FORESCOUT
Active Defense for the Enterprise of Things™

eyeControl

Durchsetzung richtlinienbasierter Kontrollen

UNTERBRECHUNGSFREI

Flexible Optionen für Bereitstellung und Zugriffskontrollen – mit oder ohne 802.1X

AGENTENLOS

Einstufung des Gerätezustands und automatische Konformitätsdurchsetzung ohne Agenten

EFFEKTIV

Modul für einheitliche Richtlinien zur Implementierung eines sicheren Zero-Trust-Zugriffs

KEINE UPGRADES ERFORDERLICH

Verwendung in vorhandener Infrastruktur ohne Software- oder Hardware-Upgrades möglich

GERINGERE GESAMTBETRIEBS-KOSTEN

Flexibler, ununterbrochener, agentenloser und anbieterübergreifender Support – niedrigere Kosten für Bereitstellung, Wartung sowie Betrieb und damit schnellere Rendite

Durchsetzung und Automatisierung von Kontrollmaßnahmen für Enterprise of Things-Geräte in heterogenen Netzwerken

Forescout eyeControl bietet die flexibelste reibungslose Netzwerkzugriffssteuerung für heterogene Unternehmensnetzwerke. Dabei setzt die Lösung für alle verwalteten und unverwalteten Geräte im Enterprise of Things (EoT) Zero-Trust-Richtlinien für den Least-Privilege-Zugriff durch und automatisiert diese. Darüber hinaus können richtlinienbasierte Kontrollen angewendet werden, um Gerätekonformität durchsetzen, Ihre Angriffsfläche proaktiv verkleinern und schnell auf Zwischenfälle reagieren zu können.

SICHERHEIT BEIM NETZWERKZUGRIFF

Durchsetzung des Netzwerkzugriffs basierend auf Benutzer- und Geräteidentität sowie Sicherheitslage

Bereitstellung mit oder ohne 802.1X in heterogenen Netzwerken

DURCHSETZUNG DER GERÄTEKONFORMITÄT

Konformität mit Sicherheitsrichtlinien, Standards und Vorschriften

Durchführung von Korrekturmaßnahmen und Workflows zur Risikominderung

AUTOMATISIERUNG DER REAKTION AUF VORFÄLLE

Automatisierte Reaktionen auf Sicherheitsvorfälle

Eindämmung von Bedrohungen zur Minimierung ihrer Ausbreitung und dadurch entstehender Unterbrechungen

ZUVERLÄSSIGE AUTOMATISIERUNG VON KONTROLLEN

Zero-Trust-Richtlinien können nur durchgesetzt werden, wenn sie auf vollständigem Gerätekontext basieren. Dazu gehören Echtzeitinformationen über Benutzer- und Geräteidentität, Sicherheitslage sowie Risikoprofil aller verbundenen Geräte. Kontrollen, die ohne vollständige Informationen implementiert werden, können zu Unterbrechungen führen und die betrieblichen Abläufe beeinträchtigen. Deshalb nutzt eyeControl die umfangreichen Gerätezusammenhänge von eyeSight, um Zero-Trust-Kontrollen zuverlässig durchzusetzen und zu automatisieren.

Den Kern von eyeControl bildet ein intuitives und flexibles Richtlinienmodul, das Ihnen die Nutzung detaillierter und gezielter Kontrollmaßnahmen ermöglicht. Dieses Modul für Zero-Trust-Richtlinien umfasst folgende Funktionen:

- Dynamische Gerätegruppierung und Umfangermittlung basierend auf Geschäftslogik und Gerätezusammenhängen
- Komplexe Bedingungen und Maßnahmen mit Boolescher Logik und Kaskadenrichtlinien, um komplexe Kontroll-Workflows zu implementieren
- Policy Graph-Funktion für die Erstellung genauer Richtlinien, die Analyse von Richtlinienflüssen sowie die Optimierung von Richtlinien vor der Aktivierung von Durchsetzungsmaßnahmen
- Möglichkeit zur anfänglichen Nutzung manuell initiierter Kontrollmaßnahmen und langsamen Einführung der Automatisierung, um die Effizienz der Sicherheitsmaßnahmen zu steigern

Die Richtlinien werden in Echtzeit von Ereignissen und Änderungen, die entweder auf einem spezifischen Gerät oder im Netzwerk erfolgen, ausgelöst und automatisch bewertet. Die nachfolgende Abbildung 1 zeigt die Bandbreite an Kontrollmaßnahmen, die in eyeControl möglich sind, wenn eine Richtlinie ausgelöst wird.

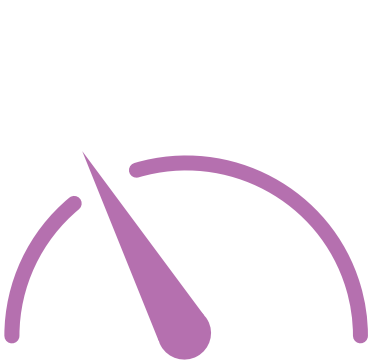

Abbildung 1. Durchsetzung von Richtlinien im Netzwerk und auf Endgeräten, sodass der Automatisierungsgrad im Laufe der Zeit zunimmt.

