

5 Reasons to Transform Your Web and Network Security:

Moving Beyond On-Prem Proxy and Branch Firewalls



Executive Summary

On-premises proxy gateways and branch firewalls are trying to protect a perimeter that no longer exists. Networks and security controls are now needed where users and their devices work, and where data resides—SaaS applications and cloud services. Physical network security appliances restrict business agility, require complex operations, limit visibility, and are expensive to maintain and patch.

What if you could transform to a network security solution that provides the following:

- Faster performance and no security trade-offs, delivering a great user experience
- Removal of blind spots for SaaS/IaaS, shadow IT, and remote working

- Consolidated, simplified infrastructure, and reduced costs
- Streamlined network operations and faster user provisioning
- Reduced network engineering backlogs, patch cycles, and infrastructure failure points
- Accelerated time-to-value, including for mergers and acquisitions

Transformation involves retiring legacy secure web gateways, firewalls, and related hardware and circuitry, unlocking labor savings in equipment management, support, and maintenance.



Reduce the number of lingering issues preoccupying networking and security teams by **over 80%** and find additional efficiencies associated with network **security modernization** not possible with legacy solutions.

Avoid performance versus security trade-offs and remove blind spots.

Unified architecture with one platform, network, gateway, and client

- Reduce complexity for network security
- Single-pass inspection for FWaaS/IPS, SWG, and CASB core defenses at the cloud edge

Enable data and threat protection with a great user experience

- Netskope NewEdge provides performance and resilience with global load balancing and optimized route control
- Full compute for all data and threat protection defenses at each data center
- Increase visibility for remote working with a cloud edge on-ramp supporting 200+ localization zones

Remove blind spots for malware, phishing, and other threats

- 40+% of threats are delivered from popular SaaS applications including Microsoft 365
- Avoid bypassing traffic as SaaS is both a target for phishing and infrastructure to deliver threats

Detect data exfiltration into SaaS including company versus personal instances of applications

- The last 30 days of employment data exfiltration increases over 3X, mainly into personal cloud storage
- Provide real-time coaching to users on risky behaviors and collect justifications for their actions

Source: Netskope Threat Lab Reports

Forrester [Total Economic Impact \(TEI\) of Netskope SSE](#)



“At the end of the day, our number one goal is to secure the endpoints and eliminate friction”.

— VP of Infrastructure



Consolidate infrastructure to increase operational efficiencies.

Decommission legacy data centers, physical equipment, and hardware

- Sunset firewalls, SWGs, and legacy DLP tools
- Consolidate switching ports and reduce hardware and circuitry

Reduce and remove infrastructure failure points for network security

- Decrease patch SLAs from weeks to on-demand
- Reduce lingering issues and rework for networking and security teams

Support remote working and improve user experience

- Avoid backhauling traffic or allowing direct access without inspection
- Re-architect to a coffee shop model to streamline, improve, and innovate

Replace VPNs with ZTNA to improve security posture and user experience

- Remove publicly exposed services, transform to an inside-out private access security posture
- Reduce complexity for users accessing private applications and resources



Netskope's automated processes for patch updates reduced engineering labor by more than

75%

and decreased the patch SLA from weeks to effectively on-demand.

“I can rip out a [legacy server] chassis and save \$100,000 a year on maintenance. Those are significant savings.”

— VP of Infrastructure

Streamline operations, provision users faster, and improve visibility.

