Forescout eyeControl

Durchsetzung und Automatisierung richtlinienbasierter Kontrollen, um proaktiv die Angriffsfläche zu verringern und schnell auf Zwischenfälle reagieren zu können

IT-Sicherheitsteams werden mit einer wachsenden Zahl von Sicherheits- und Compliance-Problemen konfrontiert, die von einer Vielzahl an Sicherheitstools gemeldet werden, ohne dass diese eine Möglichkeit für Gegenmaßnahmen bieten. Leider fehlt diesen Tools entweder der entsprechende Gerätekontext zur Priorisierung von Maßnahmen oder die Automatisierungsmöglichkeiten, um Kontrollen zur Risikobehebung zu durchzusetzen. Dadurch verlieren hochqualifizierte Sicherheitsteams wertvolle Zeit bei der manuellen Behebung geringfügiger Probleme und können sich nicht auf proaktive Risikominimierung oder schnelle Bedrohungsreaktionen konzentrieren.

Durchsetzung richtlinienbasierter Kontrollen

Forescout eyeControl nutzt umfangreichen Gerätekontext von Forescout eyeSight und bietet Sicherheitsteams die Möglichkeit, richtlinienbasierte Kontrollen zuverlässig zu priorisieren, durchzusetzen und zu automatisieren. Dadurch können Unternehmen die Sicherheitsmaßnahmen verbessern, ihre Angriffsfläche verringern und die Reaktions- sowie Behebungsmaßnahmen beschleunigen, um Bedrohungen, Sicherheitsvorfälle und Compliance-Lücken umgehend zu beseitigen.

Abhängig von Ihren Sicherheitsinitiativen können Sie mit eyeControl die Aktionen sowohl im Netzwerk als auch auf Endgeräten durchsetzen. Zum Koordinieren von Netzwerkaktionen integriert sich eyeControl direkt in heterogene physische und virtuelle Netzwerkinfrastrukturen – Switches, VPN, Software-definierte und Cloud-basierte Netzwerke sowie Drahtlosnetze. Endgeräteaktionen können auf Windows-, Mac- und Linux-Endgeräten agentenlos oder über SecureConnector™ durchgesetzt werden.

eyeControl

Kernpunkte

- Schutz sensibler Daten vor externen Bedrohungen
- Verhinderung der Malware-Verbreitung durch infizierte, anfällige oder nicht konforme Geräte
- Verhinderung von Datendiebstahl und Netzwerkausfällen durch gezielte Angriffe
- Gewährleistung von Netzwerkzugriff und -verfügbarkeit für Mitarbeiter, Auftragnehmer und Kunden
- Durchsetzung der Compliance mit internen Richtlinien und externen Vorschriften
- Automatisierung von Kontrollmaßnahmen zur Anwendung der richtigen Maßnahme(n) in jeder Situation

