinstufung, **ATD:** Intelligente Bedrohungserkennung, **IDPS:** Netzwerk-Eindringungsschutz, **UEM:** Einheitliche Endgeräteverwaltung, **AV:** Virenschutz, **SIEM:** Sicherheitsinformations- und Ereignis-Management, **WLAN:** drahtloser Zugriffspunkt, **NGFW:** Firewall der nächsten Generation

Allgemeine Anwendungsszenarien

Forescout bietet bereits 25 vorkonfigurierte Lösungen für spezifische Anwendungsszenarien. Die eyeExtend Apps sind dagegen für kundenspezifische, individuelle Anwendungsszenarien gedacht. Dies sind einige Beispiele:

Erkennung, Klassifizierung und Einstufung aller mit dem Netzwerk verbundenen Geräte, sobald diese an das Netzwerk angeschlossen werden
Forescout eyeExtend Connect, auf Basis von Forescout eyeSight, ermöglicht die Integration von IT- und Sicherheitsprodukten, damit Sie Informationen erhalten, mit denen Sie Geräte im gesamten Unternehmensnetzwerk besser identifizieren können, einschließlich Campus, Rechenzentrum, OT- und Cloud-Umgebungen. So verbessert zum Beispiel die eyeExtend-App für Ubiquiti den Überblick über die per WLAN verbundenen Geräte. Mithilfe der erkannten Geräteattribute sind in der Forescout-Plattform bessere richtlinienbasierte Aktionen möglich. Die eyeExtend-App für Ubiquiti kann die Ubiquiti-Informationen die per WLAN-verbundenen Geräte an andere IT-Verwaltungsdienste und Geräteverwaltungsanwendungen übertragen sowie deren Gerätedatenbank aktualisieren. Eine weitere wichtige App, die eyeExtend-App für Google Cloud, unterstützt Kunden dabei, einen Echtzeit-Überblick über neue Cloud-Instanzen zu erhalten. Dazu integriert sich die App mit Google Cloud und ruft den Google Cloud-Bestandskontext ab.

Verbesserung der Transparenz und Kontrolle über Geräte, die per VPN auf das Netzwerk zugreifen
eyeExtend Connect identifiziert alle Geräte, die über VPN auf das Unternehmensnetzwerk zugreifen. Dank der Integration mit der Forescout-Plattform können die Sicherheitsverantwortlichen bestimmen, ob es sich um ein firmeneigenes Gerät handelt und den Gerätezugriff von nicht genehmigten Standorten entsprechend steuern.

Koordinierung der Arbeitsabläufe bei Verletzungen von Sicherheits- und IT-Richtlinien
Sie können über verschiedene Zusammenarbeits- und Messaging-Plattformen Echtzeit-Warnmeldungen zu Richtlinienverletzungen senden. Dazu richten Sie eine Regel ein, welche die Gerätedaten bei einem Verstoß per E-Mail, Messaging- oder Zusammenarbeitsplattform von der Forescout-Plattform abruft. Auf dieser Grundlage können Sie Netzwerkkontrollmaßnahmen in Form von Richtlinien automatisieren. So integriert sich die eyeExtend-App für Slack zum Beispiel mit der Zusammenarbeitsplattform, um Echtzeit-Warnmeldungen zu Richtlinienverletzungen an einen Kanal zu senden, der vom IT- oder Sicherheitsteam in Slack verwendet wird.

Automatisierte Mobilgeräteregistrierung, Verbesserung der Sicherheitsverwaltung und Gewährleistung permanenter Konformität
eyeExtend Connect koordiniert Maßnahmen zum Austausch von Geräteinformationen und zur Gerätekontrolle mit UEM-Systemen, um die einheitliche Sicherheitsrichtlinienverwaltung für alle Geräte in Ihrem Netzwerk zu ermöglichen – unabhängig vom Typ (PC, Mac, Linux®, Tablet, Smartphone), der Verbindung (LAN, WLAN, VPN) oder Eigentümer des Geräts (unternehmenseigen oder privat). Diese umfassende Geräteverwaltung ermöglicht die Automatisierung der Geräteregistrierung, die Gewährleistung der Gerätekonformität mit Hilfe richtlinienbasierter Maßnahmen, die Anwendung benutzerdefinierter Netzwerkzugriffssteuerung sowie schnellere Reaktionen und Behebungsmaßnahmen. Mit der eyeExtend-App für Google Mobile Management haben Kunden jetzt zum Beispiel einen Überblick über Chromebook-Gerätedaten. Diese Informationen vereinfachen die Optimierung der BYOD-Sicherheits- und Zugriffsrichtlinien für das Unternehmen.

Automatisierung von Maßnahmen und Arbeitsabläufen innerhalb des IT- und Sicherheitsproduktpalette zur Optimierung von Prozessen und Verbesserung unternehmensweiter Sicherheit
eyeExtend Connect kann Aktionstrigger senden und empfangen, die auf der Forescout-Plattform oder einem anderen integrierten Produkt eine bestimmte Aktion auslösen. Diese Trigger basieren auf richtliniengestützter Automatisierung und nicht auf einer Instruktions-basierten Entscheidung, die einen manuellen Eingriff erfordert. Das beschleunigt die Abhilfemaßnahmen und stärkt die Sicherheit des Netzwerks im gesamten Unternehmen.

Nutzung detaillierter, kontextbezogener Geräteinformationen für Korrelationsanalysen zur schnelleren Ergreifung von Gegenmaßnahmen
Mit eyeExtend Connect kann die Forescout-Plattform detaillierte Daten zur Korrelationsanalyse an ein SIEM-System senden. Dadurch erhalten Sie ein vollständiges Bild der gesamten Angriffsfläche des Unternehmens, sodass die Informationssammlung und -prüfung beschleunigt und vereinfacht wird. Die Forescout-Plattform optimiert zudem Sicherheitsabläufe, da richtlinienbasierte Maßnahmen automatisiert werden. Auf diese Weise wird der Zugriff von Geräten auf das Netzwerk in Echtzeit, basierend auf den Vorfalldaten aus dem SIEM, begrenzt.

Fazit: Mit eyeExtend Connect können Sie Ihre Sicherheitstechnologien effektiver nutzen, da die Produkte nicht mehr separat agieren und mit der hochintelligenten Forescout-Plattform vernetzt werden. Zudem wird die Automatisierung der Schritte zur Bedrohungseindämmung und Richtlinieneinhaltung stark vereinfacht.

Hinweis: Einige Funktionen von eyeExtend Connect waren bisher Teil des OIM-Produkts. Alle bisherigen OIM-Funktionen sind jetzt in eyeExtend Connect enthalten.

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 Forescout.de