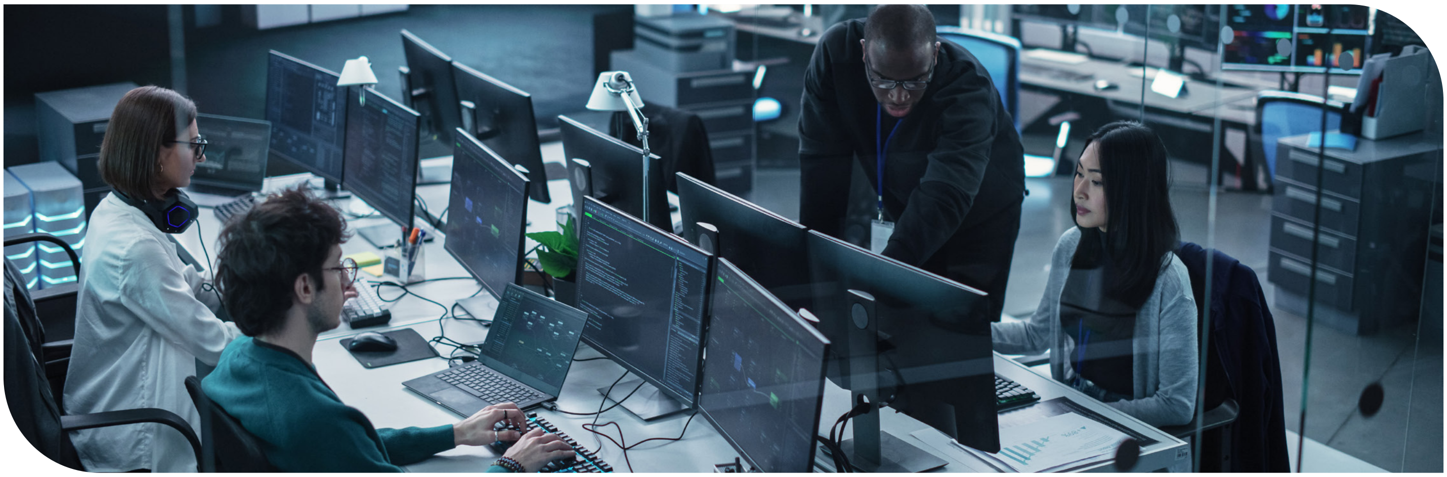
FORESCOUT®

Forescout® Risk and Exposure Management

Enhance your network security posture with risk-based prioritization



Overwhelmed by rapid asset growth and a widening attack surface, cybersecurity teams struggle to contextualize information from multiple siloed security tools. Organizations need a simplified way to maintain real-time and persistent asset intelligence for every device – managed or unmanaged, physical or virtual, including operational technology and industrial control systems (OT/ICS), Internet of Things (IoT) devices and specialty subsets like medical devices. Without this capability, organizations face high operational overhead, performance issues, downtime, and risk of security breaches due to weakness in their security posture, caused by lack of asset intelligence.

As an existing Forescout customer, you already benefit from 100% real-time visibility of all devices across your enterprise through Forescout eyeSight, and leverage the power of our centralized policy engine in Forescout eyeControl for workflow automation to help govern your network.

Forescout Risk and Exposure Management is an all-new cloud-powered solution designed to further enhance your network security posture by leveraging the rich, contextual device data in your on-prem eyeSight deployment and sharing it with the Forescout Cloud Platform. The information will be stored in the Forescout Cloud data lake for 90 days for persistent visibility and analysis by your security teams. It will also be correlated in the cloud to calculate a unique **multifactor risk score** for each device. Rather than focusing on a single viewpoint, the Forescout Risk score quantifies risk factors across configuration, function and behavior to help provide a true picture of the exposure gaps in your attack surface.

Risk-based prioritization can be used to:

- Drive remediation and response policy actions through eyeControl
- Help prove a reduction in security risk posture
- Help you better align to your compliance framework

Combining real-time and persistent device context in the Forescout Cloud will also enhance operational efficiencies. With the expanded availability of asset intelligence, you're able to track configuration changes over time and their impact on risk posture. This increased awareness can then be used for both proactive risk remediation and reactive incident investigation. The result? Streamlined design and implementation of security frameworks and reduced operational overhead of attack surface management.

