SOLUTION BRIEF

The Forescout 4D Platform™ Solution Brief

The Forescout 4D Platform™ Solution Brief

Networks used to be simpler and much easier to lock down with perimeter security defenses. However, the advancement and adoption of new business models and supporting technologies has brought more and more devices on-line, requiring the network to open up.

Growth in IoT devices is forecasted to grow from 14 billion in 2023 to 25 billion by 2030. As the attack surface gets larger, it's creating bigger gaps, enormous blind spots, and infinitely more duplicates and conflicts that cannot be easily resolved. As the size of the attack surface increases, the risk of a cyber-attack has never been greater.

Whether you care about cyber security, network access and data privacy, or infrastructure uptime, production and safety, the issues are the same:

- What is connecting to my network?
- Where are we exposed and at risk?
- What is getting past my defenses?
- How do I proactively respond, mitigate, and contain problems?

In highly-regulated environments, today's compliance requires managing it all — from strict policy enforcement within security frameworks, standards, and regulations — to having on-demand reporting that proves it.

You need a single platform that provides visibility into all enterprise assets, automated control and governance, and comprehensive risk mitigation and threat remediation. And you need it now.

The Forescout 4D Platform™ Is the Answer

The Forescout 4D Platform™ is a cyber security solution that provides intelligent control and continuous governance for any device anywhere. The Platform does this with four cross-cutting capabilities that discover, assess, control, and govern cyber assets. These capabilities span the connected edge to the cloud, providing total visibility and vulnerability scanning for managed and unmanaged assets throughout the enterprise.

Discovery

It starts with discovery. The Forescout 4D Platform™ discovery methodologies provide comprehensive asset visibility, identification, classification, and monitoring for every connected asset in your environment. That means you can count on thirty-plus discovery methods, integrations, and APIs to gain real-time asset discovery and inventory across all device types and Purdue levels.

Use the deep context created by these discovery and identification mechanisms to keep track of asset lifecycle events, from purchase to maintenance to decommissioning. The Platform detects assets and maintains accurate, contextual records over its lifetime.

Accurate records of asset lifecycle events ensure operational continuity and helps monitor asset changes that support compliance. The Platform does this by providing detailed insights that help optimize security operations, reducing downtime, refining maintenance plans, and improving system performance.

Finally, you can use discovery to extend control and compliance across domains by orchestrating unified IT, IOT, and IoMT workflows with CMDBs, IT operations and service management tools.

Assess

The Forescout 4D Platform™ assessment capabilities develop context-rich insights into the risks caused by gaps in asset security posture, behavior, and compliance. The Platform correlates multiple datapoints across heterogeneous environments that create risk scores that are prioritized based on criticality of impact. When high risks and exposures are identified, the Platform triggers control and orchestration workflows that enable automated risk mitigation and rapid, decision-making that helps manage risks with confidence.

The Platform's advanced vulnerability detection uncovers unpatched assets attempting to connect to the network using Forescout's curated database, which is enriched with EPSS, CISA KEVs, and Vedere Labs Research KEVs VL-KEV. This information continuously assesses and prioritizes risk across IT, OT, IOT, IoMT assets with real-time, contextual insights at both enterprise and device level. The result is proactive risk management and real-time awareness that builds business resilience.

Control

Forescout turns assessment into action with automated asset compliance checking and remediation. That includes quarantining, traffic blocking, and coordinated responses across operations and services. The Platform uses advanced threat detection and response, like deep packet inspection, advanced event analysis, and Vedere Labs threat intelligence for IT, OT, IOT, IoMT domains. Then, it triggers automated policy enforcement, control, and orchestration actions that contains threats, fixes misconfigurations, and resolves policy violations. The Platform can also be used to create SOAR notifications with custom fields, allowing you to use webhooks and automated workflows to provide more context to integrated systems.

And whether you work in network operations or the security operations center, you can use persona-based visualizations to see advanced alerts and case management that is specific to your responsibilities.

