SOLUTION BRIEF

The Forescout Vistaro™ Platform Solution Brief

FORESCOUT

The Forescout Vistaro™ Platform Solution

The rapid expansion of digital infrastructure across IT, OT, IoT, IoMT, and cloud environments has fundamentally transformed the enterprise attack surface — introducing unprecedented scale, complexity, and risk. At the same time, frontier AI is accelerating the speed, precision, and automation of modern cyberattacks, while emerging quantum computing threats are poised to undermine the cryptographic foundations that organizations rely on today. Together, these forces are reshaping how risk must be understood, prioritized, and managed.

Device growth continues to surge, with IoT alone projected to expand from 14 billion devices 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, so do blind spots—creating fragmented visibility, duplicated controls, and unresolved conflicts across security and operations teams.

Whether the priority is cybersecurity, cyber exposure management, regulatory compliance, or operational resilience in critical OT environments, organizations are facing the same fundamental challenges:

- What is connecting to my network?
- Where are we exposed and at risk?
- What is getting past existing defenses?
- How do we proactively mitigate and contain threats?

In highly regulated industries, these challenges are compounded by the need to demonstrate continuous compliance while enforcing Universal Zero Trust Network Access (UZTNA) across all users, devices, and environments. This requires more than point solutions — it demands a unified platform that delivers continuous visibility, contextual risk prioritization, and real-time control across the entire asset landscape, from on-premises to remote to cloud.

See More, Act Faster, Secure What Matters

The Forescout Vistaro platform is built to address the full spectrum of modern cyber risk —spanning access, exposure, and operational resilience. It brings together continuous visibility, contextual intelligence, and automated control into a unified architecture that operates across IT, OT, IoT, IoMT, and cloud environments.

At its core, the platform delivers three critical outcomes:

Universal Zero Trust Network Access (UZTNA)

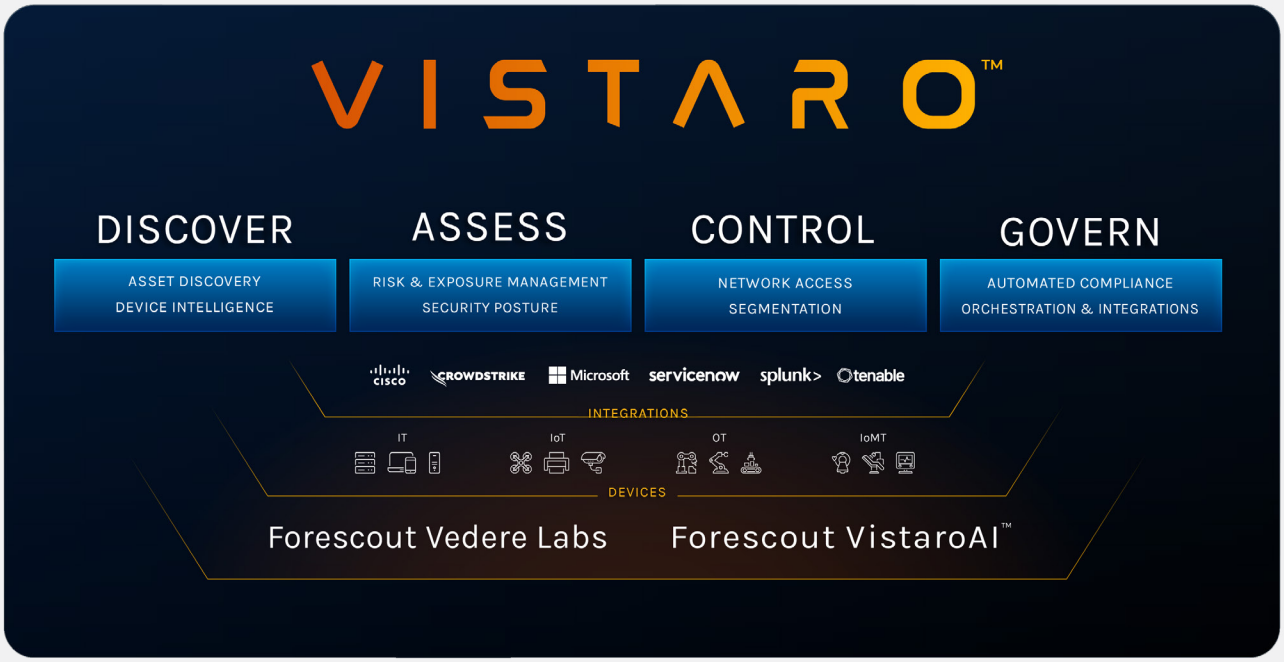
Extend Zero Trust principles across every device, user, and environment — without gaps. The Vistaro platform continuously verifies identity, posture, and behavior to enforce least-privilege access and prevent lateral movement across IT and OT systems. Unlike traditional approaches that focus on managed endpoints, UZTNA applies consistently across all asset types and locations.

