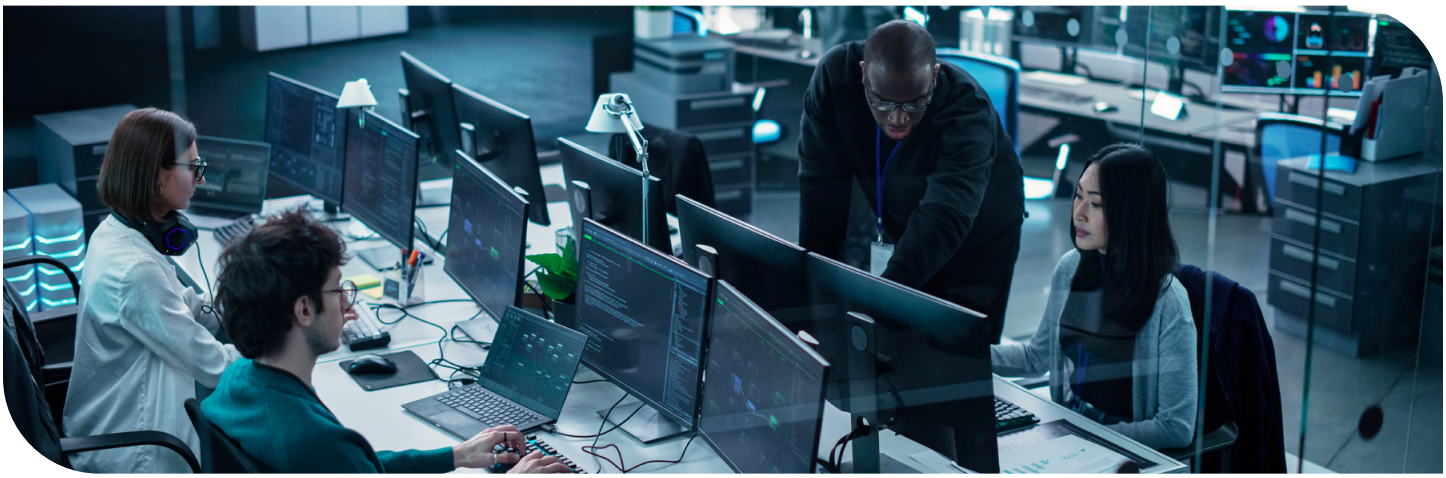
FORESCOUT

Risk and Exposure Management

Risiken und Compliance-Probleme identifizieren, quantifizieren und priorisieren



„Sicherheitsverletzungen gehen nur selten auf ausgeklügelte, staatlich gelenkte Angriffe oder komplexe Angriffsmethoden zurück. Vielmehr sind sie meist auf eine Abfolge einfacher Vorgänge zurückzuführen, die durch grundlegende Sicherheitsmaßnahmen, verhindert werden können, wie etwa risikobasiertes Schwachstellenmanagement."

Forrester Research, *The State of Vulnerability Risk Management, März 2023*

Die Angriffsfläche wächst unaufhaltsam, vorangetrieben durch die Zunahme der Schatten-IT, hybride Arbeitsumgebungen und Cloud-Nutzung. Die Netzwerk- und Sicherheitsteams, die ihre Unternehmen und deren wertvolle digitale Assets schützen müssen, können mit dem Tempo dieser Entwicklung kaum Schritt halten. Überholte Technologien, ungepatchte Sicherheitslücken und weniger „wichtige" IT-Assets werden oft übersehen, sind aber leichte Ziele. Angreifer nutzen diese Schwachpunkte, um in Netzwerke einzudringen und sich dann durch die Infrastruktur zu bewegen, um zu wertvolleren Zielen vorzudringen. Wenn sich die Teams zu sehr auf reaktive Sicherheitstools verlassen, die erst Alarm schlagen, wenn die Sicherheit bereits kompromittiert wurde, kann dies zu Ausfallzeiten führen, die durch proaktive Sicherheitskontrollen hätten verhindert werden können.

