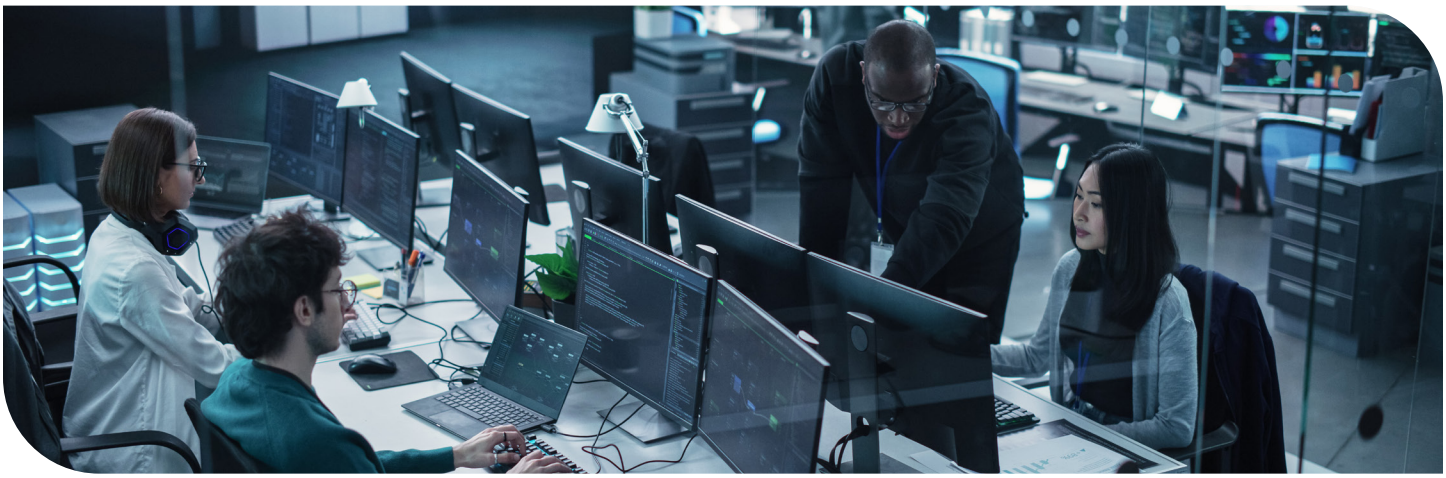
Risk and Exposure Management

Identify, Quantify and Prioritize Risk and Compliance



"Rarely are breaches due to sophisticated attacks involving nation-states or complex attack methods. Instead, most involve chains of simple procedures that can be prevented by applying security fundamentals like vulnerability risk management."

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

The attack surface is expanding, driven by the growth of shadow IT, hybrid work environments and cloud adoption. The rate of expansion continues to outpace network and security teams' ability to safeguard organizations and their high-value digital assets. Obsolete technology, unpatched vulnerabilities and other "low-value" IT assets are often forgotten but make for easy targets. Malicious actors leverage these weak points to compromise the network and spread laterally to higher-value assets. Overreliance on reactive security tools to alert when threats or breaches have already occurred can lead to downtime that could have been prevented with proactive security controls.

Organizations need a better way to understand the state of their attack surface and design security processes that don't impact business operations or cause user friction. They need tools that help them proactively prioritize asset and risk management while also providing the context necessary to implement response and remediation actions when incidents occur.

Prove a reduction in risk posture over time

- Streamlined cybersecurity asset management
- Comprehensive asset risk intelligence
- Clear and concise assessment of asset exposure
- Accelerated incident response
- Proactive security policy design
- Enhanced IoT and medical device securityof your security framework