Cyber Exposure Management

Continuously identify, prioritize, and reduce risk across the entire attack surface. The Vistaro platform provides real-time visibility into all connected assets and evaluates exposure based on exploitability, business impact, and threat intelligence—enabling organizations to focus remediation efforts where they matter most.

OT Security and Operational Resilience

Protect critical infrastructure and cyber-physical systems without disrupting operations. The platform enables complete visibility, risk management, and threat response across OT, ICS, and CPS environments—helping organizations maintain uptime, ensure safety, and meet regulatory requirements.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.



A Unified Platform Approach

These outcomes are powered by a unified set of platform capabilities that operate continuously and in coordination across every environment. Rather than relying on disconnected tools and fragmented workflows, the Vistaro platform brings visibility, risk intelligence, and enforcement together into a single, integrated system—ensuring that insights translate directly into action.

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

Discovery establishes a complete, real-time understanding of the expanded attack surface. The platform continuously identifies, classifies, and monitors every connected asset – managed and unmanaged – across IT, OT, IoT, IoMT, and cloud environments using extensive discovery methods, integrations, and APIs.

It goes beyond visibility by creating deep, contextual intelligence for each asset, tracking lifecycle events and changes over time to support operational continuity and compliance. This foundation integrates with enterprise systems to unify workflows and enables UZTNA by ensuring every asset is continuously verified and governed based on real-time context.

Assess

The Vistaro platform continuously evaluates risk across the entire attack surface by correlating asset posture, behavior, vulnerabilities, and compliance data into contextual, business-aware risk scores.

It prioritizes exposures based on criticality, exploitability, and threat intelligence—helping teams focus on what matters most. When risks are identified, automated workflows are triggered to accelerate response. Advanced vulnerability intelligence further ensures continuous identification and prioritization of exposures across IT, OT, IoT, and IoMT environments.

VistaroAI: Security That Thinks With You

- Continuously analyzes asset intelligence, exposure changes, and threat context
- Prioritizes what matters based on risk and business impact
- Delivers role-based insights so teams act faster and smarter
- Turns overwhelming data into clear, actionable decisions

Control

The Vistaro platform transforms insight into action through real-time, automated enforcement. It applies dynamic policies based on asset identity, posture, and context to contain threats, enforce compliance, and remediate issues across IT, OT, IoT, and cloud environments.

Capabilities include automated responses such as quarantining devices, blocking traffic, and orchestrating remediation workflows—enabling rapid mitigation as risks emerge.

Segmentation is a core component, allowing organizations to enforce granular policies that limit lateral movement and reduce the attack surface. Combined with continuous verification and dynamic access control, the platform enforces UZTNA principles at scale without disrupting operations.

Reduce Risk With Segmentation

- Limit lateral movement and contain threats before they spread
- Dynamically enforce Zero Trust segmentation across IT and OT
- Define granular policies based on identity, posture, and risk
- Reduce blast radius without disrupting operations

Govern

Governance ensures consistent, scalable policy enforcement and compliance across the enterprise. The Forescout Vistaro™ platform centralizes policy management and provides continuous validation, reporting, and audit-ready evidence.

Granular policy controls, role-based access, and Zero Trust segmentation help reduce attack surface while maintaining operational continuity. Governance becomes a continuous process — aligning security and compliance efforts with evolving risk and regulatory requirements.