Unternehmen brauchen einen effektiveren Ansatz, um ihre Angriffsfläche zu verstehen und Sicherheitsprozesse zu entwickeln, die den Geschäftsbetrieb nicht beeinträchtigen und die Benutzer nicht behindern. Dazu benötigen die Teams Tools, die ihnen helfen, beim Asset- und

Nachweisbare Verbesserung der Risikosituation

- Vereinfachtes Cybersecurity Asset Management
- Umfassender Einblick in die Geräterisiken
- Klare, präzise Bewertung der Anfälligkeit von Geräten
- Schnellere Reaktion auf Vorfälle
- Proaktive Gestaltung von Sicherheitsrichtlinien
- Besserer Schutz von IoT und medizinischen Geräten

Risikomanagement proaktiv Prioritäten zu setzen, und zugleich den erforderlichen Kontext liefern, um Sicherheitsvorfälle entschärfen zu können.

Stärken Sie Ihre Netzwerksicherheit durch risikobasierte Priorisierung

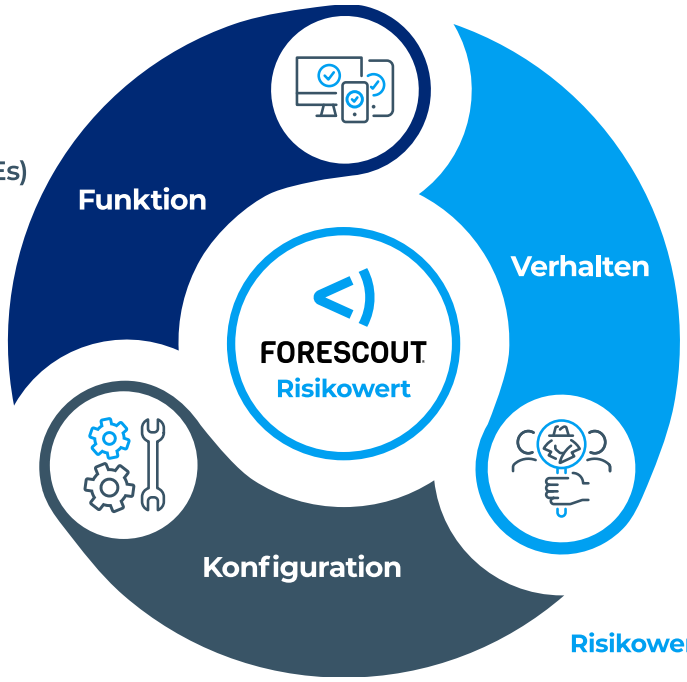
Sicherheitsteams, die mit der wachsenden Angriffsfläche und fehlendem Kontext aufgrund isolierter Tools zu kämpfen haben, erhalten mit Forescout Risk and Exposure Management ein umfassendes Asset Intelligence-Tool, das ihnen eine verlässliche Grundlage für das Verständnis der Sicherheitslage liefert. Die Lösung überwacht die Wirksamkeit der Maßnahmen im gesamten Security-Ökosystem, um Risiken und Anfälligkeiten zu reduzieren. Dabei verfolgt sie einen automatisierten, risikobasierten Ansatz zur Beseitigung von Schwachstellen.
The Forescout® Risk and Exposure Management befähigt Unternehmen, Risiken nicht nur zu erkennen, sondern auch zu verstehen. Die Sicherheitsteams können:

- Den betrieblichen Aufwand für das Cybersecurity Asset Management reduzieren
- Durch umfassende Ermittlung der Angriffsfläche die Cyber-Hygiene entscheidend verbessern
- Die Konfiguration und den Zustand jedes vernetzten Geräts verstehen und auf dieser Basis Risikograd und Ausnutzbarkeit präzise bewerten, klassifizieren und quantifizieren
- Den Nutzen bestehender Investitionen in Sicherheitstechnologien nachweisen und die Wirksamkeit von Kontrollmaßnahmen verfolgen, um die Risiken nach und nach zu reduzieren
- Die Untersuchung von Vorfällen beschleunigen und proaktive Richtlinien entwickeln, um weitere Vorfälle zu vermeiden

Konfiguration:
- Sicherheitslücken (CVEs)
- Ausnutzbarkeit (EPSS)
- Exponierte Dienste

Funktion:
- Gerätekritikalität

Verhalten:
- Erreichbarkeit aus dem Internet



$$\text{Risikowert} = f\left(\text{Erkannte Risiko-indikatoren}, \text{Geräte-kritikalität}\right)$$

Langfristig verfügbare Geräteinformationen plus Priorisierung von Cyber-Risiken

Forescout Risk and Exposure Management hilft Ihnen, Risiken durch Schwachstellen und Fehlkonfigurationen zu identifizieren, zu quantifizieren und zu priorisieren. Dazu wird für jedes Gerät ein eindeutiger Multifaktor-Risikowert errechnet, basierend auf der spezifischen Konfiguration, der Funktion und dem Verhalten des Geräts.