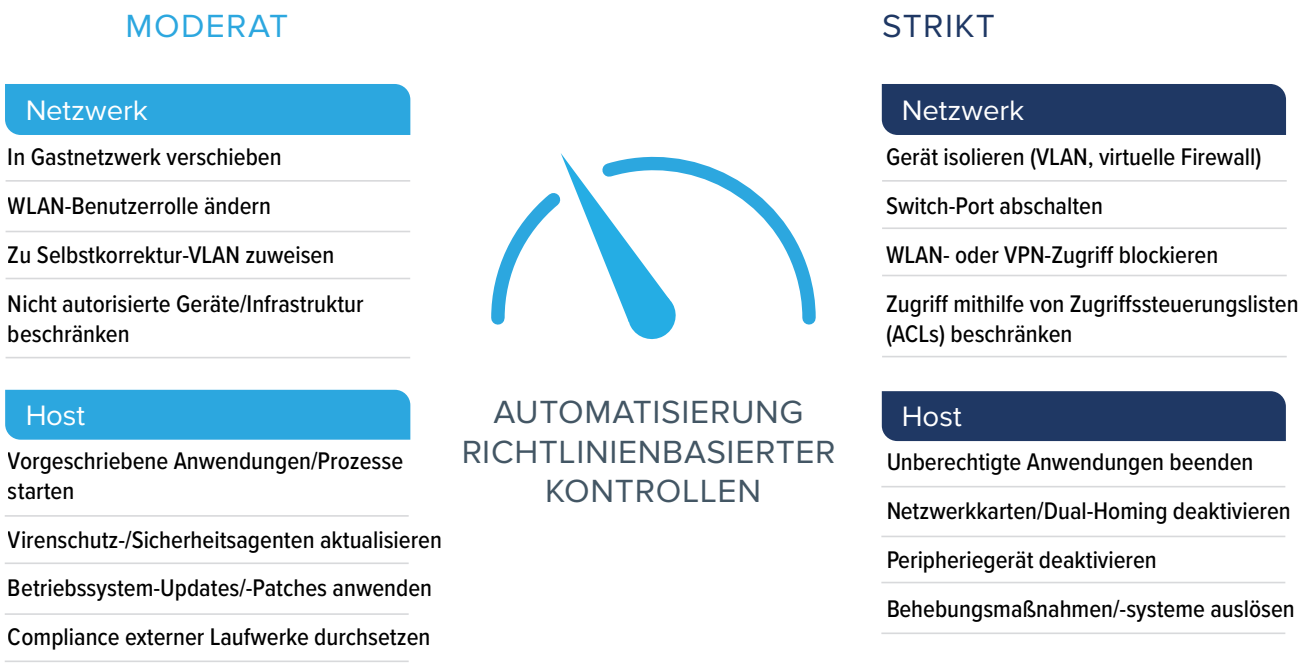

Abbildung 1. Durchsetzung von Richtlinien im Netzwerk und auf Endgeräten, sodass der Automatisierungsgrad im Laufe der Zeit zunimmt.

Zuverlässige Automatisierung von Kontrollen

eyeControl nutzt ein intuitives und flexibles Richtlinienmodul, das Unternehmen die Nutzung detaillierter und gezielter Kontrollen ermöglicht. Durch die Implementierung hochentwickelter Workflows und komplexer Maßnahmen sind einfach durchführbare dynamische Umfangermittlung, boolesche Logik und Kaskadenrichtlinien möglich. Die Policy Graph-Funktion erlaubt die Erstellung genauer Richtlinien, die Analyse von Richtlinienflüssen sowie die Optimierung von Richtlinien vor der Aktivierung von Durchsetzungsmaßnahmen.

Kontrollaktionen können von den Sicherheitsteams manuell initiiert werden. Zur Steigerung der Effizienz der Sicherheitsmaßnahmen ist es jedoch auch möglich, schrittweise Automatisierung einzuführen. Das beginnt mit grundlegenden und wiederholten Aufgaben und wird im Laufe der Zeit zu komplexeren Kontrollen erweitert, damit hochqualifizierte IT-Experten sich auf schwerwiegendere Probleme konzentrieren können. Dieser Ansatz gewährleistet minimale Betriebsstörungen und verbessert erheblich Netzwerkzugriff, Geräte-Compliance, Netzwerksegmentierung sowie die Reaktion auf Vorfälle.

> "Die Maßnahmen für Endgeräte lassen sich meist automatisieren, doch auch manuelle Eingriffe erfordern lediglich einen einfachen Mausklick." – *Joseph Cardamone, Senior Information Security Analyst und North America Privacy Officer bei Haworth*

Herausforderungen

- Nicht konforme oder unberechtigte Geräte im Netzwerk stellen ein großes Risiko dar
- Einfache, kaum segmentierte Netzwerke erhöhen die Gefahr durch laterale Bedrohungen für das Unternehmen
- Fehlende Möglichkeit zur schnellen und effektiven Reaktion auf Sicherheitsbedrohungen und Zwischenfälle
- Beschränkte Kapazitäten zur Durchsetzung eines einheitlichen Gerätezustands mithilfe von Sicherheitstools
- Risiken für geschäftliche Abläufe schränken die Automatisierung von Sicherheitskontrollen ein

Durchsetzung von Netzwerkzugriffskontrollen

Kontrollieren Sie den Zugriff auf Unternehmensressourcen anhand von Benutzerprofil (Gast, Mitarbeiter, Auftragnehmer), Geräteklassifizierung und Sicherheitsstatus.

