FORESCOUT

# eyeControl

## Durchsetzung richtlinienbasierter Kontrollen

# Kontrollmaßnahmen in heterogenen Netzwerken durchsetzen und automatisieren

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

**Agentenlos**
Kontinuierliche Einstufung des Asset-Zustands und automatische Compliance-Durchsetzung ohne Installation von Agenten.

**Effektiv**
Flexibles Modul für einheitliche Richtlinien zur Implementierung sicherer Zero Trust-Zugriffe.

**Keine Upgrades erforderlich**
Nahtlose Integration in die vorhandene Infrastruktur ohne Software- oder Hardware-Upgrades.

**Geringere Gesamtbetriebskosten**
Schnellere Rendite dank niedrigerer Kosten für Bereitstellung, Wartung und Betrieb.

**Forescout eyeControl** bietet eine flexible, reibungslose Netzwerkzugriffssteuerung für heterogene Unternehmensnetzwerke. Die Lösung erzwingt und automatisiert Zero Trust-Sicherheitsrichtlinien für Least Privilege-Zugriffe auf alle verwalteten und unverwalteten Assets in Ihrer digitalen Umgebung. Richtlinienbasierte Kontrollen ermöglichen es, die Gerätekonformität kontinuierlich durchzusetzen, Ihre Angriffsfläche proaktiv zu verkleinern und schnell auf Vorfälle zu reagieren.

## Sicherer Netzwerkzugriff

- Durchsetzung richtlinienkonformer Netzwerkzugriffe, basierend auf der Benutzer- und Geräteidentität und dem Sicherheitsstatus
- Bereitstellung mit oder ohne 802.1X in heterogenen Netzwerken

## Durchsetzung der Gerätekonformität

- Automatisierte Einhaltung von Sicherheitsrichtlinien, Branchenstandards und gesetzlichen Vorschriften
- Auslösung von Korrekturmaßnahmen und Workflows zur Risikominimierung in Echtzeit

## Automatisierte Reaktion auf Vorfälle

- Automatisierte Reaktion auf Sicherheitsvorfälle
- Eindämmung von Bedrohungen, um ihre Ausbreitung und damit verbundene Störungen zu minimieren

# Zuverlässige Automatisierung von Kontrollen

Zero Trust-Richtlinien sind nur durchsetzbar, wenn sie auf vollständiger Gerätetransparenz und umfassendem Kontext basieren. Dazu gehören Echtzeitinformationen zur Benutzer- und Geräteidentität, zum Sicherheitszustand und zum Risikoprofil aller verbundenen Geräte. Kontrollen, die ohne vollständigen Überblick implementiert werden, können Störungen verursachen und die Betriebsabläufe beeinträchtigen. Deshalb nutzt eyeControl den umfassenden Gerätekontext aus eyeSight, um Zero Trust-Kontrollen zuverlässig durchzusetzen und zu automatisieren.

Den Kern von eyeControl bildet ein flexibles Modul für einheitliche Richtlinien, das Sie befähigt, detaillierte, gezielte Kontrollmaßnahmen anzuwenden. Das Modul bietet:

- Dynamische Sondierung und Gruppierung der Assets anhand von Geschäftslogik und Kontext
- Definition komplexer Bedingungen und Maßnahmen mit Boolescher Logik und Kaskadenrichtlinien, um anspruchsvolle Kontrollabläufe zu implementieren
- Policy Graph-Funktion zur Erstellung präziser Richtlinien, Analyse von Richtlinienflüssen und Optimierung von Richtlinien vor der Aktivierung von Durchsetzungsmaßnahmen
- Möglichkeit, mit manuell eingeleiteten Kontrollen zu beginnen und schrittweise zu automatischer Durchsetzung überzugehen, um die Effizienz der Sicherheitsmaßnahmen zu steigern

Bei Ereignissen und Änderungen auf einem bestimmten Gerät oder im Netzwerk werden Richtlinien in Echtzeit ausgelöst und bewertet. Die nachstehende Abbildung 1 zeigt die Bandbreite der Kontrollmaßnahmen, die in eyeControl möglich sind, wenn eine Richtlinie ausgelöst wird.a policy is triggered.

