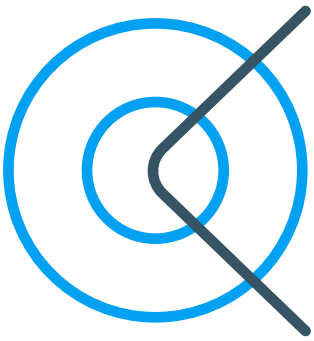
FORESCOUT



eyeSight

Die maßgebliche Informationsquelle zu jedem vernetzten Gerät in Ihrer IT-Umgebung

Agentenlos
Ganzheitliches Echtzeit-Inventar aller mit dem Netzwerk verbundenen Geräte, einschließlich Sicherheits- und Risikostatus.

Präzise
Klassifizierung aller Geräte, um Kontext für die Erstellung proaktiver Sicherheits- und Compliance-Richtlinien zu gewinnen.

Effektiv
Automatisierung von Routineaufgaben – etwa beim Compliance- und Risikomanagement –, um die Teams zu entlasten und menschliche Fehler zu minimieren.

Effizient
Echtzeit-Informationen zum ordnungsgemäßen Betrieb der Sicherheitstools und Compliance-Kontrollen.

Forescout eyeSight integriert sich tief in Ihre Netzwerkstrukturen, um Ihnen einen einzigartigen Überblick über alle verbundenen Geräte zu vermitteln.

- Erkennung sämtlicher Assets mit über 30 aktiven und passiven Techniken, die Abdeckungslücken in Ihrer IT-Umgebung aufzeigen und eine Echtzeit-Sicht auf Ihre Angriffsfläche bieten
- Automatische Klassifizierung von Geräten und Erstellung umfassender Profile einschließlich bekannter Risiken und Schwachstellen, basierend auf Threat Intelligence von Vedere Labs
- Frühzeitige Vorbereitung auf aufkommende Bedrohungen dank cloudbasiertem maschinellem Lernen, das laufend die Forescout Device Cloud optimiert, eine proprietäre Informationsquelle zu Geräten mit über 30 Milliarden einzelnen Datenpunkten
- Kontinuierliche Bewertung des Zustands, Risiko- und Compliance-Niveaus von Geräten, ohne dass ein Agent installiert werden muss – essenziell für den Schutz von IoT-, IoMT- und OT-Assets
- Automatisierte Berichte zum Compliance-Status und zur Gefährdung durch Cyberrisiken helfen, Zeit zu sparen, menschliche Fehler zu minimieren und sich auf das Wesentliche zu konzentrieren

Erkennen

Erkennung von Geräten, sobald sie sich mit dem Netzwerk verbinden
Kontinuierliche Überwachung sich an- und abmeldender Geräte
Echtzeit-Inventarisierung deckt Transparenzlücken auf

Klassifizieren

Erkennung unterschiedlicher IT-, IoT-, IoMT- und OT-Gerätetypen
Nutzung der leistungsstarken Device Cloud für vollständigen Gerätekontext
Effizientere, umfassendere und schnellere automatische Klassifizierung

Bewerten

Erkennung von Sicherheitsrisiken und Compliance-Lücken
Bewertung der Einhaltung interner und externer Vorschriften
Überblick über die bestehenden operativen und Cyberrisiken

eyeSight ist die Lösung für:

- **Transparenzlücken,** die durch isolierte Teams und verschiedenartige Sicherheitswerkzeuge verursacht werden
- **Operative und geschäftliche Risiken** aufgrund fehleranfälliger manueller Prozesse
- **Unvollständige Geräteinformationen,** durch die die Ausführung von Sicherheitsrichtlinien behindert wird
- **Sicherheitslücken,** wenn agentenbasierte Tools nicht aktualisiert sind oder nicht richtig funktionieren
- **Unbekannte, nicht autorisierte Geräte ,** oder MAC-Spoofing
- **Compliance-Verstöße,** die zwischen punktuellen Scans leicht auftreten können

Erkennen

Detaillierte Erkennung in Echtzeit

Vermeiden Sie blinde Flecken und minimieren Sie Risiken durch vollständige Transparenz über Ihre IT-Umgebung:

- Physische und SDN-Infrastruktur, einschließlich Switches, Routern, WAPs und Controllern
- Laptops, Tablets, Smartphones, BYOD-/Gastsysteme, im Homeoffice genutzte Geräte
- IoT-Assets in Campus-Netzen, Rechenzentren, Zweigstellen, an entfernten Standorten und in Edge-Netzwerken
- Public- und Private-Cloud-Instanzen in AWS-, Microsoft Azure- und VMware-Umgebungen
- OT- (Betriebstechnik) und industrielle Steuerungssysteme, einschließlich HMIs, SCADA, SPS, Gebäudemanagement- (BMS) und Gebäudeautomationssystemen (BAS)
- IoMT-Geräte in Krankenhäusern und anderen Gesundheitseinrichtungen, z. B. Infusionspumpen und Diagnosegeräte

Bedarfsgerechte Anpassung der Erkennungs- und Überwachungstechniken an Ihre Umgebung

Profitieren Sie von der Flexibilität von mehr als 30 aktiven und passiven Monitoring-Techniken für VPNs, kabelgebundene, kabellose, virtuelle und softwaredefinierte Netzwerke. So können Sie Unterbrechungen bei Geräten vermeiden, die auf aktive Scan-Techniken empfindlich reagieren.

AKTIVE INFRASTRUKTUR-ERKENNUNG

Abrufen der Netzwerkinfrastruktur

SDN-Integration
- Meraki
- Cisco ACI

Public-/Private-Cloud-Integration
- VMware
- AWS
- Azure

Abfrage von Verzeichnisdiensten (LDAP)
Abfrage von Webanwendungen (REST)
Abfrage von Datenbanken (SQL)
eyeExtend-Orchestrationen

PASSIVE GERÄTEERKENNUNG

SNMP-Traps

SPAN-Datenverkehr
Datenflussanalysen
NetFlow
- Flexible NetFlow
- IPFIX
- sFlow

DHCP-Anfragen
HTTP-Useragent
TCP-Fingerprinting
Protokollanalysen
RADIUS-Anfragen

AKTIVE GERÄTEERKENNUNG

Agentenlose Untersuchung von Windows-Geräten
- WMI
- RPC
- SMB

Agentenlose Untersuchung von macOS- und Linux-Geräten
- SSH

NMAP
SNMP -Abfragen
HTTP-Abfragen Forescout SecureConnector®

Klassifizieren

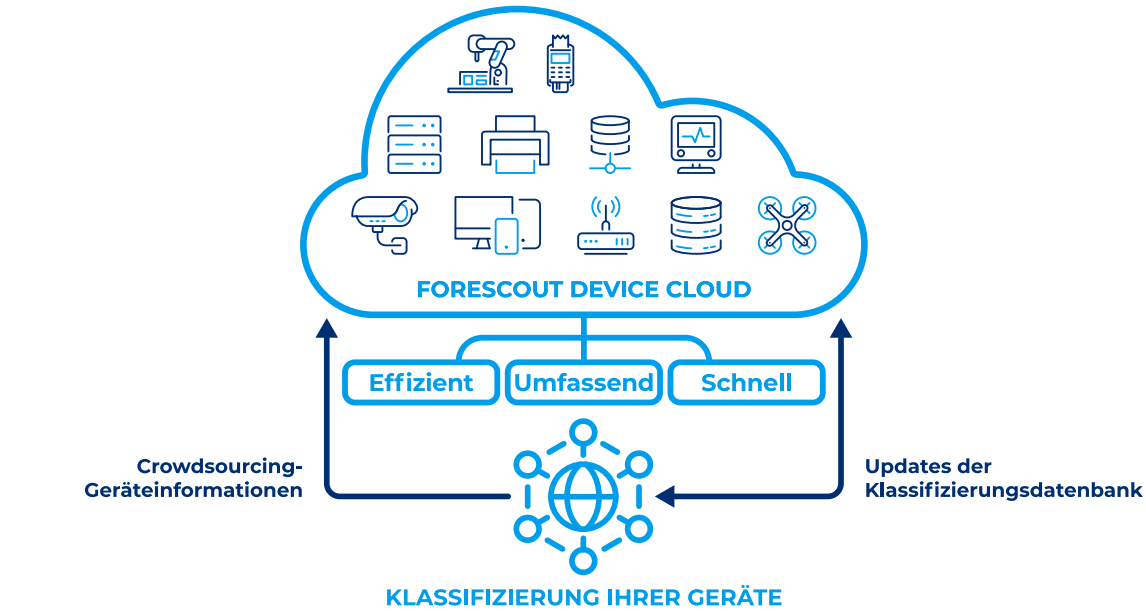
Intelligente automatische Klassifizierung