- Differenzierter Zugriff für Gast- und BYOD-Geräte
- Durchsetzung von Netzwerkzugriffsrichtlinien mit oder ohne 802.1X-Authentifizierung
- Durchführung von Maßnahmen bei verdächtigen, nicht autorisierten oder Schatten-IT-Geräten im Netzwerk
- Einschränkung oder Blockierung des Netzwerkzugriffs für kompromittierte oder böswillige Geräte
- Quarantäne für nicht konforme Geräte, bis die Compliance-Verstöße beseitigt wurden

"Wir entschieden uns zum Teil deshalb für die Forescout-Plattform, weil diese Technologie nicht zwingend auf das 802.1X-Protokoll setzt, was die Bereitstellung deutlich vereinfacht. Da wir keine Agenten installieren müssen, profitieren wir von hoher Leistung bei weniger Aufwand."
—Juan Ignacio Gordon, Leiter IT-Sicherheit bei ACCIONA

Verbesserung der Geräte-Compliance

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

- Gewährleistung der korrekten Konfiguration von Endgeräten und Durchführung von Behebungsmaßnahmen bei schwerwiegenden Konfigurationsverstößen (z. B. schwachen oder standardmäßigen Kennwörtern)
- Überprüfung der Installation, Ausführung und Aktualisierung aller erforderlichen Anwendungen und Sicherheitsagenten
- 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®)

"Wir erwarten, dass wir mit der Lösung von Forescout Millionen einsparen, da Audits exponentiell beschleunigt werden, diese weniger Problemstellen aufzeigen und weniger Korrekturmaßnahmen erfordern."
— Phil Bates, Chief Information Security Officer, US-Bundesstaat Utah

Implementierung dynamischer Netzwerksegmentierung

Mit einem einheitlichen Richtlinien-Framework können Sie in Ihrer erweiterten Unternehmensumgebung Richtlinien zur dynamischen Netzwerksegmentierung für unterschiedliche Durchsetzungstechnologien nutzen.

- Dynamische Zuweisung von Geräten in Segmentierungsgruppen basierend auf Geräteeigenschaften, Klassifizierung und Sicherheitsstatus
- Nutzung von Segmentierungskontrollen für VLANs, ACLs, WLAN-Kontrollen und Tagging in Campus- und OT-Netzwerken
- Anwendung von Segmentierungskontrollen über Sicherheitsgruppen/Tags in Public- und Private-Cloud-Umgebungen wie AWS und VMware NSX
- Segmentierung nicht konformer und anfälliger Geräte in verschiedene Zonen (insbesondere für Geräte, die nur innerhalb geplanter Wartungsfenster gepatcht oder korrigiert werden können), damit störungsfreier Geschäftsbetrieb mit minimaler Angriffsfläche gewährleistet ist
- Durchsetzung von Segmentierungsrichtlinien zur Isolierung von Geräten und kritischen Datenflüssen vom Rest des Netzwerks, wie von HIPAA, PCI, SWIFT CSP und anderen Vorschriften gefordert

"Forescout kann nicht nur Geräte isolieren und Netzwerksegmentierung durchführen, sondern auch bislang unbekannte Netzwerke entdecken." – *Stellvertretender CISO, großes Unternehmen im Gesundheitswesen*

Schnellere Reaktion auf Zwischenfälle

Mit der schnellen sowie effektiven Eindämmung von Bedrohungen und Reaktion auf Zwischenfälle können Sie Unterbrechungen der Geschäftsabläufe sowie Schäden für das Unternehmen minimieren.

- Erkennung riskanter Geräte, die nicht eingedämmt oder korrigiert wurden
- Erkennung von Kompromittierungsindikatoren 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 kompromittierten Geräten
- Kürzere mittlere Reaktionszeit durch Bereitstellung von wertvollem Gerätekontext (Geräteverbindung, Standort, Klassifizierung und Sicherheitsstatus) für funktionsübergreifende Vorfallreaktionsteams und isolierte Technologien

"Forescout ist wie ein automatischer Bedrohungsjäger für das Team, der Rund um die Uhr in unserem weltweiten Netzwerk nach Bedrohungen sucht. Wir lösen jetzt Probleme, die für uns vorher nicht lösbar waren. Aufgaben, die zuvor Stunden in Anspruch nahmen, dauern jetzt nur noch wenige Minuten." — *Nick Duda, Leitender Sicherheitstechniker, HubSpot*

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