Forescout eyeSight

Kontinuierliche Erkennung, Klassifizierung und Bewertung von Geräten für einen Überblick über die Sicherheitslage und zur Risikominimierung

CIOs tragen die Verantwortung für die Absicherung einer immer größeren Zahl von mit dem Netzwerk verbundenen Systemen, insbesondere IoT- und OT-Geräten. Da Sie nur schützen können, was Sie sehen, führt diese Zunahme an Geräten (und Gerätetypen) dazu, dass den Verantwortlichen die Bedeutung eines Überblicks über alle verbundenen physischen und virtuellen Geräte bewusst wird. Dazu gehören verwaltete, unverwaltete sowie unbekannte Geräte, die von Mitarbeitern, Auftragnehmern und Kunden oder sogar von wohlmeinenden IT-Mitarbeitern verbunden werden. Und unabhängig vom Standort all dieser Geräte im Netzwerk – auf dem Campus, im Rechenzentrum, in Private- und Public-Cloud- und sogar in OT-/ICS-Umgebungen – müssen sie alle zuverlässig erkannt, ein Profil erstellt und inventarisiert werden.

Gerätetransparenz im gesamten erweiterten Unternehmen

Abbildung 1. Detaillierte Übersicht über Campus, IoT, Rechenzentrum, Cloud und operative Technologien.

Mit Forescout eyeSight erhalten Sie einen einzigartigen Überblick über Ihren Gerätebestand, ohne dass wichtige Geschäftsprozesse unterbrochen werden. Zu Beginn erkennt die Lösung jedes per IP-Adresse verbundene Gerät in Ihren erweiterten Unternehmensnetzwerken. Die Erkennung ist jedoch nur der erste Schritt zu vollständiger Transparenz. Für die richtigen Richtlinien- und Kontrollentscheidungen ist umfassender Kontext unverzichtbar. Nach der Erkennung der verbundenen Geräte klassifiziert eyeSight diese automatisch und bewertet sie anhand von Unternehmensrichtlinien. Die leistungsstarke Kombination dieser drei Funktionen – Erkennung, Klassifizierung und Bewertung – liefert die erforderliche Gerätetransparenz, die für die richtigen Richtlinien und Aktionen erforderlich ist.

eyeSight

Kernpunkte

- Einheitliches Echtzeit-Inventar der mit dem Netzwerk verbundenen Geräte – ohne Agenten!
- Erstellung eines genauen Profils, um den erforderlichen Kontext zum Aufbau proaktiver Sicherheits- und Compliance-Richtlinien zu erhalten
- Identifizierung nicht autorisierter, anfälliger oder nicht konformer Geräte und Erstellung von Richtlinien, um die Risiken einzudämmen
- Zusätzliche Sicherheit durch eine Echtzeit-Anzeige, die Sie über das ordnungsgemäße Funktionieren der Sicherheitstools und Compliance-Kontrollen informiert
- Effiziente Erfassung und Dokumentation des Compliance-Zustands und des Cyberrisikos
- Automatisierung häufiger Aufgaben zur Minimierung menschlicher Fehler und Steigerung der Effizienz

Abbildung 2. Wichtige Transparenzfunktionen von eyeSight.

Kontinuierliche agentenlose Erkennung

Bei IoT- und OT-Geräten bestehen völlig neue Herausforderungen bezüglich der Transparenz. Durch die schiere Menge dieser Geräte wird die Skalierung zum Problem, da eine manuelle Erkennung nicht mehr sinnvoll möglich ist. Hinzu kommt, dass die meisten dieser Geräte keine Unterstützung für Agenten bieten und aktive Tests oder Scans System- und Geschäftsstörungen verursachen können. Deshalb nutzt eyeSight mehr als 20 aktive und passive Monitoring-Techniken (siehe Abbildung 3) und vermeidet potenzielle Transparenzlücken durch die automatische Erkennung von :

- Laptops, Tablets, Smartphones, BYOD-/Gastsystemen und IoT-Geräten in Campus-Netzwerken
- Virtuellen Maschinen, Hypervisoren und physischen Servern in Rechenzentren
- AWS-, Azure- und VMware-Instanzen in Public und Private Clouds
- Medizin-, Industrie- und Gebäudeautomatisierungsgeräten in OT-Netzwerken
- Physischen und Software-definierten Netzwerkinfrastrukturen einschließlich Switches, Routern, VPNs, drahtlosen Zugriffspunkten und Controllern

Zusammen können diese Erkennungsfunktionen die operativen Risiken minimieren und blinde Flecken beseitigen, um ein vollständiges und stets aktuelles Geräteinventar für das gesamte erweiterte Unternehmen zu erstellen.