Use Case-driven Outcomes

The Forescout Vistaro platform delivers a comprehensive set of security capabilities designed to address the most critical challenges across today's expanded attack surface. By combining continuous visibility, contextual risk analysis, and real-time control, organizations can secure every connected asset and operational workflow — across IT, OT, IoT, IoMT, and cloud environments.

Forescout Vistaro Platform Solutions by Industry

Organizations across industries face unique security, compliance, and operational challenges — but share the same need for continuous visibility, risk reduction, and resilient operations. The Forescout Vistaro platform adapts to these environments, enabling organizations to secure complex infrastructures, enforce policy at scale, and protect mission-critical systems without disruption.

Financial Services

Forescout helps you comply with rigorous standards and secure complex environments at scale with agentless device visibility, continuous monitoring and automated policy-based control enforcement.

Government

Forescout helps government IT and security professionals protect sensitive information, secure access to resources and demonstrate compliance through continuous monitoring and automated risk mitigation.

Healthcare

Forescout helps you safely expand network access to clinicians, caregivers, research organizations and contractors while securely embracing agentless medical devices, IoMT and IoT.

Power & Utilities

Forescout helps you protect critical infrastructure from cyberthreats, mitigate operational risks to reduce downtime, and demonstrate compliance with NERC CIP.

Oil & Gas

Forescout provides complete visibility and automated risk mitigation in OT/ICS networks to ensure safety, improve uptime and enforce compliance with the NIST Cybersecurity Framework and IEC 64223.

Manufacturing

Forescout provides comprehensive asset visibility, risk mitigation and policy compliance across OT, IoT and IT networks to help increase manufacturing efficiency, automation and uptime.

Education

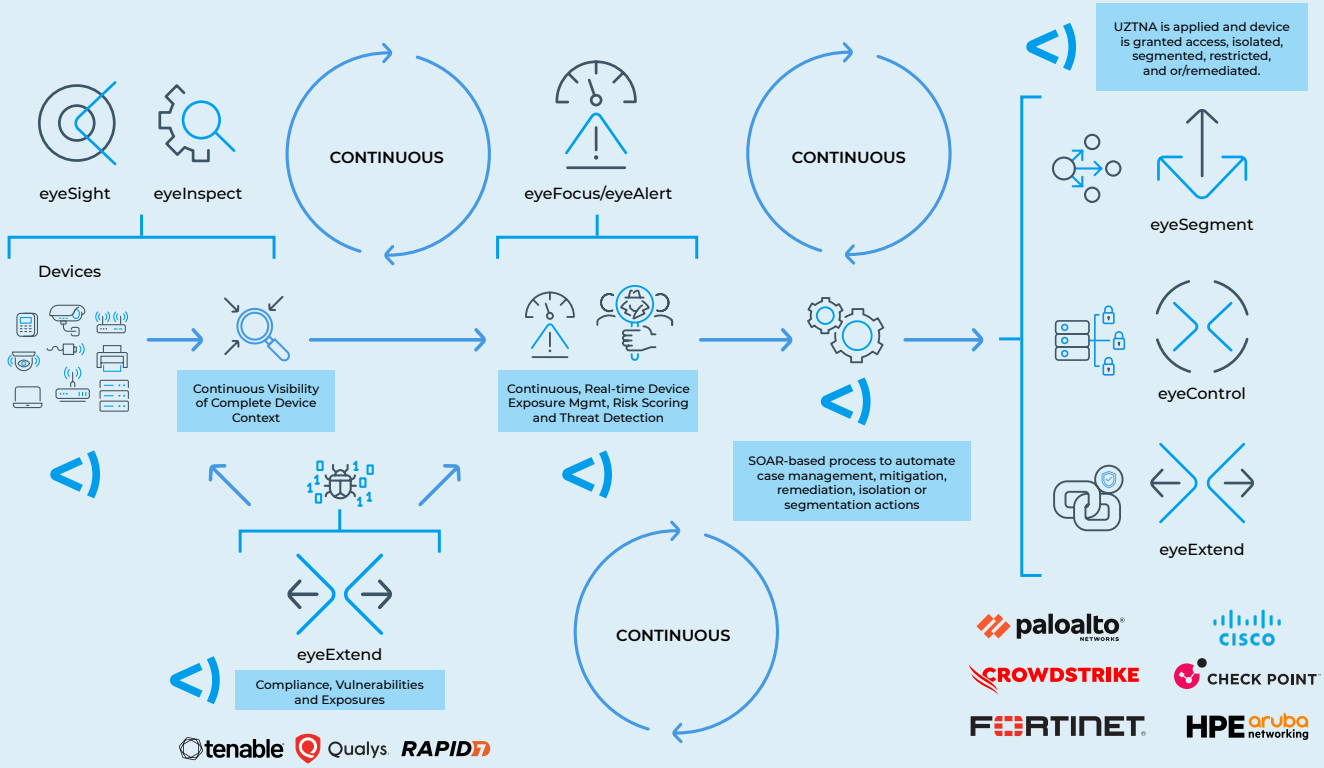
Forescout makes it possible for students and faculty to connect via a vast array of devices by enforcing least-privilege access based on identity, device type and security hygiene.

