SOLUTION BRIEF

Forescout eyeFocus

Navigate Uncertainty Confidently: Strategize, Mitigate and Succeed

FORESCOUT

Forescout eyeFocus

Organizations are seeking 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.

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 high-value digital assets. Obsolete technology, unpatched vulnerabilities and weak postures 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.

"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

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® eyeFocus is a comprehensive asset intelligence tool that provides the foundation for understanding the security posture of your attack surface. Empowered by an AI-driven engine, it tracks the effectiveness of response actions across the security ecosystem to reduce your risk posture and exposure state using an automated risk- based approach to remediate vulnerabilities.

The Forescout eyeFocus 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

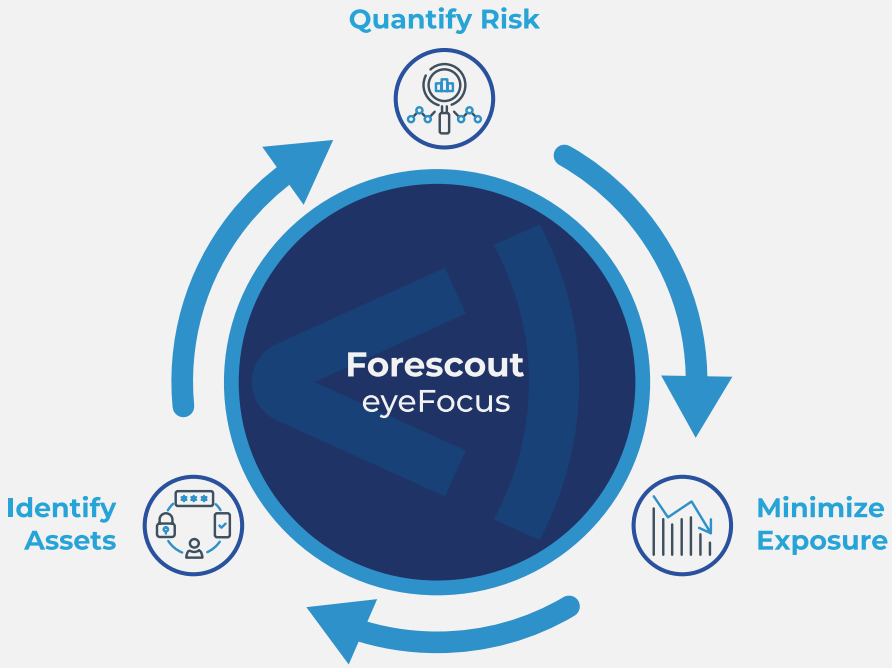
Why Forescout

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

The Forescout eyeFocus framework revolves around three pivotal components: identification of assets, quantification of risk, and minimization of exposure.

This holistic approach begins with the meticulous identification and cataloging of assets, providing a crucial understanding of the vulnerability landscape. The platform then employs sophisticated AI-powered risk quantification techniques, offering insightful analytics to assess and prioritize potential threats.

Finally, it minimizes exposure through proactive measures and control, ensuring vulnerabilities are addressed effectively.



Identify Assets

Continuously identify all devices, managed and unmanaged, and their exposure attributes to achieve real-time awareness of the attack surface

Asset visibility serves as a cornerstone in safeguarding digital environments, empowering security professionals to gain a comprehensive understanding of the organization's attack surface. Forescout eyeFocus meticulously identifies and classifies all network-connected devices, including traditional managed IT assets and even unmanaged devices such as OT and IoT devices. This insight is pivotal in identifying potential vulnerabilities and assessing the overall risk landscape, providing cybersecurity teams with the necessary foundation to develop proactive defense measures.

Your cybersecurity team can use Forescout to:

Discover every asset: Leverage passive monitoring and active scanning techniques to maintain a real- time inventory of all connected network devices, including IT, OT, IoT and IoMT.

Classify assets: Automate high-fidelity classification of assets based on 150+ attributes and employ advanced filtering capabilities to locate and track assets with shared attributes.

Navigate historical data: Query, investigate and analyze contextual asset data over a 90-day timeline to establish historical compliance and identify potential risks and gaps.

Quantify Risk

Identify, assess, and prioritize risks in a meaningful way to empower better security and business decisions

Forescout utilizes advanced AI-driven risk assessment methodologies to thoroughly examine vulnerabilities, identify potential threat vectors, and assess the possible consequences of cyber threats. Through continuous monitoring and employing sophisticated algorithms, Forescout eyeFocus quantifies and prioritizes potential risks through numerical values, enabling a clear and data driven understanding of cyber threats. This quantitative approach empowers organizations to optimize resource allocation for addressing the most substantial threats, implement targeted and proactive security measures, and develop robust risk mitigation strategies. Cybersecurity teams can leverage Forescout to:

Identify risk: Utilize diverse methods from agent-based to agentless to detect vulnerabilities and policy compliance across all connected managed and unmanaged devices.

Assess risk: Analyze the vulnerability and exploitability of connected assets, considering factors like misconfigurations, open ports, and irregular activity.

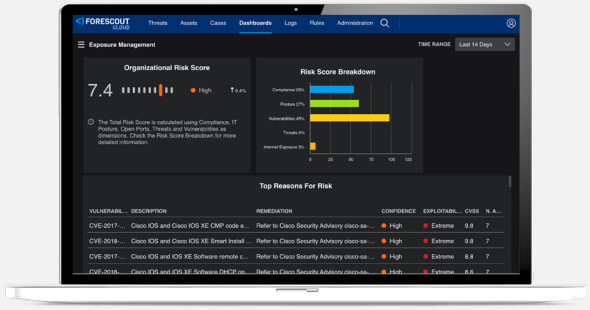
Monitor risk: Continuously monitor essential mission-critical business functions, identify the risks to which these resources are exposed, define the potential impact of an attack, and determine the likelihood of that attack occurring.

Minimize Exposure

Enhance the organization's risk posture with recommended remediation actions to ensure adherence to compliance standards

Minimizing the attack surface against potential threats empowers organizations to enhance their security posture, mitigate financial and reputational damages, and improve ROI through resource allocation in the most cost-effective manner Cybersecurity teams can utilize Forescout to:

Prioritize Risk: Evaluate and rank potential risks at the device or organizational level to determine effective allocation of resources and mitigation strategies.



Implement mitigation plans: Enable security teams to reduce risk exposure by constructing remediation and risk mitigation workflows based on recommended actions.

Track return on investment: Review the historical overall organizational risk posture to make informed decisions on optimizing cybersecurity investments.

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