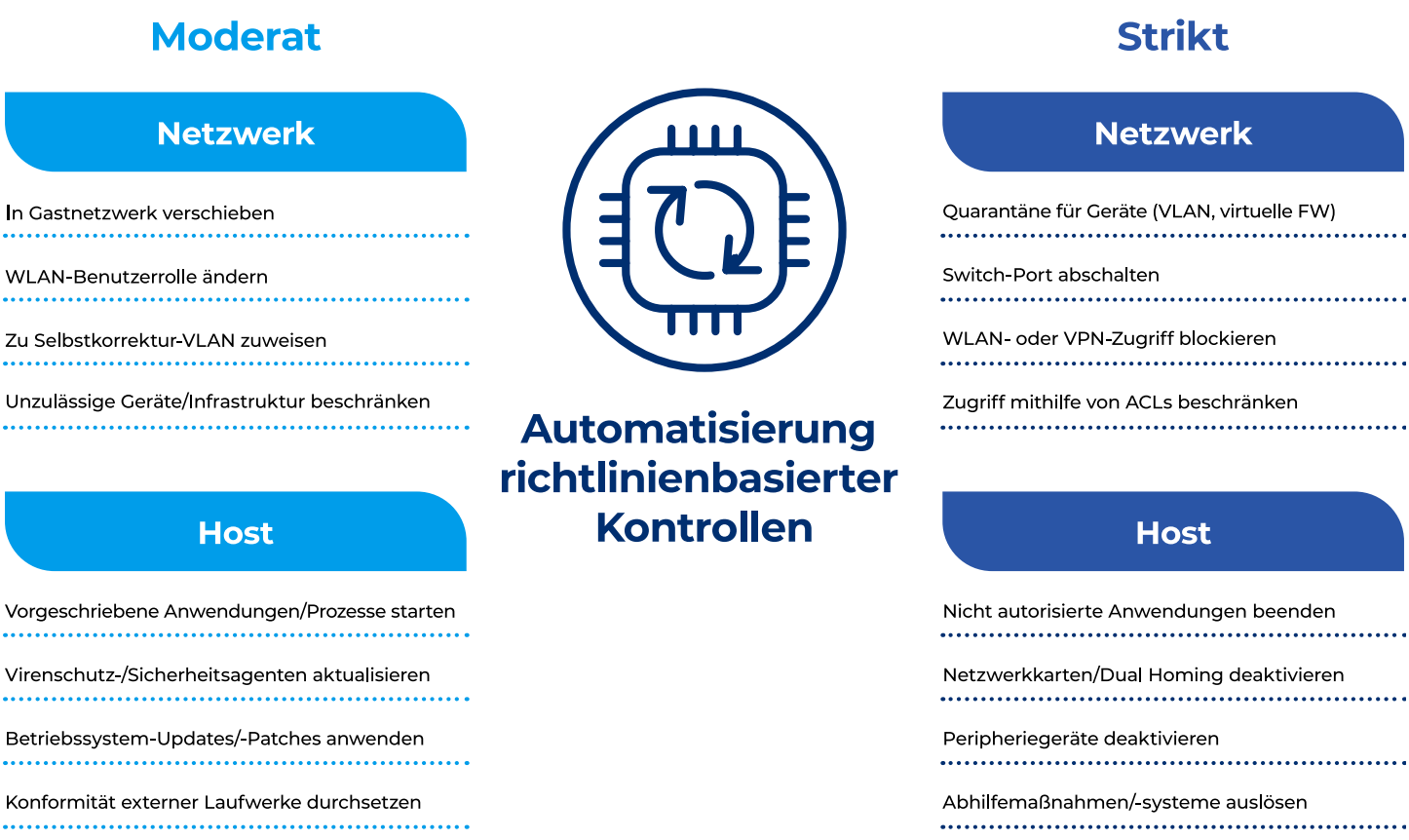


Abb. 1. Durchsetzung von Richtlinien im Netzwerk und auf Endgeräten mit nach und nach zunehmendem Automatisierungsgrad.

**eyeControl ist die Lösung für:**

- **Nicht autorisierte, unzulässige oder Spoofing-Geräte** im Netzwerk, die Risiken und Compliance-Probleme verursachen.
- **Sicherheitslücken,** wenn agentenbasierte Tools nicht aktualisiert sind oder nicht richtig funktionieren.
- **Flache kaum segmentierte Netzwerke,** die Unternehmen anfällig für Bedrohungen machen und den Wirkungsradius von Angriffen vergrößern.
- **Risiken für die Geschäftsabläufe** durch anfällige Geräte, auf denen wichtige Patches fehlen, sowie nicht autorisierte Anwendungen.
- **Seitliche Ausbreitung** von Bedrohungen, wenn kompromittierte oder bösartige Assets nicht schnell entschärft werden können.
- **Compliance-Verstöße,** wenn Richtlinien für verbundene Geräte nicht laufend überwacht und durchgesetzt werden können.
- **Probleme bei der NAC-Implementierung** in heterogenen Multivendor-Umgebungen und kabelgebundenen Netzwerken.