Identifizieren

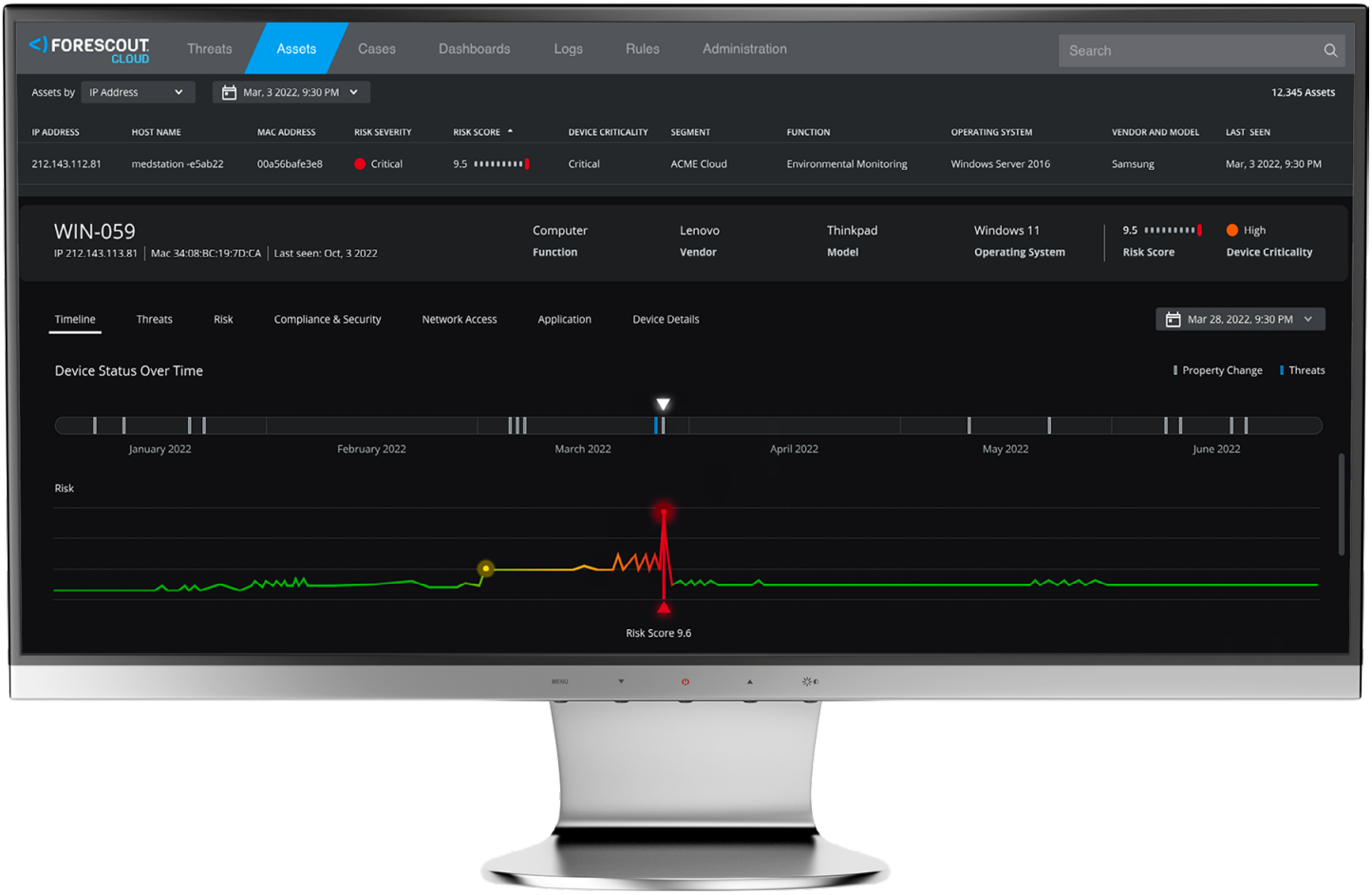
Optimiertes Cybersecurity Asset Management dank klarer, präziser Erkenntnisse zu jedem Gerät im Netzwerk

Profitieren Sie von einem langlebigen, präzisen Inventar mit historischen Verlaufsdaten zum Gerätestatus und zu Konfigurationsänderungen, gestützt auf eine cloudbasierte Klassifizierung der verwalteten und unverwalteten Geräte (IT, IoT, IoMT, OT/ICS).