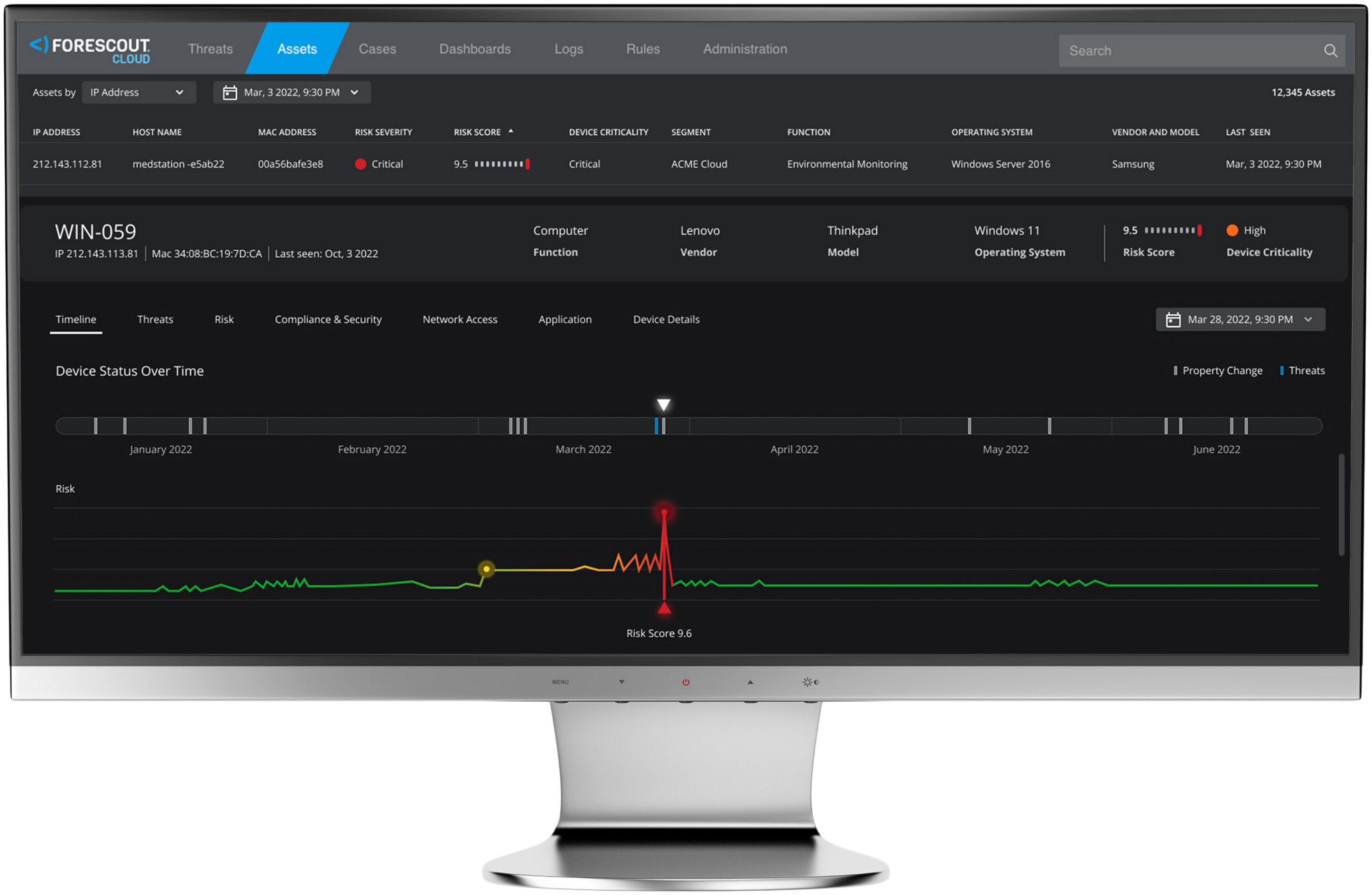
Business value and outcomes

- Reduced risk of a breach or incident due to visibility gaps, weaknesses in your attack surface and exposed vulnerabilities in both managed and unmanaged assets
- Proactive risk remediation and reactive incident investigation fueled by the rich contextual information stored in the Forescout Cloud data lake
- Streamlined design and implementation of your security framework
- Reduced operational overhead for attack surface management

Enhance asset management

Identifying new assets and auditing their configuration to keep your asset inventory up-to-date doesn't have to be time intensive. The Forescout Device Cloud is one of the world's largest repositories of connected enterprise device data, containing 39+ billion data points from 18+ million devices. It provides an accurate classification system for both managed and unmanaged assets.

- Classify and inventory all connected assets automatically, and retain their state information for 90 days.
- Ensure all IP-connected devices across your network are found without using agents – and without causing disruption to business operations.
- Track configuration changes and fluctuations in security posture across your entire attack surface using both real-time and persistent asset intelligence – continuously as devices connect and throughout their lifecycle, to power business processes and drive digital transformation.



