FORESCOUT®

Forescout eyeSentry

Continuously Evaluate the Accessibility, Exposure, and Exploitability of Your Digital and Physical Assets

THE CHALLENGE

Modern digital environments are dynamic, complex, and under constant threat. Traditional security solutions can't keep up with evolving attack surfaces and sophisticated threats. With 13 cyber attacks every second, the volume of threat noise is overwhelming. Your cybersecurity team is drowning in daily alerts that lack context or accuracy. This leads to fatigue, burnout, and critical threats slipping through the cracks.

You need streamlined, real-time asset intelligence across all device types — managed, unmanaged, physical, virtual, IoT, and medical devices. Without it, you face high operational overhead, degraded performance, and critical vulnerabilities from visibility gaps.

THE SOLUTION

Forescout eyeSentry continuously identifies, assesses, and reduces cyber risk across every connected asset. Unlike traditional vulnerability management tools that focus on known CVEs, eyeSentry provides real-time visibility into your full attack surface. It factors in asset criticality, active exploits, misconfigurations, and business impact. eyeSentry also tracks Internet of Things (IoT) devices, and specialized assets, such as medical devices.

This new, cloud-powered solution provides rich, contextual device data automatically and retains state information for 90 days. The Forescout Device Cloud one of the largest repositories with over 39+ billion data points from 18+ million devices, delivering accurate classification for both managed and unmanaged assets.

eyeSentry identifies all IP-connected devices without agents or business disruption. You can track configuration changes and security posture fluctuations across your attack surface continuously.

KEY CAPABILITIES

Identify Exposure and Quantify Risk

Powered by an AI-driven engine, eyeSentry continuously monitors the effectiveness of response actions across your security ecosystem, using an automated, risk-based approach to remediate vulnerabilities and reduce overall risk exposure. eyeSentry automatically calculates a unique multifactor risk score for each discovered device. This score spans configuration, function, and behavior to reveal exposure gaps in your attack surface. Use risk-based prioritization to drive remediation, prove risk reduction, and align with compliance frameworks.

USE CASES:

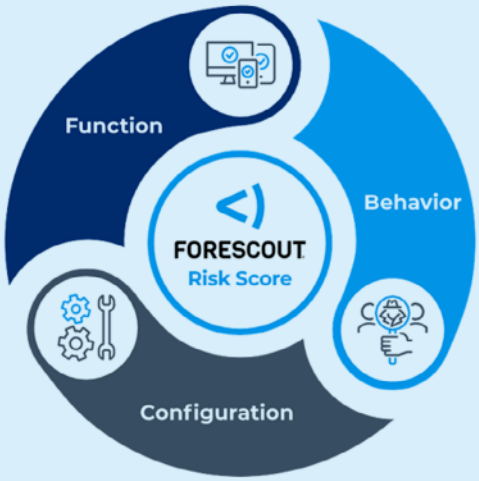
- **Asset Management**
  Discover and classify every device across any environment with 90-day retention.
- **Risk Intelligence**
  Gain situational awareness with multifactor risk scoring based on vulnerabilities and misconfigurations.
- **Real-Time Monitoring**
  Continuously monitor for vulnerabilities with prioritization based on exploitability and business impact.
- **Threat-Centric Management**
  Focus on exposures that are accessible, valuable, and under active threat through integrated intelligence.
- **Incident Response**
  Leverage historical context to minimize blast radius and reduce mean time to resolution.
- **Compliance Support**
  Provide continuous evidence of security posture for regulated industries adopting CDM and Zero Trust frameworks.

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)

eyeSentry reduces operational overhead by streamlining the identification and monitoring of all connected assets. It enables organizations to achieve a higher level of cybersecurity hygiene by identifying exposures and providing deep insights into each asset's configuration and state. This allows for accurate assessment, classification, and quantification of risk severity and exploitability.