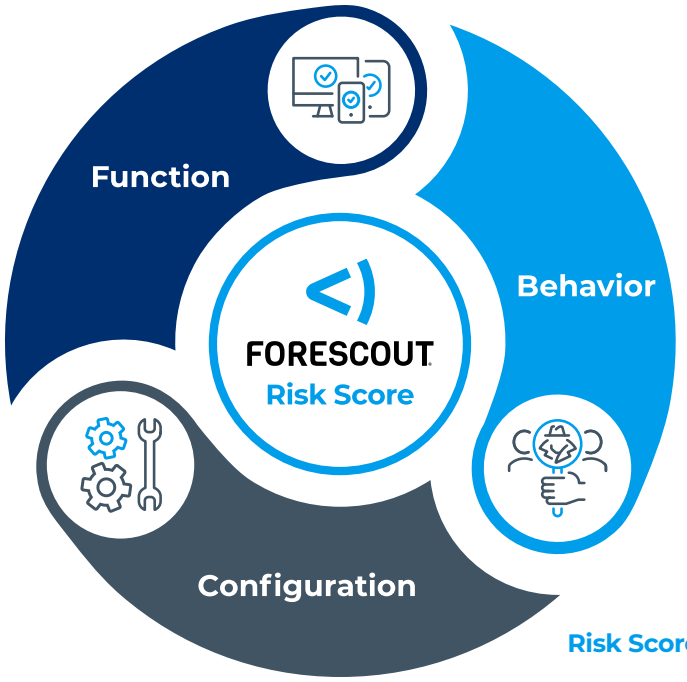
Enhance your network security posture with risk-based prioritization

For cybersecurity teams overwhelmed by their widening attack surface and struggling to contextualize information from siloed security tools, 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. It tracks the effectiveness of response actions across your security ecosystem to reduce your risk posture and exposure state, using an automated risk-based approach to remediate vulnerabilities.

The Forescout® Risk & Exposure Management solution helps organizations move beyond visibility to understanding by enabling them to:

- Reduce operational overhead for cybersecurity asset management
- Attain a new level of cybersecurity hygiene by identifying attack surface exposure
- Accurately assess, classify and quantify the risk severity and exploitability of every connected asset by understanding its configuration and state
- Prove the value of existing security investments and track the effectiveness of control actions to reduce risk over time
- Reduce the time spent investigating incidents and designing proactive response policies to prevent future incidents

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



$$\text{Risk Score} = f\left(\text{Detected Risk Indicators}, \text{Device Criticality}\right)$$

Combine persistent asset intelligence with cybersecurity risk prioritization

Forescout Risk & Exposure Management helps you identify, quantify and prioritize risk based on exposure from vulnerabilities and misconfiguration. A unique multifactor risk score correlates factors across each asset's configuration, function and behavior.

Identify

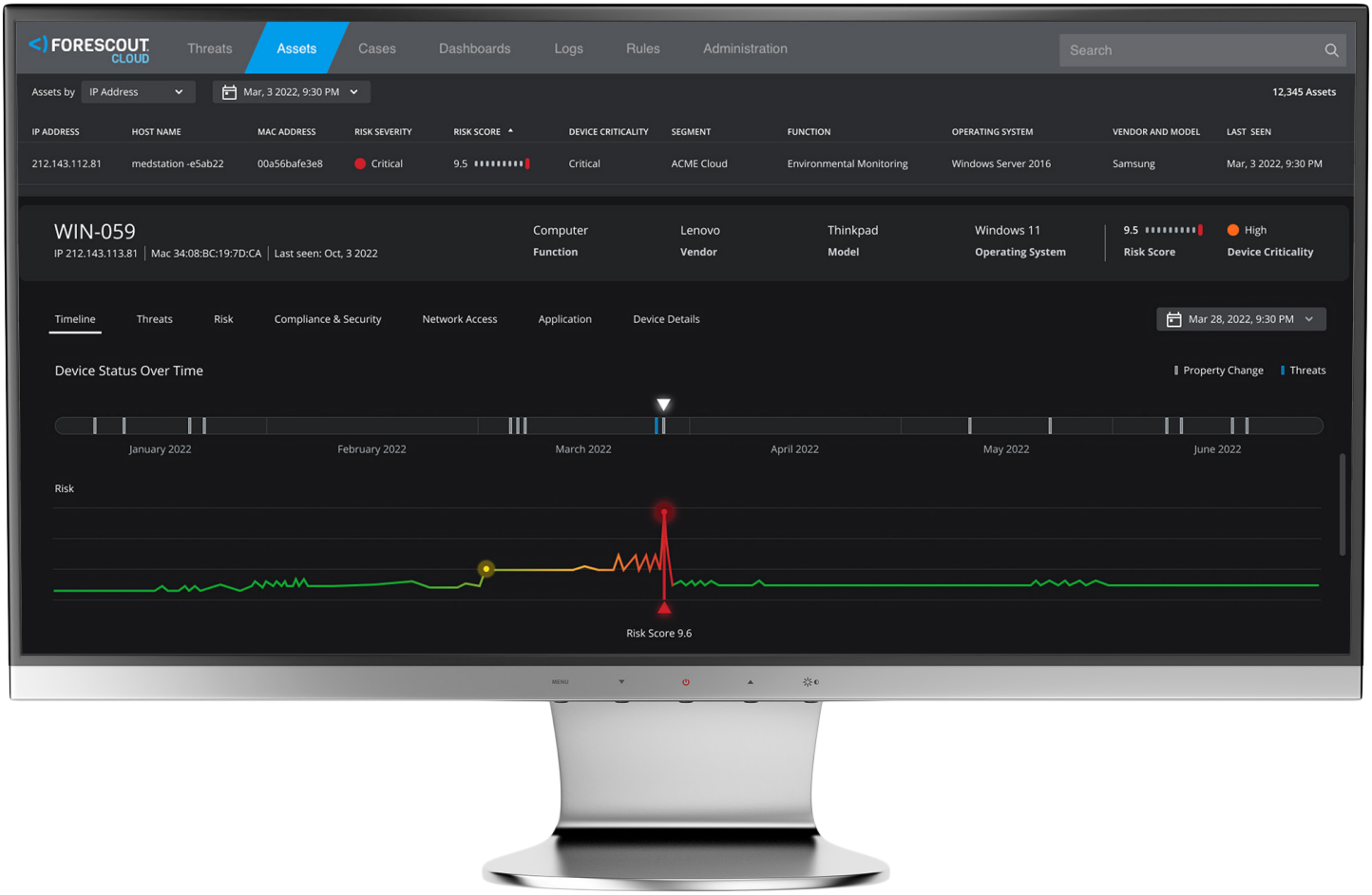
Streamlined cybersecurity asset management with clear and concise intelligence for every connected asset

