SOLUTION BRIEF

Lösungsbeschreibung der Forescout 4D Platform™

FORESCOUT

LÖSUNGSBESCHREIBUNG DER FORESCOUT 4D PLATFORM™

Früher waren Netzwerke einfacher aufgebaut und konnten mit klassischen Perimeterschutzmaßnahmen zuverlässig abgesichert werden. Mit dem Aufkommen und der zunehmenden Nutzung neuer Geschäftsmodelle und unterstützender Technologien kommen jedoch immer mehr Geräte online – das Netzwerk wird dadurch zunehmend erweitert und schwerer zu kontrollieren.

Die Zahl der IoT-Geräte wird voraussichtlich von 14 Milliarden im Jahr 2023 auf 25 Milliarden bis 2030 steigen. Mit der wachsenden Angriffsfläche entstehen größere Sicherheitslücken, massive Blind Spots sowie zahlreiche Duplikate und Konflikte, die sich nicht einfach auflösen lassen. Je größer die Angriffsfläche wird, desto höher ist das Risiko eines Cyberangriffs.

Unabhängig davon, ob Ihre Priorität auf Cybersicherheit, Netzwerkzugriff und Datenschutz oder auf Systemverfügbarkeit, Produktion und Sicherheit liegt – die Fragen bleiben die gleichen:

- Was verbindet sich mit meinem Netzwerk?
- Wo bestehen Schwachstellen und Risiken?
- Welche Bedrohungen durchdringen meine Verteidigung?
- Wie kann ich proaktiv reagieren, Schäden begrenzen und Probleme eindämmen?

Wer für hochregulierte Umgebungen verantwortlich ist, in denen strenge Richtlinien und Compliance gefordert sind, muss nicht nur Sicherheitsrahmenwerke, Branchenstandards und gesetzliche Vorgaben erfüllen, sondern auch jederzeit belastbare Nachweise für deren Einhaltung liefern können.

Dafür brauchen Sie eine zentrale Plattform, die Ihnen vollständige Sichtbarkeit über alle Unternehmensressourcen, automatisierte Kontrolle, IT-Compliance und Steuerung sowie umfassende Risikominimierung und Bedrohungsabwehr bietet – und zwar sofort.

DIE FORESCOUT 4D PLATFORM™ ALS ANTWORT

Die Forescout 4D Platform™ ist eine Cybersicherheitslösung, die intelligente Kontrolle und kontinuierliche IT-Compliance und Steuerung für jedes Gerät an jedem Ort ermöglicht. Die Plattform basiert auf vier zentralen Funktionen: **Erkennen (Discover), Bewerten (Assess), Reagieren (Respond) und Kontrollieren (Control)**. Diese erstrecken sich über lokale Installationen ebenso wie über die Cloud und liefern vollständige Transparenz sowie Schwachstellenanalysen für verwaltete und nicht verwaltete Geräte im gesamten Unternehmen.

DISCOVER (ERKENNEN)

Alles beginnt mit der Erkennung. Die Forescout 4D Platform™ nutzt über 30 Erkennungsmethoden, Integrationen und APIs zur umfassenden Sichtbarkeit, Identifizierung, Klassifikation und Überwachung jedes angeschlossenen Geräts in Ihrer Umgebung – in Echtzeit und auf allen Gerätetypen und Purdue-Ebenen.

Die durch diese Mechanismen gewonnenen Kontextinformationen ermöglichen es Ihnen, den gesamten Lebenszyklus eines Assets – von der Anschaffung über Wartung bis zur Außerbetriebnahme – präzise zu verfolgen. Die Plattform erkennt Geräte und führt über die gesamte Nutzungsdauer hinweg aktuelle, kontextbezogene Aufzeichnungen.

Diese lückenlosen Aufzeichnungen sichern die Betriebsabläufe und ermöglichen die Nachverfolgbarkeit von Änderungen – ein wichtiger Beitrag zur Einhaltung von Vorschriften. Die Plattform liefert darüber hinaus detaillierte Einblicke, die den IT-Betrieb optimieren, Ausfallzeiten reduzieren, Wartungspläne verbessern und die Systemleistung steigern.

Erkennungsfunktionen lassen sich außerdem nutzen, um IT-, IoT- und IoMT-Domänen zu vereinheitlichen – durch die Orchestrierung mit CMDBs, IT Operations und Service-Management-Tools.

ASSESS (BEWERTEN)

Die Bewertungsfunktionen der Forescout 4D Platform™ erzeugen kontextreiche Einblicke in Risiken, die durch Sicherheitslücken im Asset-Zustand, im Verhalten und bei der Compliance entstehen. Die Plattform korreliert verschiedene Datenpunkte aus heterogenen Umgebungen und erstellt priorisierte Risikobewertungen auf Grundlage der Kritikalität.

Sobald hohe Risiken und Schwachstellen identifiziert werden, aktiviert die Plattform Kontroll- und Orchestrierungsprozesse zur automatisierten Risikominderung und unterstützt schnelle Entscheidungen – für ein selbstbewusstes Risikomanagement.

