FORESCOUT
Active Defense for the Enterprise of Things™

eyeSight
Umfassende Gerätetransparenz

AGENTENLOS

Gesamtheitliches Echtzeit-Inventar der mit dem Netzwerk verbundenen Geräte

AKKURAT

Profilerstellung für alle Geräte, um Zusammenhänge für die Definition von Sicherheit und Konformität besser zu verstehen

EFFEKTIV

Identifizierung von nicht zugelassenen Geräten, welche für Angriffe anfällig oder nicht richtlinienkonform sind und Erstellung entsprechender Regeln zur Risikominderung

ZUVERLÄSSIG

Echtzeit-Informationen zum ordnungsgemäßen Betrieb aller Sicherheitsanwendungen und Konformitätskontrollen

EFFIZIENT

Automatische Erfassung und Berichterstellung zur Konformitäts- und Risikolage sowie gleichzeitige Minimierung menschlicher Fehler und Steigerung der Effizienz

Kontinuierliche Erkennung, Klassifizierung und Einstufung aller vernetzten „Dinge“ im gesamten Unternehmen

Mit Forescout eyeSight verschaffen Sie sich einen einzigartigen Überblick über Ihr komplettes Enterprise of Things (EoT, Unternehmen der Dinge), ohne dass dafür wichtige Geschäftsprozesse unterbrochen werden.

- Erkennung aller per IP-Adresse vernetzten Geräte
- Automatische Klassifizierung von Geräten und Erhalt umfassender Zusammenhänge
- Einstufung der Richtlinienkonformität und des Sicherheitsstatus von Geräten

ERKENNUNG

Geräteerkennung bei Netzzutritt

Permanente Überwachung von sich an- und abmeldenden Geräten

Echtzeitinventarisierung ohne Störung der Geschäftsabläufe

KLASSIFIZIERUNG

Erkennung unterschiedlicher IT-, IoT- und OT-Gerätetypen

Nutzung der leistungsfähigen Forescout Device Cloud

Verbesserung der Effizienz, Abdeckung und Geschwindigkeit der automatischen Klassifizierung

EINSTUFUNG

Erkennung der Sicherheitslage und Konformitätslücken

Bewertung der Einhaltung interner und externer Regularien

Überblick über die Sicherheitslage bei operativen und Cyber-Risiken

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

ERKENNUNG

Permanente, agentenlose Geräteerkennung

Vermeiden blinder Flecken und Minimieren des operativen Risikos mit vollständiger Transparenz über Ihr EoT:

- Laptops, Tablets, Smartphones, BYOD-/Gastsysteme und im Homeoffice verwendete Geräte
- IoT-Geräte in Campus-Netzwerken, Rechenzentren, Niederlassungen, an entfernten Standorten und in Edge-Netzwerken
- Public- und Private-Cloud-Instanzen in AWS-, Azure- und VMware-Umgebungen
- OT-Systeme (operative Technologie), einschließlich Medizin-, Industrie- und Gebäudeautomatisierungsgeräte
- Physische und SDN-Infrastrukturen, einschließlich Switches, Routern, WLAN-APs und Controllern

Profitieren Sie von der Flexibilität von über 20 aktiven und passiven Monitoring-Techniken für drahtgebundene, drahtlose, VPN, virtuelle und Software-definierte Netzwerke. Vermeiden Sie Unterbrechungen bei Geräten, die sensibel auf aktive Scan-Techniken reagieren.

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

KLASSIFIZIERUNG

Intelligente automatische Klassifizierung

Zero-Trust-Richtlinien können nur durchgesetzt werden, wenn sie auf vollständigem Gerätekontext basieren. Es ist nahezu unmöglich, diese Zusammenhänge manuell zu sammeln. Zudem können Zero-Trust-Richtlinien, die ohne vollständigen Gerätekontext implementiert werden, die betrieblichen Abläufe beeinträchtigen. Dank Deep Packet Inspection von mehr als 150 IT- und OT-Protokollen erstellt eyeSight umfassende Profile aller IT-, IoT- und OT-Geräte. Ein mehrdimensionales Klassifizierungsschema identifiziert die Gerätefunktion und -art, das Betriebssystem und seine Version sowie Anbieter und Modell, darunter:

- Mehr als 600 unterschiedliche Betriebssystemversionen
- Mehr als 5.700 unterschiedliche Geräteanbieter und -modelle
- Medizinische Geräte von mehr als 400 führenden Anbietern medizinischer Geräte
- Tausende Industriesteuerungssysteme und Automatisierungsgeräte, die in Fertigung, Energieversorgung, Öl- und Gas-Sektor, Versorgungsunternehmen, Bergbau und anderen Bereichen zum Einsatz kommen

EYESIGHT BIETET LÖSUNGEN FÜR:

Transparenzlücken, die durch isoliert arbeitende Teams und separate Sicherheitstools verursacht werden

Operative und geschäftliche Risiken aufgrund von fehleranfälligen manuellen Prozessen

Unvollständige Geräteinformationen, die die Ausführung von zuverlässigen Zero-Trust-Richtlinien behindern