Inventarisierung der Angriffsfläche – Zuverlässige, cloudbasierte Klassifizierung verwalteter und unverwalteter Geräte.

Persistente, kontextbezogene Gerätedaten – Durchsuchbar; 90 Tage Aufbewahrung und Nachverfolgung umfangreicher kontextbezogener Gerätedaten, einschließlich Status- und Konfigurationsänderungen.

Filterung von Anfälligkeitsprofilen – Erweiterte Filterfunktionen ermöglichen es, Geräte ausfindig zu machen und nachzuverfolgen, die bestimmte Anfälligkeitsmerkmale mit kompromittierten Geräten gemeinsam haben. So können Sie die Probleme proaktiv beheben.



Warum Forescout

1. Persistentes Inventar aller Gerätearten auf einer modernen Oberfläche
2. Eindeutiger Multifaktor-Risikowert, basierend auf Konfiguration, Funktion und Verhalten
3. Zuverlässige, cloudbasierte Klassifizierung
4. Patentierte Deep Packet Inspection-Technologie
5. Korrelation der Ausnutz-barkeit von Sicherheitslücken mit der Exponiertheit von Geräten
6. Integrationen mit führenden Sicherheitsprodukten und Möglichkeit, die Wirksamkeit zu überprüfen
7. Praktisch umsetzbare Erkenntnisse zu Risiken und Anfälligkeiten
8. Cloudbasierter Data Lake mit Informationen zu Risiken und Bedrohungen

Besuchen Sie [www.forescout.com,](http://www.forescout.com) um mehr über den Ansatz zu erfahren, den Forescout für das Risiko- und Exposure-Management verfolgt, und eine Demo anzufordern.

Quantifizieren

Umfassende Erkenntnisse zu den Cybersicherheitsrisiken

Verfolgen Sie kontinuierlich das Cybersicherheitsrisiko aller verbundenen Geräte, gestützt auf einen Multifaktor-Risikowert, der auf Konfiguration, Funktion und Verhalten basiert. So können Sie Ihr Netzwerk proaktiv schützen.

Konfiguration – Erfassung der spezifischen Konfigurations-anforderungen jedes Geräts, um festzustellen, ob es für Angreifer zugänglich ist und ausnutzbare Sicherheitslücken aufweist:

- Common Vulnerabilities and Exposures (CVEs), korreliert mit dem CISA-Katalog bekannter ausgenutzter Schwachstellen (KEVs)
- Exploit Prediction Scoring System (EPSS)
- Exponierte Dienste und offene Ports sowie potenzielle Gefährdung (Kontrolle oder Zugriff)

Funktion – Ermittlung und Bewertung der Kritikalität von Geräten, ausgehend von ihrer Funktion und Nutzung.
Verhalten – Verfolgung der Konfigurations- und Verhaltensänderungen bei jedem Gerät, um Anomalien zu erkennen, die das Risiko einer Kompromittierung erhöhen können, unter anderem durch Angreifer aus dem Internet.

Priorisieren

Schnellere Untersuchung von Vorfällen und Entwicklung proaktiver Abhilfemaßnahmen

Erleichtern Sie Ihren IT- und Sicherheitsteams den Zugang zu Echtzeit- und persistenten Bestandsdaten, um sie bei der proaktiven Risikominimierung und der Untersuchung von Vorfällen zu unterstützen.

Überall zugängliche Geräteinformationen – Das Forescout Cloud-Portal bietet allen IT- und Sicherheitsteams einfachen, verlässlichen Zugriff auf umfangreiche, kontextbezogene Informationen zu den Geräten.

Risikobasierte Priorisierung – Nutzen Sie Risiko- und Anfälligkeitsmerkmale in Kombination mit Informationen zum Compliance- und Konfigurationsstatus von Geräten, um die Untersuchung von Vorfällen und die Entwicklung von Abhilfemaßnahmen zu vereinfachen.

Historischer Gerätekontext – Beschleunigen Sie Risikoanalysen und die Reaktion auf Vorfälle, um den Wirkungsradius von Angriffen zu minimieren und die mittlere Reparaturzeit (MTTR) zu verkürzen.

FORESCOUT®

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