SOLUTION BRIEF

The Forescout 4D Platform™ Solution Brief

FORESCOUT

The Forescout 4D Platform™ Solution

The rapid expansion of digital infrastructure, including IT, OT, IoT, and IoMT, presents far more network and security blind spots. Cloud operational models and multi-environment scale demand flexible, manageable, and automated platform approaches rather than siloed point products. And heightened threats from surging risks and new vulnerable device types require deep visibility, real-time controls, and orchestration across ecosystems.

Growth in IoT devices is forecasted to grow from 14 billion in 2023 to 25 billion by 2030. Forescout Vedere Labs Research shows that the enterprise device landscape is becoming much more complex and dangerous, with the average device risk per industry increasing by 15% year-over-year. As the attack surface gets larger, it's creating bigger gaps and infinitely more duplicates and conflicts that cannot be easily resolved.

Whether you care about cybersecurity, 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, complying with Universal Zero Trust Network Access (UZTNA) 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 UZTNA by domain, risk management, and threat remediation over all enterprise assets: on-prem, remote, and in the cloud. And you need it now.

The Forescout 4D Platform™ is the Answer

Your journey to Universal Zero Trust Network Access starts with the Forescout 4D platform™: the only platform for UZTNA powered by agentic AI. Continuously identify, protect, and ensure the compliance of all assets – IT, IoT, IoMT and OT – regardless of location, automatically. Deliver cloud-native network security intelligence boosted by agentic workflows from the pioneer of traditional NAC.

With four cross-cutting capabilities, the platform spans the connected edge to the cloud, providing total visibility and scanning of managed and unmanaged assets: discover, assess, control, govern.

Discover

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, reduce downtime, refine maintenance plans, and improve 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 Service Management, Service Impact and Event Management, and other enterprise operations tools.

This same foundation enables Universal Zero Trust Network Access (UZTNA), ensuring that every asset, whether it's IT, OT, IoT, or IoMT, is continuously verified and granted the least-privileged access based on real-time context. By combining discovery with UZTNA, the Forescout 4D Platform™ enforces adaptive access policies that reduce risk, strengthen compliance, and secure your entire connected ecosystem.

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 to enable UZTNA.

With Forescout, you can ensure continuous verification and dynamic access control based on real-time asset posture and context, reducing risk and strengthening compliance. It goes on to trigger automated policy enforcement and orchestration control actions that contain threats, fix misconfigurations, and resolve policy violations. Forescout can also 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 UZTNA and security policy enforcement ensures operational consistency and organizational governance at scale. The Forescout 4D Platform™ provides unified policy management across critical decision points, enabling enterprise-wide compliance with evidentiary artifacts, 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 for remote users, the connected edge, on-prem, and the cloud. It does this with a hybrid cybersecurity 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 offpremises, reducing blind spots and the need for multiple point solutions. This visibility is the foundation for Universal UZTNA, enabling continuous verification and adaptive, least-privileged access policies for every device.

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 access and control over them. eyeControl provides UZTNA and best-in-class policy-based automation that allows IT and security teams to enforce compliance and security standards across their entire network.

Key Features:

- UZTNA and automated policy enforcement 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, and swiftly enforce 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.

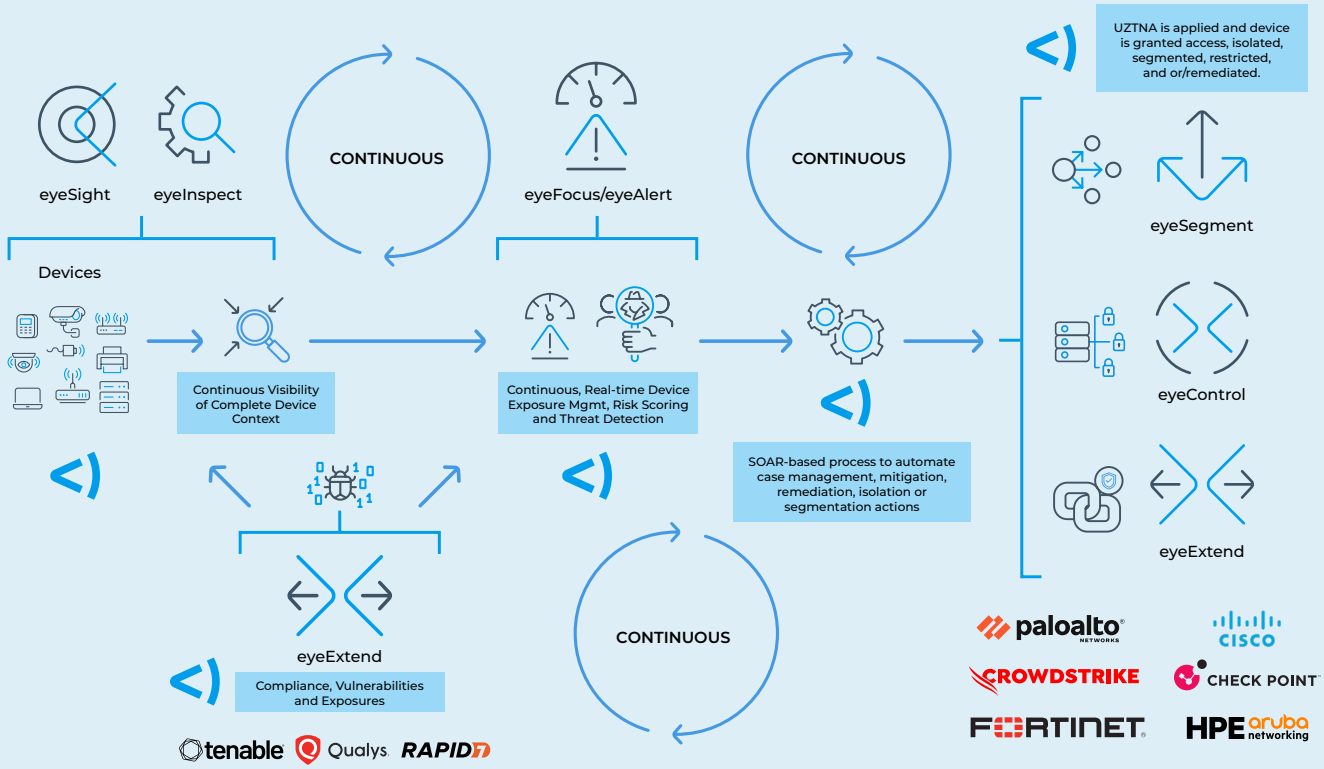
Continuously monitor and orchestrate dynamic, non-disruptive segmentation and simply Zero Trust enforcement.

It's Under Control.

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

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



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 granted access, isolated, remediated, and/or its traffic is segmented.
9. The risk the device poses the organization mitigated.

About Forescout

For over 25 years, organizations and governments worldwide have trusted Forescout to secure their networks. From pioneering Network Access Control (NAC) to delivering Universal Zero Trust Network Access (UZTNA), Forescout leads the evolution of enterprise network security across IT, OT, IoT, and IoMT environments. The Forescout 4D Platform™ delivers comprehensive asset intelligence, continuous risk assessment, and dynamic control, over all managed and unmanaged assets, enhanced by the proprietary threat intelligence research of Vedere Labs. Leveraging agentic AI workflows with human-in-the-loop actions, Forescout continuously analyzes threats, orchestrates response, and integrates seamlessly with 180+ security and IT products.

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