Govern

Centralized enforcement of security policies and access rules ensure operational consistency and organizational governance at scale. The Forescout 4D Platform™ provides unified policy management across critical decision points, enabling enterprise-wide compliance, consistency, and automated control that scales with precision and provides continuous governance.

Operators can define and enforce granular policies with templates or use custom profiles to simplify compliance and reporting. It's also possible to use the Platform's control and governance capabilities to enforce role-based access and deploy zero trust segmentation. This helps reduce the attack surface across all environments without disrupting operations.

Forescout 4D Platform™ Components and Deployment

The Forescout 4D Platform™ delivers scalable, integrated and intelligent asset security from the connected edge to the cloud. It does this with a hybrid cyber-security framework that provides comprehensive protection no matter where the Forescout 4D Platform™ is deployed.

Forescout eyeSight: Real-Time Asset Visibility

Forescout's eyeSight provides complete, real-time visibility into all devices across an organization's extended enterprise, ensuring that no asset is left unmonitored, regardless of whether it is managed or unmanaged.

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, reducing blind spots and the need for multiple point solutions.

Forescout eyeScope

Forescout eyeScope provides unified visibility for cyber assets across the enterprise, no matter where Forescout eyeSight is deployed. This enables administrators to optimize operations, enhance performance and resource utilization, and make more informed decisions across branches, campuses, data centers, and co-locations.

Key Features:

- See all assets in one console, and filter and search using dozens of asset properties.

- Deployment-wide insights and health metrics covering hardware utilization, plugins, and more. This includes health alerts to identify problems before they become outages and plugin health per appliance.
- Operational dashboards and executive reports that use generative AI to summarizes data into insights and recommendations provide simplified communications and compliance reporting. You can extend reporting capabilities by using Xplorer to query asset data and generate visualizations for custom dashboards.

eyeScope enables users expand Forescout asset intelligence to other departments or teams within their organization with easy user management and customizable RBAC.

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 best-in-class 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 automatically to security incidents, swiftly enforcing policies without interrupting business operations with eyeControl.

Forescout eyeInspect: OT/ICS Security

The security challenges facing operational technology (OT) and industrial control systems (ICS) are unique. eyeInspect is specifically designed to offer real-time visibility and security for OT/ICS environments.

Key Features:

- Full asset visibility for both IT, OT, IOT, IoMT environments and passive monitoring of OT networks.
- Automated vulnerability management that helps enterprises stay ahead of emerging threats and minimizes the likelihood of cyber-attacks.
- Threat detection and anomaly identification based on OT-specific protocols.

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

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.

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 augments Security Core solutions with a proactive approach to identifying, prioritizing, and remediating risks based on exposures.

Key Features:

- eyeFocus continuously assesses devices' risk scores based on vulnerabilities, configuration errors, and other threat vectors.
- Devices are prioritized based on their risk, ensuring that the most critical threats are addressed first.
- 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.

Forescout eyeAlert

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

Key Features:

- eyeAlert uses machine learning and advanced analytics to detect suspicious behavior patterns across devices and the network.
- Integrates with global threat intelligence feeds to identify and respond to emerging threats quickly.
- 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.

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.

