Netskope + Forescout

Universal Zero Trust Network Access (UZTNA) Powered by Real Time Device Intelligence and Cloud Smart Enforcement

Details

- **Universal Zero Trust Across All Assets:** Granular access enforcement spanning IT, IoT, IoMT, and OT across cloud, on prem, and remote environments.
- **Unified Asset and User Identity Visibility:** Correlate device posture, identity, and behavioral context for dynamic, real time access decisions.
- **Continuous Compliance and Audit Readiness:** Enforce ongoing security validation and automated evidence collection across the environment.
- **Adaptive Threat Defense:** Identify anomalies early using behavioral analytics and automated response to block unauthorized access.

Overview

Modern enterprises depend on an expanding mix of IT, IoT, IoMT, and OT devices for campus, cloud services, and remote environments. Yet achieving consistent Zero Trust across these diverse assets remains one of the more formidable security challenges, especially when visibility is fragmented, device posture is variable, and traditional network controls fail to extend into unmanaged or critical systems.

The joint Netskope + Forescout solution delivers a unified approach to Universal Zero Trust Network Access by combining Forescout's continuous, agentless device intelligence with Netskope's cloud native Security Service Edge (SSE) and Zero Trust Engine.

Together, the combined solution provides comprehensive visibility, dynamic risk scoring, and adaptive access enforcement across both North/South and East/West traffic. This ensures that every user, every device, and every application connection is continuously validated, even across the most complex hybrid infrastructures.

Challenge

- Need to secure a rapidly growing and diverse ecosystem of devices, from traditional IT systems to IoT sensors, medical equipment, and financial applications
- Remote users can connect from anywhere and everywhere
- Disconnected security controls create blind spots
- Security teams are unable to enforce consistent Zero Trust policies or detect risky behavior in real-time

Organizations need a unified, automated, and context rich approach to Zero Trust that spans all device types and traffic flows.

The Solution: Netskope + Forescout

The combined Netskope + Forescout solution:

- Operationalizes Universal Zero Trust Network Access across hybrid environments
- Continuously discovers, classifies, and scores every device—managed or unmanaged—across IT, IoT, OT, and IoMT ecosystems
- Enforces context driven, least privileged access through a cloud-native Zero Trust engine
- Provides bi-directional enforcement between cloud and on-prem environments
- Ensures consistent control across North/South and East/West traffic

Organizations gain a continuously validated security posture, automated compliance evidence, and faster incident response through enriched context and coordinated remediation.

Use Cases

1. Universal Zero Trust Enforcement Across All Devices

The Netskope + Forescout solution extends Zero Trust to every device, whether enterprise managed or remote or third-party. Netskope provides granular session, user, and application controls, while Forescout adds real time device intelligence and posture assessment. This allows every connection to be authenticated and authorized based on dynamic conditions, reducing attack surfaces and preventing lateral movement.

2. Complete Visibility & Contextual Intelligence

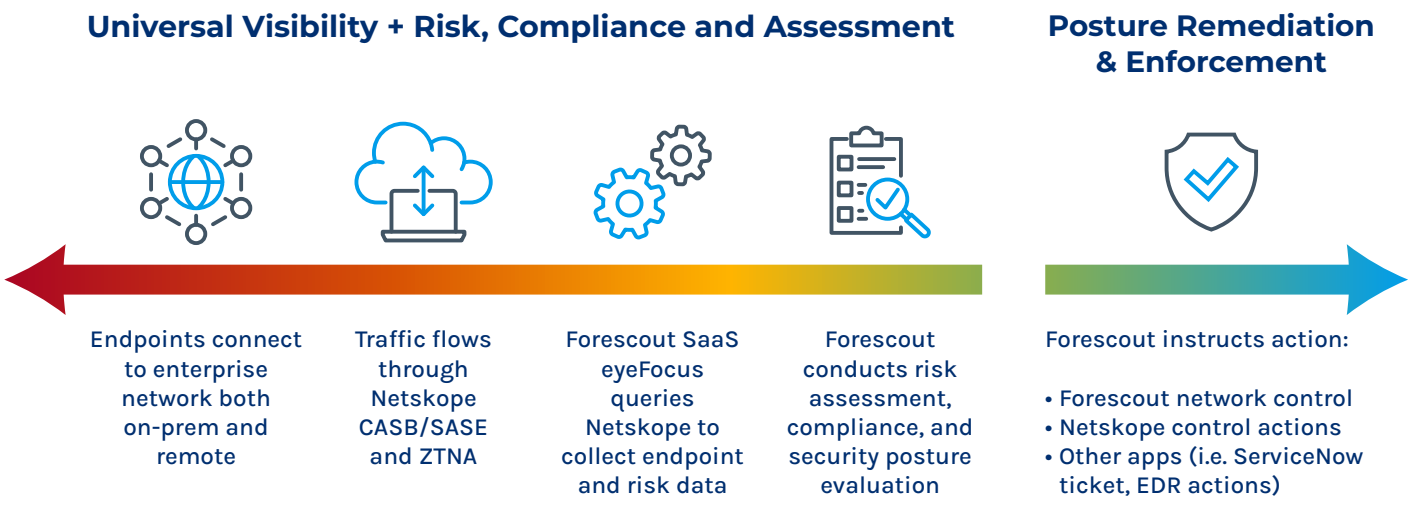
Security teams gain a consolidated, real time view of device posture, identity, and behavior. Forescout discovers and categorizes all devices (including unmanaged), while Netskope adds deep context on user activity, cloud services, and application behavior.

3. Continuous Compliance & Audit Readiness

The integration shifts organizations from periodic compliance checks to continuous enforcement. Netskope handles data protection and policy enforcement while Forescout provides real time posture validation and automated remediation workflows.

4. Adaptive Threat Defense & Automated Response

Combining Netskope's behavioral analytics with Forescout's device intelligence, the joint solution detects anomalies—such as unusual lateral movement, suspicious access attempts, or potential data exfiltration—before they escalate.



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.

About Netskope

Netskope is a global leader in cloud native security, providing a modern SSE architecture and Zero Trust Engine that deliver granular visibility, adaptive access control, and advanced data protection across cloud, web, and private applications.

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