Solution Brief

Netskope and Forescout

Netskope and Forescout unify asset intelligence with adaptive enforcement. By combining Forescout's continuous device visibility and risk assessment with Netskope's Zero Trust Engine, organizations secure all on-premises and remote traffic. This delivers granular access control and automated compliance across the entire digital landscape.

Quick Glance

- **Unified zero trust:** Secure all IT, IoT, and OT traffic across every location.
- **Unified visibility**: Create one source of truth using shared device and risk data.
- **Continuous compliance**: Automate security audits with real-time policy enforcement for all assets.
- **Adaptive defense**: Use risk scores to block threats and stop data loss instantly.

The Challenge

Modern enterprises face significant challenges in enforcing consistent unified zero trust across a rapidly growing and diverse set of devices—including IT systems, IoT sensors, IoMT, and OT controllers—while supporting users in both on-premises and remote environments. This complexity is compounded by fragmented visibility and siloed security tools that fail to provide a unified view of assets and user activity. Disjointed policies across multiple platforms create operational inefficiencies and leave critical gaps in enforcement and in security posture. Blind spots in device and user context increase the risk of unauthorized access, complicate compliance with regulatory frameworks, and slow incident response times, ultimately exposing organizations to greater security threats and operational risk.

The Solution

Netskope and Forescout deliver a unified security shield by combining secure cloud access with deep device intelligence. Netskope manages remote user traffic, while Forescout adds vital context for IT, IoT, and OT devices. Together, they enforce consistent policies across all environments, closing security gaps. This partnership ensures continuous compliance and faster threat response through automated risk assessments and behavioral analytics, protecting your entire digital landscape at scale.

Unified zero trust enforcement across all devices

The joint solution delivers unified zero trust by extending policy enforcement beyond traditional IT endpoints to include IoT, IoMT, and OT devices—whether on-premises or remote. Netskope provides granular control over user sessions and cloud access (north-south traffic), while Forescout adds deep device intelligence and posture assessment to secure network communications (east-west traffic). This combination ensures that every connection is authenticated, authorized, and continuously validated against dynamic risk criteria. Unlike siloed approaches that leave gaps in coverage, this integrated solution applies consistent security policies across diverse environments, reducing attack surfaces and preventing lateral movement.

Organizations benefit from a unified enforcement model that adapts to changing conditions, enabling secure access without compromising productivity. By correlating user identity, device posture, and network context, the solution enforces least-privilege principles at scale, helping enterprises meet zero trust mandates and regulatory requirements. Ultimately, the joint solution empowers security teams to close blind spots, simplify policy management, and maintain strong security across hybrid infrastructures. Key capabilities include:

- Enforcing **least-privilege principles** across all device types and environments
- Applying **dynamic, risk-based policies** to prevent unauthorized access and lateral movement
- Closing coverage gaps and simplifying policy management for hybrid infrastructures
- Helping meet zero trust mandates and regulatory requirements at scale

Netskope secures north-south cloud traffic, while Forescout governs east-west lateral movement for all on-premises and remote assets.

Unified visibility and contextual intelligence

Visibility is foundational to security, and this combined solution offers unmatched clarity into who and what is connecting to your environment. Forescout's asset intelligence discovers and classifies every device—managed or unmanaged—while Netskope adds rich telemetry on user sessions, applications, and data flows. Together, they create a single source of truth that correlates identity, device posture, and behavioral context in real time. This holistic view enables security teams to detect anomalies, enforce granular policies, and respond faster to emerging threats.

Unlike fragmented tools that provide partial insights, this capability eliminates blind spots across IT, IoT, IoMT, and OT ecosystems. It also supports dynamic risk scoring, allowing organizations to prioritize actions based on actual exposure.

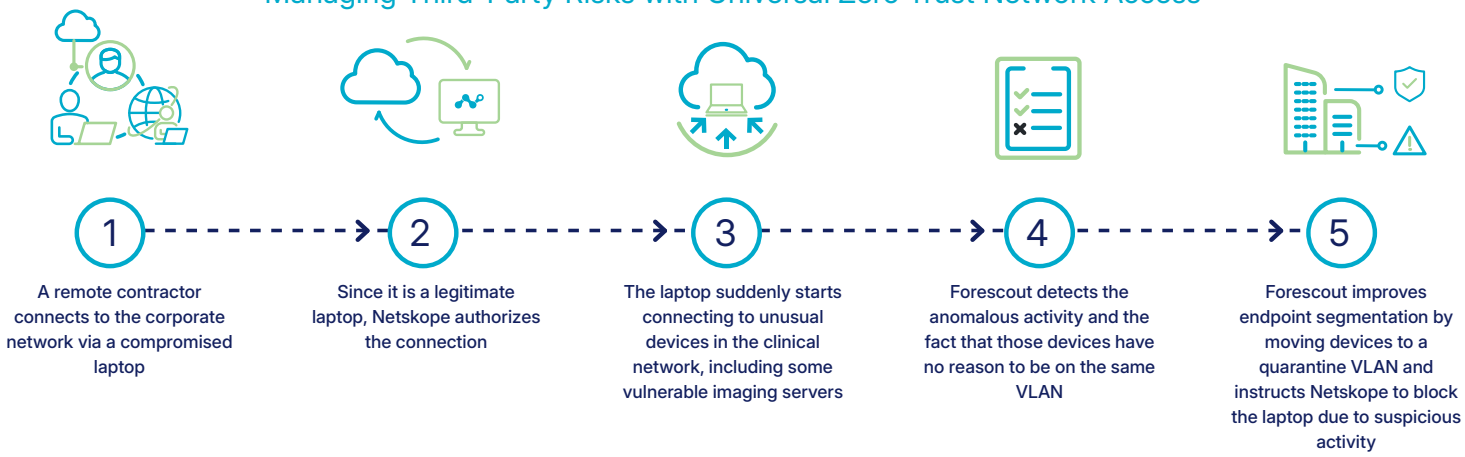
With unified visibility, enterprises can confidently implement zero trust strategies, streamline compliance reporting, and reduce operational complexity. The result is a proactive security posture that minimizes risk while enabling business agility. The key capabilities include:

- Correlation across identity, device posture, and behavioral context for **dynamic risk scoring**
- Eliminating blind spots across IT, IoT, IoMT, and OT ecosystems
- Enabling anomaly detection and **granular policy enforcement** with confidence

The result is a proactive security posture that minimizes risk while enabling business agility.

Scenario: Third-Party and Supply Chain Compromise

Managing Third-Party Risks with Universal Zero Trust Network Access



Continuous compliance and audit-readiness

Maintaining compliance in today's dynamic environment is challenging when relying on periodic audits and manual checks. The Netskope and Forescout joint solution transforms this process by enabling continuous security validation and automated evidence collection. Policies are enforced in real time, ensuring that devices and users meet compliance requirements before and during access.

Forescout's posture assessment and remediation workflows pair with Netskope's continuous compliance and data loss prevention (DLP) capabilities to proactively block non-compliant connections. By enforcing granular, real-time access controls based on Forescout's device intelligence, organizations automate audit readiness, lower operational overhead, and minimize regulatory risk across the entire environment.

Organizations gain confidence that compliance is not a point-in-time exercise but an ongoing state, supported by automated reporting and actionable insights. By embedding compliance into daily operations, the solution helps enterprises meet frameworks such as CIS, NIST, and zero trust architecture without disrupting productivity, allowing security teams to focus on strategic initiatives rather than manual enforcement. The key capabilities include:

- Real-time posture checks ensure **devices and users meet compliance before access**.
- Automated workflows remediate non-compliant endpoints proactively.
- Reduced audit preparation time and operational overhead.
- Support for frameworks like **CIS, NIST, and zero trust architecture**.

Adaptive threat defense and risk management

The Netskope and Forescout joint solution delivers adaptive threat defense by unifying Netskope's behavioral analytics with Forescout's device intelligence to identify high-risk patterns before they escalate. By correlating user identity, cloud activity, and real-time device posture, the joint solution detects anomalies—such as lateral movement, data exfiltration, or policy violations—at the earliest possible stage.

This capability transcends simple alerting. By leveraging the **Netskope Zero Trust Engine**, the solution enforces dynamic, context-aware policies that automatically restrict access or isolate compromised endpoints without manual intervention. This proactive approach minimizes false positives, accelerates containment, and reduces breach impact. Security teams gain actionable intelligence to prioritize threats and respond confidently, while maintaining business continuity.

Adaptive threat defense empowers enterprises to protect sensitive data, uphold compliance mandates, and maintain trust across hybrid environments—all while reducing operational overhead. With continuous monitoring and automated response, customers shift from reactive security to a predictive, preventive posture that secures both north-south and east-west traffic flows seamlessly.

- Monitor user and device activity in real time to identify anomalies before they become incidents.
- Automatically enforce access restrictions or isolate risky endpoints without manual intervention.
- Correlate identity, device posture, and behavioral patterns to minimize false positives and accelerate response.
- Detect unusual access attempts and data exfiltration behaviors early to prevent costly breaches.
- Move from reactive alerts to proactive, automated threat containment for stronger resilience.

USE CASE MATRIX	DESCRIPTION
Mitigate third-party access risk (healthcare)	Reduce third-party cyber risk in hospitals by enforcing device compliance at the point of access, while applying continuous visibility and data protection controls across cloud and web interactions involving sensitive patient data.
Secure hybrid work and high-value transactions (financial)	Banking and financial institutions face strict regulatory and audit requirements. With unified visibility and continuous compliance enforcement, the joint solution strengthens controls around highly sensitive data, privileged access, and remote workforce interactions.
Protect critical infrastructure	Operational technology environments benefit from Forescout's deep OT visibility and Netskope's adaptive enforcement, preventing lateral movement between production systems and safeguarding industrial reliability.

netskope + FORESCOUT

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.