Abbildung 3. Aktive und passive Erkennungstechniken.

PASSIVE INFRASTRUK-TUR-ERKENNUNG	PASSIVE ENDGERÄTE-ERKENNUNG	AKTIVE ENDGERÄTE-ERKENNUNG
SNMP-Traps	Abrufen der Netzwerkinfrastruktur	Agentenlose Windows-Untersuchung • WMI • RPC • SMB
SPAN-Datenverkehr	SDN-Integration • Meraki • Cisco ACI	Agentenlose macOS- und Linux-Untersuchung • SSH
Datenflussanalysen • NetFlow • Flexible NetFlow • IPFIX • sFlow	Public/Private-Cloud-Integration • VMware • AWS • Azure	NMAP
DHCP-Anforderungen	Abfrage von Verzeichnisdiensten (LDAP)	SNMP-Abfragen
HTTP-Benutzeragent	Abfrage von Webanwendungen (REST)	HTTP-Abfragen
TCP-Fingerabdrücke	Abfragedatenbanken (SQL)	SecureConnector®
Protokollanalysen	eyeExtend-Koordinierungen	
RADIUS-Anforderungen		

Herausforderungen

- Isolierte Teams, Sicherheitstools und Prozesse führen zu Transparenzlücken
- Fehleranfällige manuelle Prozesse führen zu operativen und geschäftlichen Risiken
- Durch unvollständige Geräteinformationen hat die IT nicht genügend Kontext für den Aufbau zuverlässiger Richtlinien
- Fehlende Möglichkeit zur Überprüfung, ob Sicherheitstools installiert, konfiguriert und ordnungsgemäß in Betrieb sind
- Unerkannte, nicht autorisierte Geräte verursachen unnötige Sicherheits- und Compliance-Risiken
- Veraltete punktuelle Scans führen zu fehlendem Vertrauen in den Compliance-Status