A Platform Built for the Modern Attack Surface

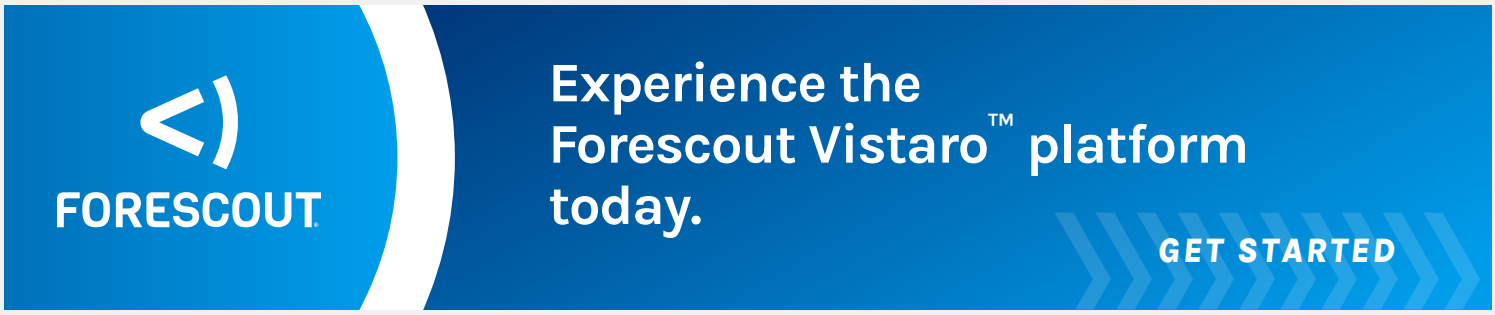
- **See everything** – Gain complete visibility across IT, OT, IoT, IoMT, and cloud to eliminate blind spots across your entire attack surface.
- **Understand your risk** – Continuously prioritize exposures based on real-world exploitability and business impact.
- **Act with speed and precision** – Automate enforcement, segmentation, and response to reduce risk and lateral movement in real time.
- **Enforce Universal ZTNA** – Apply continuous verification, dynamic access control, and least-privilege policies across all environments.
- **Strengthen resilience** – Protect critical operations, reduce downtime, and ensure compliance across complex infrastructures.

The Forescout Vistaro platform brings access, exposure, and operational security together — so you can see more, act faster, and secure what matters most.

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

As AI-driven vulnerability discovery and exploitation accelerate attack velocity to machine speed, Forescout is a foundational cyber defense layer that allows organizations to segment and isolate compromised systems, block lateral movement, and automate response across IT, OT, IoT, and IoMT environments. The Forescout Vistaro™ platform, powered by agentic AI and enhanced with Vedere Labs threat intelligence, delivers a Universal Zero Trust Network Access (UZTNA) architecture that integrates seamlessly with 180+ security and IT products. With Forescout Vistaro, organizations get comprehensive inventory and classification of both managed and unmanaged assets, continuous exposure management, and real-time protection including dynamic network segmentation and automated threat response.

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