Dank fortschrittlicher Schwachstellenerkennung erkennt die Plattform nicht gepatchte Geräte, die versuchen, sich zu verbinden – basierend auf einer kuratierten Datenbank, angereichert mit EPSS, CISA KEVs und den Forschungserkenntnissen von Vedere Labs (VL-KEV). Die Plattform bewertet kontinuierlich Risiken über IT-, OT-, IoT- und IoMT-Geräte hinweg – mit Echtzeit-Einblicken auf Geräte- und Unternehmensebene. Das Ergebnis: proaktives Risikomanagement und erhöhte betriebliche Resilienz.

RESPOND (REAGIEREN)

Forescout wandelt Bewertungen direkt in Handlungen um – mit automatisierter Compliance-Prüfung und Remediation. Dazu gehören etwa das Isolieren von Geräten, das Blockieren von Datenverkehr sowie koordinierte Reaktionen zwischen IT- und Sicherheitsdiensten.

Die Plattform nutzt moderne Bedrohungserkennungsmethoden wie Deep Packet Inspection, Eventanalyse und Threat Intelligence von Vedere Labs für IT-, OT-, IoT- und IoMT-Umgebungen. Automatisierte Richtlinienmaßnahmen und Orchestrierung greifen sofort bei erkannten Bedrohungen, Fehlkonfigurationen und Regelverstößen.

Zudem lassen sich SOAR-Benachrichtigungen mit benutzerdefinierten Feldern erstellen, um Webhooks und automatisierte Workflows mit weiterem Kontext anzureichern.

Ob im Netzwerkbetrieb oder im Security Operations Center: Rollenbasierte Dashboards zeigen Warnungen und Fälle an, die exakt auf Ihre Verantwortlichkeiten abgestimmt sind.

CONTROL (KONTROLLIEREN)

Zentralisierte Durchsetzung von Sicherheitsrichtlinien und Zugriffsregeln sichert konsistente Abläufe und IT-Compliance und Steuerung im großen Maßstab. Die Forescout 4D Platform™ bietet einheitliches Richtlinienmanagement an kritischen Entscheidungspunkten – für unternehmensweite Konsistenz, Compliance und automatisierte Kontrolle mit präziser Skalierbarkeit.

Administratoren können granulare Richtlinien über Vorlagen definieren oder eigene Profile verwenden, um Konformität und Berichtswesen zu vereinfachen. Die Plattform unterstützt außerdem rollenbasierten Zugriff und Zero-Trust-Segmentierung – für eine reduzierte Angriffsfläche ohne Beeinträchtigung des laufenden Betriebs.

KOMPONENTEN DER FORESCOUT 4D PLATFORM™

FORESCOUT eyeSIGHT: ECHTZEIT-ASSET-TRANSPARENZ

- Passives Netzwerkmonitoring mit Echtzeit-Geräteerkennung
- Agentenlos – keine Softwareinstallation auf Endgeräten
- Umfassende Asset Intelligence (Gerätetyp, Betriebssystem, Software)

FORESCOUT eyeSCOPE

- Ein konsolenbasierter Überblick über alle Assets
- Zustands- und Performanceüberwachung der Deployment-Umgebung
- KI-gestützte Dashboards & Berichte; erweiterbar mit Xplorer
- Benutzerverwaltung und rollenbasierte Zugriffskontrolle

FORESCOUT eyeCONTROL: RICHTLINIENBASIERTE KONTROLLE

- Automate network access control based on security posture.
- Quarantine, block, or limit device access if they fail to meet security requirements.
- Orchestrate remediation steps, like patching or software updates, for non-compliant devices.

FORESCOUT eyeINSPECT: OT/ICS-SCHUTZ

- Vollständige Transparenz in IT, OT, IoT und IoMT
- Passives Monitoring industrieller Netzwerke
- Automatisiertes Schwachstellenmanagement
- Protokollbasierte Bedrohungserkennung und Anomalieerkennung

FORESCOUT eyeEXTEND: ÖKOSYSTEM-INTEGRATION

- Verbindet Forescout mit ITSM, NGFW, SIEM, EDR etc.
- Orchestriert Workflows zwischen Tools
- Erweiterung auf Cloud-, OT- und Drittplattformen

FORESCOUT eyeFOCUS: RISIKOBEWERTUNG &

- Automatisiertes Risikoscoring nach Schwachstellen und Fehlkonfigurationen
- Kritikalitätsbasierte Priorisierung
- Handlungsempfehlungen und automatische Behebung