Intelligente automatische Klassifizierung

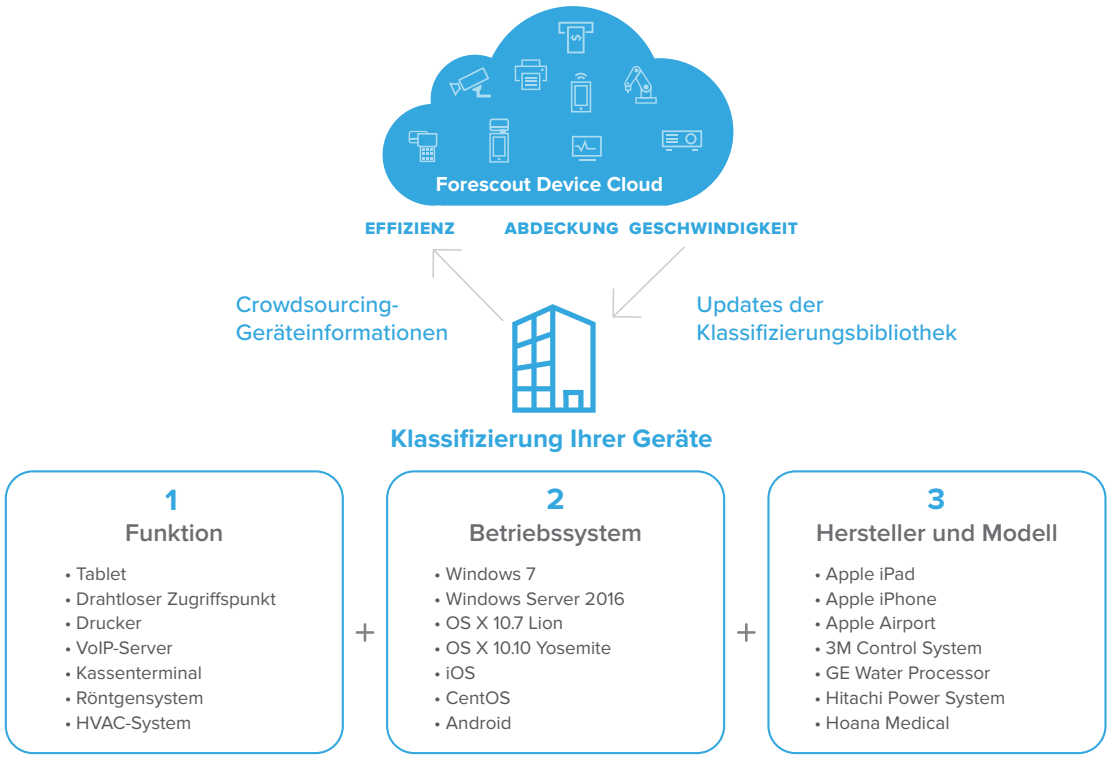
Vollständiger Kontext für jedes Gerät ist für die Erstellung detaillierter Richtlinien unverzichtbar. Sie müssen den operativen Kontext oder Zweck jedes Geräts kennen, um entscheiden zu können, wie es am besten abgesichert oder verwaltet werden kann. Aufgrund der wachsenden Zahl und Vielfalt der Geräte ist die manuelle Erfassung dieses Kontexts praktisch unmöglich. Gleichzeitig gefährdet die Erstellung von Richtlinien ohne den richtigen Kontext die betrieblichen Abläufe. Mit eyeSight werden herkömmliche, IoT- und OT-Geräte automatisch klassifiziert, wobei eine mehrdimensionale Klassifizierungstaxonomie verwendet wird, um Gerätefunktion und -typ, Betriebssystem und Version sowie Anbieter und Modell zu identifizieren. Dank Deep Packet Inspection von mehr als 100 IT- und OT-Protokollen erhält eyeSight umfassende Erkenntnisse über die Identität der IoT- und OT-Geräte.

eyeSight klassifiziert automatisch :

- Mehr als 500 unterschiedliche Betriebssystemversionen
- Mehr als 5.000 unterschiedliche Geräteanbieter und -modelle
- Geräte im Gesundheitswesen von mehr als 350 führenden Anbietern medizinischer Geräte
- Tausende Industriesteuerungs- und Automatisierungsgeräte, die in Fertigung, Energieversorgung, Öl- und Gas, Versorgungsunternehmen, Bergbau und anderen Bereichen zum Einsatz kommen

Forescout Device Cloud führt die automatische Klassifizierung in eyeSight durch und gewährleistet, dass diese umfangreiche Kontextquelle mit dem Wachstum und der Vielfalt bei Geräten Schritt halten kann. Forescout Research nutzt Informationen von über 8 Millionen realen Geräten in unserer Geräte-Cloud* und veröffentlicht regelmäßig neue Profile, um die Effizienz, Abdeckung und Geschwindigkeit bei der Klassifizierung in Ihrem gesamten Gerätebestand zu verbessern.

Abbildung 4. Forescout Device Cloud.



Stand: 31. Dezember 2018.

Bewertung des Gerätezustands

Die Geräteklassifizierung liefert betrieblichen Kontext über den Zweck eines Geräts – und informiert Sie letztendlich darüber, um was für ein Gerät es sich handelt. Für vollständigen Kontext ist jedoch eine weitere Perspektive erforderlich, um den Zustand und Patch-Status jedes Geräts zu bewerten.