Improve network availability and operations

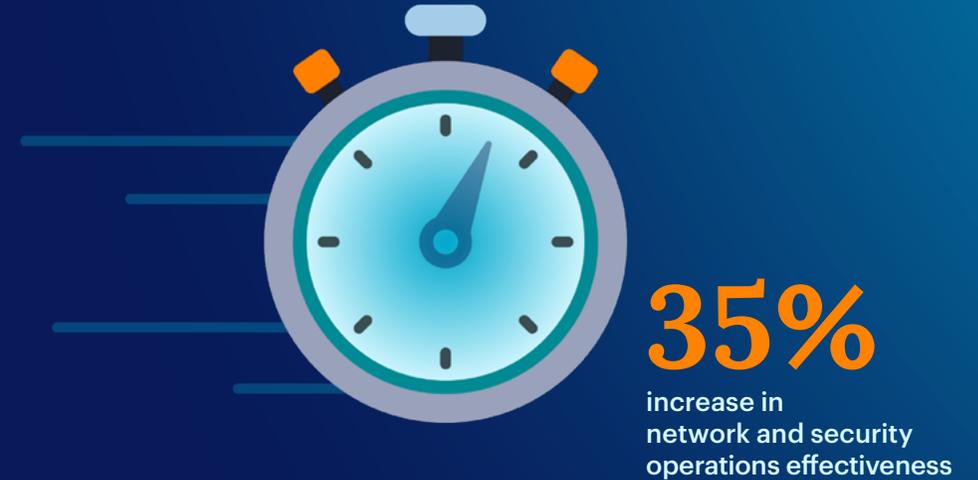
- Reduce engineering labor, security processes, and automate workflows
- Improve network resilience, performance, and user productivity

Single client for web, SaaS, IaaS, and private application access

- Provision users faster and shift operational resources to higher-value activities
- Reduce user effort and related troubleshooting issues

Full path visibility for users and apps from client to destination

- Real user monitoring (RUM) for users and apps on the full path from client to destination
- Enable traffic packet captures for investigations, performance, and compliance



“Before [Netskope SSE], we were below 90% [availability] without a doubt. ... Now, we are probably around 3 Sigma [99.73%].”

— VP of digital experience in the financial services industry



Reduce risk and encourage safe behaviors through contextual data insights.

Inline inspection of web, SaaS, and IaaS traffic

- Content and context analysis prevents risky behaviors before they do harm, reducing incidents and time for resolution
- Content inspection enables real-time AI/ML-based defenses to detect unknown threats and data risks

Enable adaptive access controls for zero trust principles

- Netskope Zero Trust Engine analyzes multiple trust and risk variables for each transaction
- Providing real-time decisions for adaptive access control
- Coach users to safer application alternatives and provide company guidance

Continuous monitoring detects unknowns and refines policy controls

- Netskope One Advanced Analytics provide insights on users, apps, activities, data movement, and trends
- Review justifications to understand new use cases and to further refine policy controls



“Netskope SSE was 50% better at providing insightful contextual data than other solutions tested.”



Accelerate time-to-value and improve business agility.

Shift to a cloud-edge platform to protect any user, device, or location

- Shifting to and operating Netskope SSE is faster than with traditional networking
- Protect managed and unmanaged devices

Protect new employees, contractors, or partners on day one

- Quickly provision new users, partners, or contractors with full SSE protection and seamless access
- Attract top talent in remote locations

Secure data to protect revenue, partnerships, and customer retention

- Meet the rising need to show strong data security to customers and data sharing partners
- Reduce the effort to comply and report on compliance regulations

Accelerate time-to-value for mergers and acquisitions

- Streamline M&A labor efforts and reduce costs
- Quickly assess new applications to reduce risk and centralize application use

50%

reduction in integration costs associated with mergers and acquisitions.



Transformation delivers overwhelming business value and technical gains.

It's hard to ignore benefits including:

- Greater visibility and insights
- More control and adaptive access
- Improved performance and availability
- Consolidation and cost savings
- Positive ROI based on hard cost alone
- Reduced backlogs and lingering issues
- Improved resolution times and less effort
- The freeing up of networking and security teams for higher-value projects

While it feels safe to stick with the technologies you already have, the indisputable reality is that transformation is a better alternative, and the urgency for change is growing.

Advances in AI and machine learning require access to content and context for actionable network security real-time detections and to enable adaptive access controls. On top of this, blocking is recognized as an inappropriately blunt tool for controlling GenAI apps, impeding innovation when more granular controls can enable data security for safe use.

Security should not compromise user experience. The right networking and security architecture turns remote users into the IT team's fan club as they experience great performance, seamless access, and new paths to improve their productivity.

Reject compromise in your network security. Transform to enable your business and its agility.



 Organizations that have moved beyond legacy tools are already seeing significant benefits. Explore five short, ungated videos showcasing key outcomes.

[Learn More](#)



About Netskope

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.

Interested in learning more?

Request a demo



©2025 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized “N” logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners. 03/25 EB-824-2