Wenn Sicherheitsrichtlinien ohne vollständigen Gerätekontext umgesetzt werden, kann dies zu unerwünschten Ergebnissen führen und die Betriebsabläufe gefährden. Die Forescout Device Cloud – das größte Repository für Gerätedaten, gesammelt bei über 50 Millionen Assets – liefert automatisch umfassenden Kontext für jedes vernetzte Gerät. Unser mehrdimensionales Klassifizierungsschema umfasst die Gerätefunktion und -art, das Betriebssystem und dessen Version sowie Hersteller und Modell, darunter:

- Mehr als 1.900 verschiedene Betriebssystemversionen
- Mehr als 7.700 verschiedene Gerätehersteller und -modelle
- Medizinische Geräte von mehr als 400 führenden Anbietern
- Tausende von industriellen Steuerungssystemen und Automatisierungsgeräten, die in der Fertigung, im Energiesektor, in der Öl- und Gasindustrie, bei Versorgungsunternehmen, im Bergbau und in anderen kritischen Infrastrukturbereichen zum Einsatz kommen

Automatische Klassifizierung auf Basis der Forescout Device Cloud

Die Device Cloud, das weltweit größte Repository für Geräteinformationen, bietet die umfassendsten und präzisesten Erkenntnisse zu Geräterisiken in Unternehmen aller Art.



Bewerten

Agentenlose Bewertung des Gerätezustands

eyeSight überwacht kontinuierlich das Netzwerk und prüft erkannte Geräte sofort auf ihre Konfiguration, ihren Sicherheitsstatus und ihre Risikoprofile, um festzustellen, ob sie den Compliance-Vorgaben und Sicherheitsrichtlinien entsprechen. Um die Risiken besser zu quantifizieren, können Richtlinien zur Prüfung von Konformitätsbedingungen angewandt werden, wie etwa folgende:

- Ist Sicherheitssoftware installiert, aktiv und aktuell?
- Ist das Gerät geschäftskritisch?
- Wurden Geräte entdeckt, auf denen nicht autorisierte Anwendungen laufen oder die gegen Konfigurationsstandards verstoßen?
- Gibt es Geräte – insbesondere IoT-, IoMT- und OT-Systeme –, die standardmäßige oder schwache Passwörter verwenden?
- Wurden unzulässige Geräte entdeckt, einschließlich solcher, die sich mithilfe von Spoofing-Techniken als legitim ausgeben?
- Welche verbundenen Geräte sind für die neuesten Bedrohungen am anfälligsten?

Überwachen

Compliance-Informationen erhalten

Holen Sie sich über vorkonfigurierte Dashboards praktisch umsetzbare Erkenntnisse, um Risiken in Ihrer gesamten Umgebung schnell zu erkennen, zu priorisieren und proaktiv einzudämmen. Anpassbare Dashboard-Ansichten erleichtern den Sicherheitsanalytikern und SOC-Teams zahlreiche Aufgaben:

- Bewertung der Risiken und Compliance-Fortschritte für alle oder eine beliebige Untergruppe von Richtlinien
- Ermittlung anfälliger und kompromittierter Geräte, um auf Vorfälle schneller und gezielter reagieren zu können
- Langfristige Verfolgung von Compliance-Trends
- Anpassung von Ansichten über den Risiko- und Compliance-Status zur Weitergabe an Führungskräfte und Prüfer
- Schnelle Suche und Filterung von Assets nach Richtlinien oder Geräteeigenschaften

Segmentieren, orchestrieren, durchsetzen

Die Plattform von Forescout steigert den Nutzen von eyeSight mit automatisierten Cybersecurity-Lösungen, die die Erstellung und Implementierung einheitlicher Richtlinien für die Netzwerkzugriffssteuerung sowie eine dynamische Netzwerksegmentierung ermöglichen, und schafft die Grundlage für Zero Trust-Sicherheit.

Um mehr über die Plattform von Forescout zu erfahren, besuchen Sie bitte www.forescout.com/platform/

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