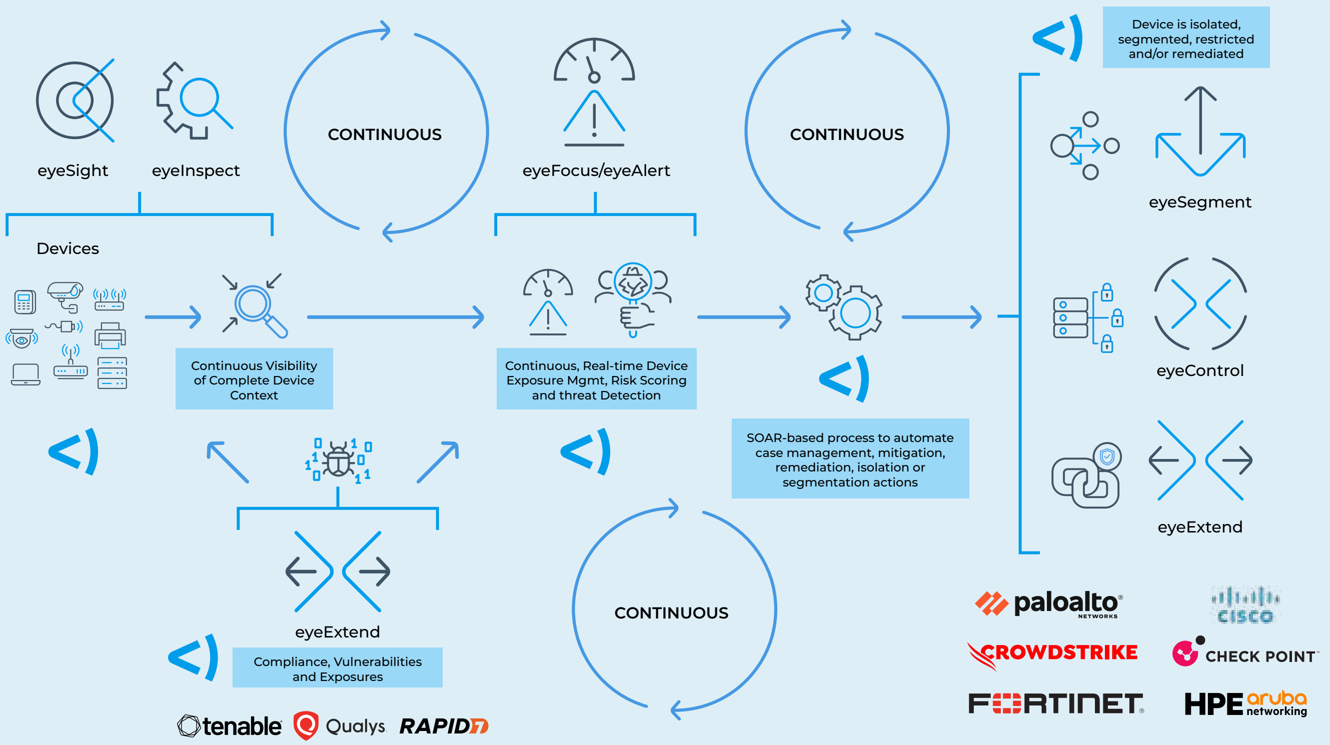
Reduce the mean time to detect (MTTD) and respond (MTTR) to cyber incidents, ensuring minimal damage and disruption to business operations with eyeAlert.

It's Under Control.

The Forescout 4D Platform™ provides cyber security solutions at scale, giving our customers the insights and flexibility they need to govern cyber assets continuously and in near real-time no matter what their deployment model is. Forescout is always watching. And with Forescout cyber security assurance, your network is under control.

To describe the capabilities of the platform, below is a graphic outlining the various products of the Forescout 4D Platform™ and their associated capabilities.

A Day in the Life of a Device


eyeSight
eyeInspect
CONTINUOUS
eyeFocus/eyeAlert
CONTINUOUS
Device is isolated, segmented, restricted and/or remediated
eyeSegment
Devices
Continuous Visibility of Complete Device Context
Continuous, Real-time Device Exposure Mgmt, Risk Scoring and threat Detection
SOAR-based process to automate case management, mitigation, remediation, isolation or segmentation actions
eyeControl
eyeExtend
eyeExtend
Compliance, Vulnerabilities and Exposures
CONTINUOUS
tenable
Qualys
RAPID7
paloalto NETWORKS
CISCO
CROWDSTRIKE
CHECK POINT
FORTINET
HPE aruba networking

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.

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. An IOT security leader dedicated to protecting the quality care of health delivery worldwide.

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