Deshalb überwacht eyeSight kontinuierlich das Netzwerk und bewertet Konfiguration, Status sowie Sicherheitslage der verbundenen Geräte. Auf diese Weise werden ihre Risikoprofile ermittelt und festgestellt, ob sie die Sicherheits- und Compliance-Richtlinien einhalten. eyeSight beantwortet beispielsweise folgende wichtige Fragen:

- Ist Sicherheitssoftware installiert, aktiv und mit den neuesten Patches aktualisiert?
- Führen Geräte nicht autorisierte Anwendungen aus oder verletzen sie Konfigurationsstandards?
- Nutzen Geräte standardmäßige oder schwache Kennwörter (ein besonderes Risiko für IoT-Geräte)?
- Wurden nicht autorisierte Geräte entdeckt, beispielsweise solche, die sich mithilfe von Spoofing-Techniken als legitime Geräte ausgeben (und sind diese Geräte mit dem Netzwerk verbunden)?
- Welche verbundenen Geräte sind für die neuesten Bedrohungen am anfälligsten?

Die Möglichkeiten von Geräteinformationen

Die Gerätetransparenz von eyeSight, die durch Erkennung, Profilerstellung, automatische Klassifizierung und Bewertung ermöglicht wird, steht über die Forescout-Konsole zur Verfügung. Hier können Sie allgemeine Informationen in anpassbaren Dashboards erfassen und diese Snapshots weitergeben, während Sie an Ihren Risiko- und Compliance-Zielen arbeiten. Mithilfe dieser dynamischen Ansichten haben die Teams folgende Möglichkeiten:

- Analyse, wie erfolgreich eine bestimmte Richtlinie implementiert wurde
- Erkennung anfälliger Geräte im Falle einer Kompromittierung, um die Reaktion auf Zwischenfälle zu beschleunigen
- Überwachung der Einhaltung bestimmter Compliance-Vorschriften über einen längeren Zeitraum
- Erstellung von Ansichten über den Risiko- und Compliance-Status sowie potenzielle Schwachstellen für Führungskräfte und Prüfer
- Aufschlüsselung von Details zur Behebung von Problembereichen in Bezug auf bestimmte Richtlinien, Gerätetypen, Standorte usw.

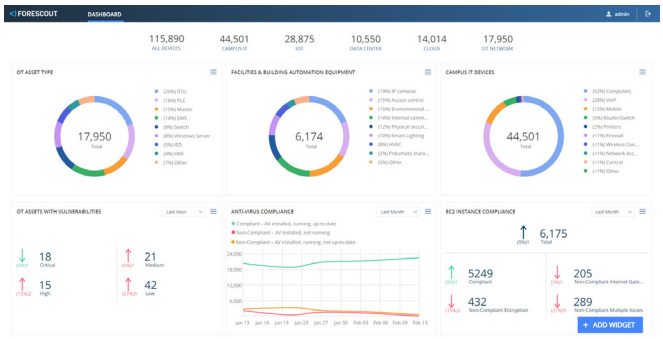


Abbildung 5. Das Dashboards ist anpassbar, damit jeder Verantwortliche den jeweils notwendigen Kontext erhält.

Die mit eyeSight ermöglichte Gerätetransparenz kann über Benachrichtigungsfunktionen und APIs gemeinsam mit funktionsübergreifenden IT-Verantwortlichen genutzt werden. Das eyeExtend-Produktportfolio gibt diesen Gerätekontext an andere führende IT- und Sicherheitsprodukte weiter, um Workflows zu automatisieren und systemweite Gegenmaßnahmen zu koordinieren.

Ohne den wichtigen Gerätekontext von eyeSight fehlt den Unternehmen das notwendige Wissen für die Implementierung optimaler Kontrollrichtlinien, was den reibungslosen Geschäftsbetrieb gefährden kann. Mit eyeSight erhalten Sie umfassende Erkenntnisse, auf deren Grundlage Sie detaillierte Richtlinien erstellen und implementieren können. Zudem lassen sich damit Maßnahmen für die Ressourcenverwaltung, Geräte-Compliance, Netzwerksegmentierung, den Netzwerkzugriff und die Reaktion auf Zwischenfälle automatisieren. Anschließend haben Sie mithilfe von Forescout eyeControl und Forescout eyeExtend die Möglichkeit, zuverlässige und effektive richtlinienbasierte Kontrollen einzurichten und Maßnahmen zu koordinieren.

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