Assets by IP Address

Mar, 3 2022, 9:30 PM

12,345 Assets

IP ADDRESS	HOST NAME	MAC ADDRESS	RISK SEVERITY	RISK SCORE	DEVICE CRITICALITY	SEGMENT	FUNCTION	OPERATING SYSTEM	VENDOR AND MODEL	LAST SEEN
212.143.112.81	medstation -e5ab22	00a56bafe3e8	● Critical	9.5	Critical	ACME Cloud	Environmental Monitoring	Windows Server 2016	Samsung	Mar, 3 2022, 9:30 PM

WIN-059

IP 212.143.113.81 | Mac 34:08:BC:19:7D:CA | Last seen: Oct, 3 2022

Function	Vendor	Model	Operating System	Risk Score	Device Criticality
Computer	Lenovo	Thinkpad	Windows 11	9.5	● High

Real-time and persistent asset context and security risk score

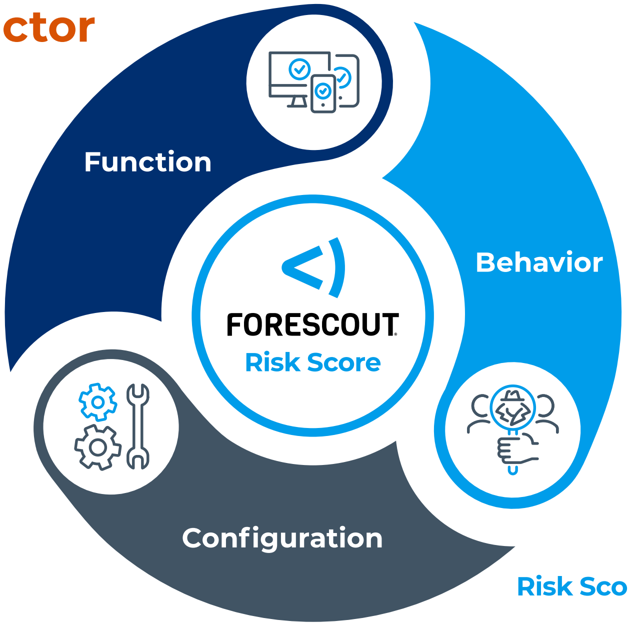
Identify exposure and quantify risk

Safeguard your network by first understanding the attack surface and then considering the unique, multifactor risk score calculated for each asset based on configuration, function and behavior that helps quantify Its exposure and risk posture.

- Understand the unique configuration requirements of each asset to identify its exposure and the exploitability of its vulnerabilities – combine information from the Cybersecurity and Infrastructure Security Agency (CISA) and Exploit Prediction Scoring System (EPSS) – to pinpoint which assets need remediation.
- Determine device criticality as a key factor for function to provide additional context (such as FDA class and recall information for medical devices).
- Track configuration and behavior changes for each asset to detect anomalies that may increase risk of compromise, such as internet exposure.

Forescout Multifactor Risk Score

- **Configuration:**
  - Vulnerabilities (CVE's)
  - Exploitability (EPSS)
  - Exposed Services
- **Function:**
  - Device Criticality
- **Behavior:**
  - Internet Exposure



Risk Score = f (Detected Risk Indicators , Device Criticality)

Increase operational efficiency

Forescout Risk and Exposure Management helps reduce operational overhead by leveraging rich, real-time and persistent contextual device data to accelerate incident investigation and root cause analysis.

- Proactively identify high-risk assets and exposure gaps to formulate and then automate remediation processes.
- Analyze your return on investment for third-party security tools by tracking the effectiveness of your security measures and tools, and their ability to reduce your security risk.

Why Forescout?

Unlike other security solutions that fail to deliver real-time, actionable asset intelligence and cannot assess compliance without installing an agent, our solution offers diverse discovery techniques that provide complete asset visibility and agentless assessment.

Forescout's Risk and Exposure Management solution is a comprehensive asset intelligence tool that provides the foundation for understanding the security posture of your attack surface and yields a greater return on investment across your security ecosystem, by tracking the effectiveness of response actions to reduce your risk posture and exposure state, through an automated risk-based remediation approach to your asset vulnerabilities.

Benefits and Use Cases

Cybersecurity asset management

Discover and classify every device across any environment (90 days retention) to help IT security teams leverage asset context and status trends to streamline their operations.

Asset risk intelligence

Gain situational awareness of cybersecurity risk posture based on exposure from vulnerabilities and misconfiguration with a unique multifactor risk score.

Accelerated incident response

Leverage historical asset context to aid analysts' proactive investigation of risks and reactive response to incidents and events to help minimize the blast radius and reduce mean-time-to-resolution (MTTR).

Enhanced IoT security

Leverage high-fidelity IoT classification through non-disruptive, passive discovery techniques for deployment flexibility, with real-time identification of xIoT vulnerabilities to help security teams understand the attack surface and prioritize response actions.

Medical device security

Clear and concise risk assessment of each connected medical device based on known exposures, attack potential and operational criticality, with insights into FDA class and recall status, to help ensure security without impacting patient care.

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