Achieve a persistent and accurate asset inventory with historical tracking of device status and configuration changes using cloud-powered classification for both managed and unmanaged devices (IT, IoT, IoMT, OT/ICS).

Attack surface asset inventory – High-fidelity, cloud-powered classification of managed and unmanaged devices.

Persistent asset context – Searchable 90-day retention and tracking of rich contextual asset data, including state and configuration changes.

Exposure profile filtering – Advanced filtering capabilities to help locate and track assets that share common exposure attributes with compromised assets so you can proactively remediate them.



Why Forescout

1. Modern asset view of persistent inventory of all device types
2. Unique multifactor risk score based on configuration, function and behavior
3. High-fidelity cloud classification
4. Patented deep packet inspection technology
5. Correlation of vulnerability exploitability and asset exposure
6. Integrations with leading security products and ability to track effectiveness
7. Actionable risk and exposure insights for response actions
8. Cloud data lake of risk and threat intelligence

Visit www.forescout.com to learn more about Forescout's approach to risk and exposure management and request a demo.

Quantify

Comprehensive cybersecurity risk intelligence

Proactively safeguard the network and continuously track the cybersecurity risk posture of all connected devices by calculating a multifactor risk score based on configuration, function and behavior.

Configuration – Capture the unique configuration requirements of each asset to identify its exposure and the exploitability of its vulnerabilities, including:

- Common Vulnerabilities and Exposures (CVEs) correlated to the CISA Known Exploited Vulnerabilities (KEVs) catalog
- Exploit Prediction Scoring System (EPSS)
- Exposed services and open ports, and potential exposure (control or access)

Function – Understand and classify device criticality based on function and use.

Behavior – Track the configuration and behavior changes of each asset to detect anomalies that may increase risk of compromise, including internet exposure.

Prioritize

Spend less time investigating incidents and designing proactive remediation policies

Expand the availability of real-time and persistent asset data across IT and security teams to aid proactive remediation of risks and reactive investigation of incidents.

Access-anywhere asset intelligence – The Forescout Cloud portal provides greater availability and ease of access to rich, contextual asset intelligence across all IT and security teams.

Risk-based prioritization – Leverage risk and exposure attributes combined with asset compliance and configuration state intelligence to aid incident investigation and the design of remediation workflows.

Historical asset context – Accelerate risk analysis and incident response to help minimize the blast radius and reduce mean-time-to-resolution (MTTR).

FORESCOUT

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