FORESCOUT

The Forescout Platform

A Comprehensive Overview, Including Risk, Exposure, Segmentation and Threat Detection Management

INTRODUCTION

In today's rapidly evolving digital landscape, ensuring the security of a company's network infrastructure is more important than ever. With the rise of connected devices, IoT, and complex cloud environments, visibility and control over network assets have become increasingly challenging. This is where the **Forescout Platform** comes into play.

Forescout helps businesses secure their networks against modern threats with on-prem product solutions like eyeSight, eyeInspect, and eyeExtend, delivering visibility, control, and orchestration across diverse digital ecosystems. Use cloud services with Forescout **eyeFocus** and **eyeAlert**, which provide secure risk assessment and advanced threat detection for cyber assets connected to the network.

The products that comprise the Forescout Platform include:

eyeSight:
enterprise visibility, compliance assurance and policy engine for IT cyber assets

eyeControl:
enforcement capability

eyeInspect:
complete OT and IoT device visibility, risk, vulnerability and threat solution

eyeExtend:
3rd party bi-directional integrations for ITSM, VA, EMM/EDR, NGFW, SBOM, PAM and SIEM (among others) solutions

eyeFocus:
cloud-based attack surface and exposure management capability

eyeAlert:
next-gen SIEM providing a multi-stage detection capability

eyeSegment:
visualization of and policy creation/monitoring of segmentation rules

THE SUM IS GREATER THAN THE PARTS

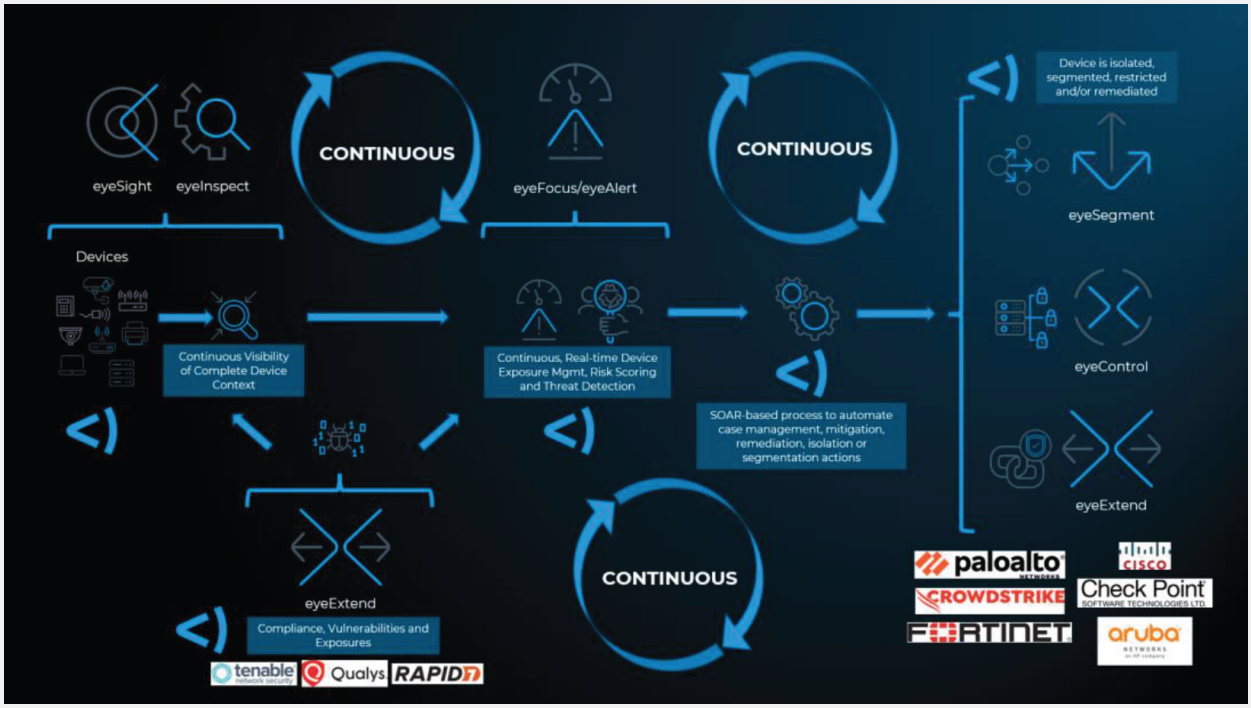
Forescout stands out in the market due to its agentless approach and its ability to provide comprehensive visibility across IT, IoT, OT, and IoMT environments. With Forescout risk and exposure management and enhanced threat detection and response solutions, the platform delivers an all-encompassing security solution that helps organizations proactively manage risk and mitigate threats in real-time.