KONTROLLIEREN

Sicherheit beim Netzwerkzugriff

eyeControl bietet die flexibelste heterogene und unterbrechungsfreie Netzwerkzugriffssteuerungs-Lösung für Unternehmen. Mit eyeControl können Sie nicht nur den sicheren Zugriff aller verwalteten und unverwalteten EoT-Systeme auf kabelgebundenen und drahtlosen Netzwerken durchsetzen, sondern auch Audit-Anforderungen erfüllen, Ihre Angriffsfläche reduzieren und Bedrohungen schnell beheben. Zu den Funktionen gehören:

- Implementierung von Zero-Trust-Netzwerkzugriff für Geräte von Mitarbeitern, Gästen oder Auftragnehmern sowie für BYOD-Geräte
- Identifizierung und Blockierung nicht autorisierter, unberechtigter Schatten-IT-Geräte und Geräte für Spoofing-Versuche
- Quarantäne oder Isolierung nicht konformer und stark gefährdeter Geräte bis zur Problembehebung
- Nutzung vielfältiger Methoden zur Zugriffskontrolle – mit oder ohne 802.1X-Authentifizierung
- Implementierung einer agentenlosen Prüfung des Gerätezustands und Durchsetzung von Maßnahmen im Netzwerk und auf Endgeräten mit einem Modul für einheitliche Zero-Trust-Richtlinien
- Interoperabilität mit vorhandener Infrastruktur ohne Software-/Hardware-Upgrades
- Direkte Integration mit mehr als 30 Netzwerkinfrastruktur-Anbietern für hunderte Produktmodelle

EINHALTEN

Durchsetzung der Gerätekonformität

Automatisieren Sie die Bewertung der Sicherheitslage und setzen Sie Behebungsmaßnahmen durch, um die kontinuierliche Einhaltung interner Sicherheitsrichtlinien, externer Standards und branchenspezifischer Vorschriften zu gewährleisten.

- Validierung der korrekten Konfiguration von Endgeräten und Durchführung von Behebungsmaßnahmen bei schwerwiegenden Konfigurationsverstößen

eyeControl BIETET LÖSUNGEN FÜR:

Nicht autorisierte, unberechtigte oder Spoofing-Geräte im Netzwerk, die ein Risiko und Konformitätsproblem darstellen

Sicherheitslücken, wenn agentenbasierte Tools nicht auf dem neuesten Stand sind oder nicht richtig funktionieren

Einfache, kaum segmentierte Netzwerke, die die Gefahr durch Bedrohungen für das Unternehmen und den Wirkungsradius von Angriffen erhöhen

Risiken für geschäftliche Abläufe, die durch anfällige Geräte, auf denen kritische Patches fehlen, und unberechtigte Anwendungen entstehen

Ausbreitung von Bedrohungen innerhalb des Netzwerks, wenn kompromittierte oder böswillige Geräte nicht schnell eingedämmt werden können

Konformitätsverstöße, wenn der Gerätezustand verbundener Geräte nicht permanent überwacht und durchgesetzt werden kann

Herausforderungen bei der NAC-Implementierung in heterogenen Umgebungen mit mehreren Anbietern und kabelgebundenen Netzwerken

forescout.com/platform/eyeControl info-dach@forescout.com Telefon (weltweit): +1-408-213-3191

- Erkennung und Deaktivierung unberechtigter Anwendungen, die zu Risiken führen bzw. Netzwerkbandbreite oder Produktivität beeinträchtigen
- Erkennung von Geräten mit gefährlichen Schwachstellen und fehlenden kritischen Patches sowie Durchführung von Korrekturmaßnahmen
- Agentenlose Durchsetzung von Risikobehebungs- und Korrekturmaßnahmen auf Windows-, Mac-, Linux-, IoT- und OT-Geräten
- Implementierung von Richtlinien und Automatisierung von Kontrollen zur Einhaltung von Konfigurationsvorschriften in Cloud-Bereitstellungen (z. B. AWS, Azure und VMware)

AUTOMATISIEREN

Schnellere Reaktion auf Zwischenfälle

- Schnelle sowie effektive Eindämmung von Bedrohungen und Reaktion auf Zwischenfälle, um Unterbrechungen der Geschäftsabläufe sowie Auswirkungen auf das Unternehmen zu minimieren. Automatisierung grundlegender und wiederholter Aufgaben zur Reaktion auf Zwischenfälle, damit hochqualifizierte Mitarbeiter sich auf schwerwiegendere Probleme und Prioritäten konzentrieren können
- Erkennung von Kompromittierungsindikatoren und Risiken auf Geräten beim Herstellen der Verbindung, um die mittlere 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 Geräten
- Verkürzung der mittleren Reaktionszeit durch Bereitstellung wertvoller Gerätezusammenhänge (Geräteverbindung, Standort, Klassifizierung und Sicherheitsstatus) für funktionsübergreifende Vorfallreaktionsteams und isolierte Technologien

Nicht nur alles sehen, sondern alles schützen.

Kontaktieren Sie uns noch heute, damit Sie Ihr Enterprise of Things aktiv verteidigen können.

forescout.com/platform/eyeControl 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