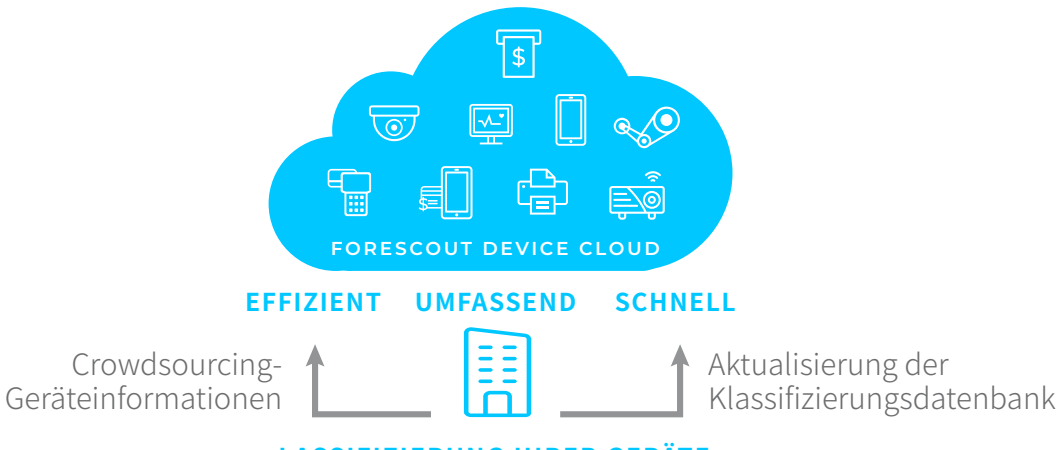
Sicherheitslücken, wenn agentenbasierte Tools nicht auf dem neuesten Stand sind oder nicht richtig funktionieren

Unerkannte nicht autorisierte Geräte oder Spoofing

Konformitätsverstöße, die schnell zwischen punktuellen Scans auftreten können

Automatische Klassifizierung auf Basis von Forescout Device Cloud

Device Cloud, der weltweit größte Crowdsourcing-Data Lake für Geräteinformationen, bietet die umfangreichsten und genauesten Erkenntnisse über alle Geräterisiken mit Bezug auf jedes individuelle Unternehmen.



LASSIFIZIERUNG IHRER GERÄTE

Funktion		+	Betriebssystem		+	Anbieter und Modell	
• Tablet	• Kassenterminal		• Windows 7	• iOS		• Apple iPad	• GE Water Processor
• WLAN Access Point	• Röntgensystem		• Windows Server 2016	• CentOS		• Apple iPhone	• Hitachi Power System
• Drucker	• HVAC-System		• OS X 10.7 Lion	• Android		• Apple Airport	• Hoana Medical
• VoIP-Server			• OS X 10.10 Yosemite			• 3M Control System	

EINSTUFUNG

Prüfung des Gerätezustands

Ein weiteres grundlegendes Element von Zero-Trust-Richtlinien ist die Berücksichtigung der Sicherheitsmaßnahmen und Risikoprofile der Geräte, die sich mit dem Netzwerk verbinden. eyeSight überwacht das Netzwerk kontinuierlich, um die Konfiguration, Sicherheitslage und Risikoindikatoren vernetzter Geräte zu beurteilen und zu prüfen, ob sie die Konformitätsvorgaben und Sicherheitsstandards erfüllen. Zero-Trust-Richtlinien können auf Risiko- und Konformitätsbedingungen basieren, wie zum Beispiel:

- Ist Sicherheitssoftware installiert, aktiv und auf dem neuesten Stand?
- Führen Geräte nicht autorisierte Anwendungen aus oder verletzen sie Konfigurationsstandards?
- Nutzen Geräte, insbesondere IoT- und OT-Systeme, standardmäßige oder schwache Kennwörter?
- Wurden nicht autorisierte Geräte entdeckt, einschließlich solcher, die sich mithilfe von Spoofing-Techniken als legitime Geräte ausgeben?
- Welche verbundenen Geräte sind für die neuesten Bedrohungen am anfälligsten?

ÜBERWACHUNG

EoT-Transparenz und -Konformität

Holen Sie sich über vorkonfigurierte und anpassbare Dashboards verwendbare Informationen, um Risiken für alle Ihre vernetzten „Dinge“ schnell zu identifizieren, zu priorisieren und proaktiv einzudämmen. Dynamische Ansichten helfen Sicherheitsanalysten und SOC-Teams bei:

- Die Erfassung des Fortschritts mit Bezug auf die Erreichung von richtlinienbasierten Risiko- und Konformitätszielen
- Der Identifizierung anfälliger und kompromittierter Geräte zur schnelleren Reaktion auf Vorfälle
- Der Verfolgung von Konformitätstrends über einen längeren Zeitraum
- Der Bearbeitung von Dashboards über den Risiko- und Konformitätsstatus zur Weitergabe an Führungskräfte und Prüfer
- Der schnellen Suche und Filterung von Geräten im EoT basierend auf Richtlinien oder Geräteattribute

Segmentierung, Koordinierung und Durchsetzung

Steigern Sie den Wert von eyeSight mit Forescout-Produkten zur Erstellung und Implementierung von Zero-Trust-Richtlinien für die Netzwerkzugriffssteuerung, IoT-Sicherheit, Netzwerksegmentierung und OT-Sicherheit.

Besuchen Sie die Seite www.forescout.de, um mehr über die Forescout-Produkte eyeSegment, eyeControl, eyeInspect und eyeExtend zu erfahren.

Nicht nur alles sehen, sondern alles schützen.

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

forescout.com/platform/eyeSight 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