Additionally, you can track the effectiveness of control actions in reducing risk over time. By automating key processes, eyeSentry reduces the time spent investigating incidents and supports the design of proactive response policies to prevent future threats.

IDENTIFY ASSETS

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

Comprehensive network asset visibility is essential for effective cybersecurity. Without a clear, real-time inventory of all assets, organizations are left with blind spots that can be exploited by threat actors. Asset visibility enables security teams to identify unmanaged or unauthorized systems, prioritize vulnerabilities based on business impact, and reduce the overall attack surface by eliminating shadow IT and misconfigured assets. It also ensures that security controls are properly deployed across the entire environment, enabling faster threat detection, response, and continuous validation of security posture. Providing comprehensive visibility enables organizations to implement proactive defense strategies effectively, allowing for ongoing identification and mitigation of risks while maintaining readiness against emerging threats. Cybersecurity teams can utilize 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, 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

Quantifying the risk of discovered assets is essential for turning visibility into actionable security intelligence. Forescout utilizes advanced AI-driven risk assessment methodologies to thoroughly examine vulnerabilities, identify potential threat vectors, and assess the possible consequences of cyber threats. By assigning risk levels based on these factors, organizations can prioritize remediation efforts on the assets that matter most. This risk-based approach helps security teams make smarter decisions, align with business objectives, and reduce overall threat exposure more efficiently. It also enables measurable improvements in security posture and supports compliance reporting for faster, more effective threat mitigation. Cybersecurity teams can utilize 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.

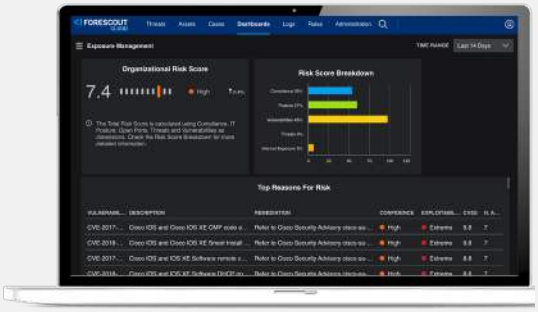
Monitor risk: Continuously monitor essential mission-critical business functions, identify the risks to which these resources are exposed, define the potential impact of an attack, and determine the likelihood of that attack occurring.

MINIMIZE EXPOSURE

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

Providing recommended remediation actions for high-risk assets enables organizations to reduce cybersecurity exposure quickly and efficiently by focusing efforts where they matter most. Instead of attempting to address every vulnerability, security teams can prioritize fixes for assets that pose the greatest risk based on exploitability, business impact, and exposure. Clear, actionable remediation guidance accelerates response times and ensures resources are used effectively. This targeted approach significantly reduces the attack surface and strengthens overall security posture, helping to 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.

OVERALL BUSINESS VALUE

Executive Communication

Translate cyber risk into business terms with dashboards and AI reporting for stakeholder communication.

Enhanced Visibility

Get real-time risk assessment with contextual scoring. Focus resources on what matters most to your business.

Cost Optimization

Prioritize remediation based on actual business risk. Avoid devastating breach costs through early threat detection.

Compliance Ready

Support NIST, ISO 27001, and GDPR frameworks. Simplify audits with generative AI reporting and exposure visibility.

Rapid Response

Adapt to evolving threats with integrated detection and intelligence. Ensure defenses work as expected through continuous validation.

Proactive Security

Move from reactive to continuous assessment. Identify and mitigate risks before exploitation while reducing attack surface pathways.

WHY CHOOSE FORESCOUT

The Forescout 4D Platform™ provides complete asset intelligence and control across IT, OT, IoT, and IoMT environments. For more than 20 years, Fortune 100 organizations, government agencies, and large enterprises have trusted Forescout as their foundation to manage cyber risk, ensure compliance, and mitigate threats with seamless context sharing and orchestration across more than 180 fully featured security and IT product integrations. With Forescout, every cybersecurity investment is more effective.

Learn more at forescout.com.

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