# Kontrollieren

## Sicherer Netzwerkzugriff

eyeControl ist die flexibelste NAC-Lösung für Unternehmen mit heterogenen Netzwerken und arbeitet ohne Störung von Geschäftsabläufen. Mit eyeControl können Sie den sicheren Zugriff aller verwalteten und unverwalteten Assets auf kabelgebundene und drahtlose Netzwerke durchsetzen, Audit-Anforderungen erfüllen, Ihre Angriffsfläche reduzieren und Bedrohungen schnell entschärfen. Die Funktionen umfassen:

- Implementierung von Zero Trust-Netzwerkzugriffen für die Geräte von Mitarbeitern, Gästen und Dienstleistern sowie BYOD-Geräte
- Ermitteln und Blocken von unzulässigen, nicht autorisierten und Spoofing-Geräten einschließlich Schatten-IT
- Quarantäne/Isolierung nicht konformer und stark gefährdeter Geräte bis zur Problembehebung
- Nutzung vielfältiger Methoden zur Zugriffskontrolle – mit oder ohne 802.1X-Authentifizierung
- Implementierung agentenloser Prüfungen des Gerätezustands; Durchsetzung von Maßnahmen im Netzwerk und auf Endgeräten mit einem Modul für einheitliche Zero Trust-Richtlinien
- Interoperabilität mit der bestehenden Infrastruktur ohne Software- oder Hardware-Upgrades
- Direkte Integration mit mehr als 30 Netzwerkinfrastruktur-Anbietern für hunderte Produktmodelle

# Einhalten

## Durchsetzung der Gerätekonformität

eyeControl ermöglicht die automatisierte Bewertung des Sicherheitszustands und Durchsetzung von Korrekturmaßnahmen. So können Sie interne Sicherheitsrichtlinien, externe Standards und branchenspezifische Vorschriften kontinuierlich einhalten.

- Validierung der korrekten Konfiguration von Endgeräten und Einleitung von Abhilfemaßnahmen bei gravierenden Konfigurationsverstößen
- Erkennung verwalteter Assets mit fehlenden oder defekten Sicherheitsagenten und Ausführung von Korrekturmaßnahmen
- Erkennung und Deaktivierung nicht autorisierter Anwendungen, die Risiken bewirken, die Netzwerkbandbreite beeinträchtigen oder die Produktivität behindern
- Erkennung von Geräten mit gefährlichen Schwachstellen oder fehlenden wichtigen Patches; automatische Einleitung von Abhilfemaßnahmen
- Agentenlose Durchsetzung von Maßnahmen zur Korrektur und Risikominderung auf Windows-, Mac-, Linux-, IoT-, IoMT- und OT-Geräten
- Implementierung von Richtlinien und Automatisierung von Kontrollen für vorschriftengerechte Konfigurationen in Cloud-Implementierungen (z. B. Amazon Web Services, Microsoft Azure, VMware)

# Automatisieren

## Schnellere Reaktion auf Vorfälle

Dämmen Sie Bedrohungen schnell ein und reagieren Sie effektiv auf Sicherheitsvorfälle, um Unterbrechungen der Betriebsabläufe und Auswirkungen auf das Geschäft zu minimieren.

- Automatisierung grundlegender, wiederkehrender Incident Response-Maßnahmen, damit die Teams Zeit für komplexere Aufgaben haben
- Erkennung von Indikatoren für Kompromittierungen (IOCs) und Risiken für Assets in Echtzeit, um die mittlere Reaktionszeit (MTTR) zu verkürzen
- Automatische Isolierung und Eindämmung kompromittierter oder bösartiger Assets, um die Ausbreitung von Malware im Netzwerk zu vermeiden und so den potenziellen Wirkungsradius zu begrenzen
- Automatisierte Reaktion auf Vorfälle und Einleitung von Korrektur-Workflows auf Geräten in Echtzeit
- Verkürzung der MTTR durch Bereitstellung von wertvollem Geräte-Kontext (Verbindung, Standort, Klassifizierung und Sicherheitsstatus) für funktionsübergreifende Incident Response-Teams und isolierte Technologien

# Erkennen, bewerten, steuern

Die Plattform von Forescout steigert den Nutzen von eyeControl mit Lösungen,die hundertprozentige Gerätetransparenz, kontinuierliche Compliance und Netzwerksegmentierung ermöglichen und eine solide Grundlage für Zero Trust-Strategien schaffen.

Für weitere Informationen besuchen Sie bitte www.forescout.com/products.

**Forescout Technologies, Inc.**

Gebührenfrei (US) 1-866-377-8771
Tel (intl) +1-408-213-3191
Support +1-708-237-6591

Erfahren Sie mehr auf Forescout.com