The Platform provides a variety of capabilities, including:

- **Visibility**: through a variety of mechanisms Forescout agentlessly and continuously discovers all devices and correlates context on the user, network, posture and compliance.
- **Assessment of Posture/Risk/Vulnerabilities/Threats**: Forescout ingests and amalgamates data regarding the device's posture, it's associated risks and detected vulnerabilities.
- **Prioritization**: Forescout helps prioritize the devices that need to be acted upon with the most urgency due to risks, vulnerabilities, exposures or threats.
- **Remediation**: Forescout can automatically remediate devices, either directly via script execution or via a 3rd party integration for patching or configuration changes.
- **Orchestration**: Forescout can integrate with hundreds of 3rd party cybersecurity, monitoring and management tools. These bi-directional integrations can empower multiple use cases including asset management, vulnerability scanning and network segmentation.
- **Mitigation/Isolation/Restriction/Segmentation**: Through native integration into the network fabric, Forescout can automate mitigation of the risks posed by the devices, via device isolation/restriction or segmentation.

A DAY IN THE LIFE OF A DEVICE

To describe the capabilities of the platform, below is a graphic outlining the various products of the Forescout Platform and their associated capabilities.



1. The device appears on the network and can be authenticated by Forescout prior to gaining network access.
2. The device is then classified and categorized before it is analyzed for compliance and is possibly remediated/isolated/segmented or restricted post-analysis.
3. Alternatively, an OT device appears on the network (where possible and permitted, see #1).
4. For all devices, their Communications Flows (source→destination) overlay onto a contextual view of the discovered and categorized devices.
5. All device vulnerabilities, exposures and risks are then amalgamated which results in a dynamic device risk score enabling the prioritization of response actions against the riskiest devices.
6. Continuous monitoring and ingestion of 100's of log and telemetry sources enable robust and accurate detection of threats targeting the previously discovered devices.
7. The device risk score and other properties including detected threats enable SOAR-powered actions, policy-based actions or even actions performed by integrated third-party solutions.
8. The device is automatically isolated/remediated and/or it's traffic is segmented.
9. The risk the device poses the organization mitigated.

PRODUCTS COMPRISING FORESCOUT PLATFORM

Let's dive into the key components that make this platform a leader in continuous asset protection and understand what whole platform solution can provide.

1. FORESCOUT EYESIGHT: REAL-TIME ASSET VISIBILITY

One of the primary challenges that organizations face is keeping track of the devices that connect to their networks. Whether these are IT, IoT, IoMT or OT, unmanaged and unknown devices can pose a serious security threat.

Forescout's eyeSight provides complete, real-time visibility into all devices across an organization's extended enterprise.

Key Features:

- Passive network monitoring with real-time device discovery.
- Agentless operation, meaning no software installation is required on endpoints.
- Comprehensive asset intelligence, including device type, operating system, and software details.

You can't secure what you can't see. Forescout eyeSight ensures visibility for all devices, whether they are on or off-premises.

2. FORESCOUT EYECONTROL: DEVICE CONTROL AND ENFORCEMENT

Once an organization has visibility into the devices on its network, the next step is to establish control over them. eyeControl provides policy-based automation that allows IT and security teams to enforce compliance and security standards across their entire network.