FORESCOUT eyeALERT: FRÜHERKENNUNG VON BEDROHUNGEN

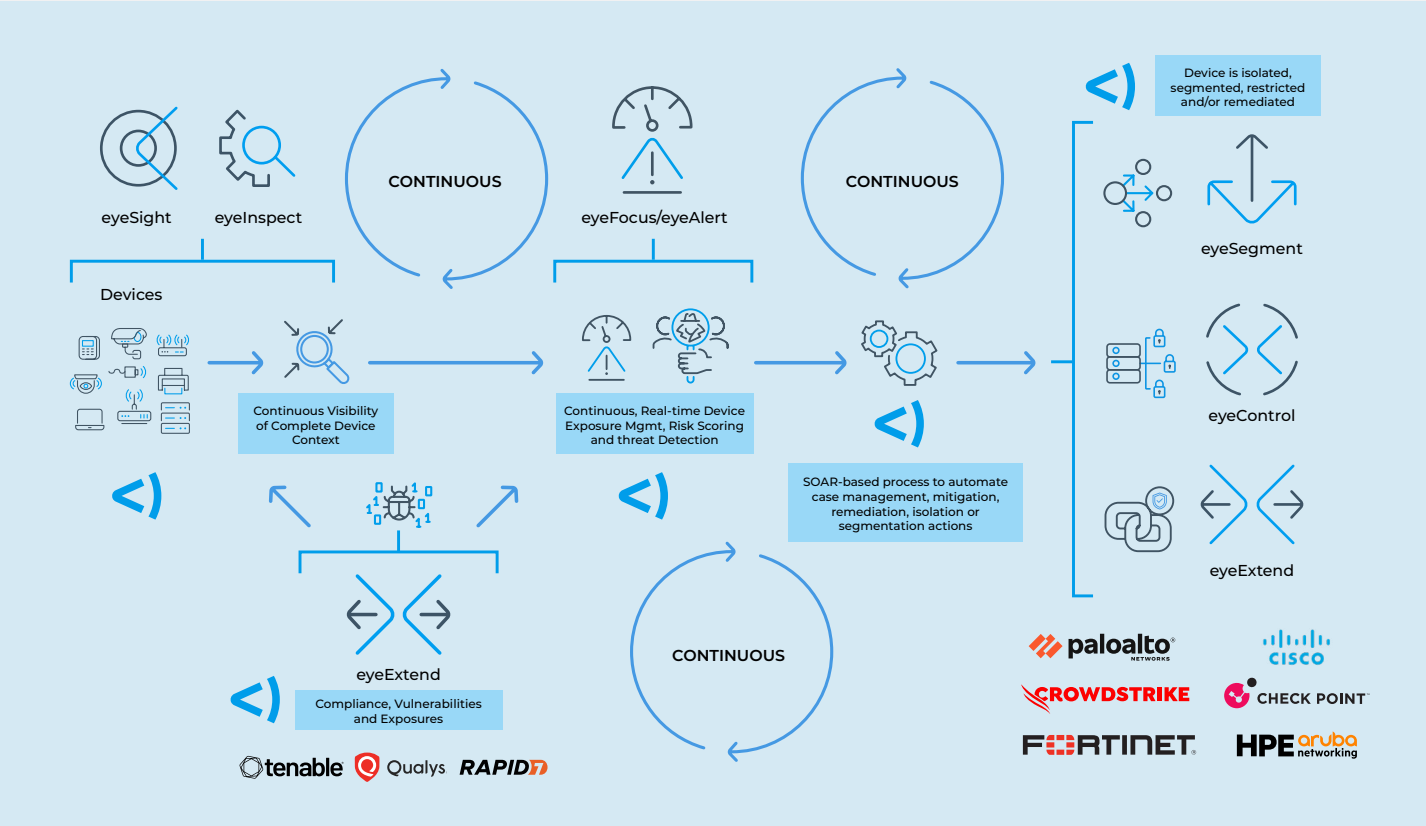
- Verhaltensanalytik mit Machine Learning
- Integration globaler Threat Feeds
- Automatisierte Incident Response mit eyeControl

JEDES ASSET. JEDES RISIKO. UNTER KONTROLLE.

Die Forescout 4D Platform™ bietet skalierbare Cybersicherheitslösungen mit den nötigen Einblicken und der Flexibilität, Cyber-Assets kontinuierlich und nahezu in Echtzeit zu steuern – unabhängig vom Bereitstellungsmodell.

Forescout sieht alles. Mit Forescout ist Ihr Netzwerk unter Kontrolle.

EIN TAG IM LEBEN EINES GERÄTS



1. Gerät erscheint im Netzwerk und wird ggf. authentifiziert
2. Es wird klassifiziert, bewertet, ggf. remediated oder segmentiert
3. OT-Geräte können ebenfalls erkannt und analysiert werden
4. Kommunikationsflüsse werden kontextualisiert visualisiert
5. Schwachstellen und Risiken werden zu einem dynamischen Risikowert verdichtet
6. Log- und Telemetriedaten ermöglichen frühzeitige Bedrohungserkennung
7. SOAR-, Richtlinien- oder Drittanbieteraktionen können ausgelöst werden
8. Gerät wird isoliert, remediated oder der Verkehr segmentiert
9. Das vom Gerät ausgehende Risiko wird eingedämmt

ABOUT FORESCOUT

Forescout Technologies, Inc., a global cybersecurity leader, continuously identifies, protects and helps ensure the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide vendor-agnostic, automated cybersecurity at scale.

The Forescout Platform delivers comprehensive capabilities for network security, risk and exposure management, and threat detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats. An IOT security leader dedicated to protecting the quality care of health delivery worldwide.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com