Key Features:

- Automate network access control based on security posture.
- Quarantine, block, or limit device access if they fail to meet security requirements.
- Orchestrate remediation steps, like patching or software updates, for non-compliant devices.

Respond swiftly to security incidents, enforcing policies without interrupting business operations with eyeControl.

3. FORESCOUT EYESEGMENT: NETWORK SEGMENTATION

Segmentation involves isolating sensitive assets and restricting access to them to help reduce the attack surface and limit the impact of potential breaches. eyeSegment provides the tools to design, implement, and manage network segmentation policies efficiently.

Key Features:

- Micro and macro-segmentation capabilities for greater control over traffic flows.
- Visual mapping of device communications and traffic patterns.
- Policy-based segmentation, reducing manual intervention and configuration errors.

Ensure that sensitive data remains protected and reduce lateral movement within the network with eyeSegment.

4. FORESCOUT EYEEXTEND: ECOSYSTEM INTEGRATION AND ORCHESTRATION

Security infrastructures are made up of a variety of tools and platforms. Ensuring seamless integration between them is essential for an efficient and cohesive security strategy. eyeExtend offers pre-built integrations with leading IT, security, and operational technology systems.

Key Features:

- Connects Forescout with IT Service Management platforms, next generation firewalls (NGFWs), security information and event management tools (SIEMs), endpoint detection tools, and vulnerability management platforms.
- Orchestrates workflows between security tools for faster incident response.
- Extends Forescout's capabilities into cloud, OT, and third-party platforms.

Maximize existing security investments while ensuring a unified and orchestrated defense system with Forescout ecosystem integrations.

5. FORESCOUT EYEINSPECT: OT/ICS SECURITY

The security challenges facing operational technology (OT) and industrial control systems (ICS) are unique. These environments often run on legacy systems with limited or no native security capabilities. eyeInspect is specifically designed to offer real-time visibility and security for OT/ICS environments.

Key Features:

- Passive monitoring of OT networks, ensuring no disruption to operations.
- Threat detection and anomaly identification based on OT-specific protocols.
- Full asset visibility for both IT and OT environments.

With eyeInspect, organizations can protect critical infrastructure, ensuring that industrial processes remain secure and operational.

6. FORESCOUT EYEFOCUS

As cyber threats grow more sophisticated, organizations must have the tools to assess risk and manage exposure before attackers exploit vulnerabilities. Forescout eyeFocus provides a proactive approach to identifying, prioritizing, and remediating risks based on exposure across the entire digital infrastructure.

Key Features:

- **Automated Risk Scoring**: eyeFocus continuously assesses devices' risk scores based on vulnerabilities, configuration errors, and other threat vectors.
- **Prioritization**: Devices are prioritized based on their risk, ensuring that the most critical threats are addressed first.
- **Actionable Insights**: eyeFocus integrates with other Forescout modules to recommend and, if needed, automatically remediate exposed devices.

Significantly reduce the window of opportunity for attackers, improving overall security posture with eyeFocus.

7. FORESCOUT EYEALERT

Modern cyber-attacks can evade traditional defenses, making detection and response complicated at best. Forescout eyeAlert ensures that threats are detected early and the right actions are taken to contain and neutralize them.

Key Features:

- **Behavioral Analytics**: eyeAlert uses machine learning and advanced analytics to detect suspicious behavior patterns across devices and the network.
- **Threat Intelligence Integration**: Integrates with global threat intelligence feeds to identify and respond to emerging threats quickly.
- **Automated Incident Response**: When a threat is detected, eyeAlert works with eyeControl to quarantine infected devices, enforce segmentation, or trigger automated responses.

Reduce the mean time to detect (MTTD) and respond (MTTR) to cyber incidents, ensuring minimal damage and disruption to business operations with eyeAlert.

ABOUT FORESCOUT

Forescout Technologies, Inc., a global cybersecurity leader, continuously identifies, protects and helps ensure the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide vendor-agnostic, automated cybersecurity at scale. The Forescout Platform delivers comprehensive capabilities for network security, risk and exposure management, and threat detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats.

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