netskope

White Paper

Seven Strategies to Jumpstart Your Network Security Transformation

Table of Contents

INTRODUCTION:
EMBRACING THE NETWORK SECURITY TRANSFORMATION JOURNEY

In today's rapidly evolving digital landscape, network security transformation is crucial for enhancing agility, improving performance, and securing enterprise environments. It involves adopting new technologies and strategies to boost productivity, enhance security, and improve operational efficiency. Key drivers for network security transformation include protecting assets, ensuring compliance, and positioning enterprises for future success in an increasingly digital world.

1. **Evolving Threat Landscape**

   Cybercriminals are leveraging advanced techniques, such as artificial intelligence (AI) and machine learning (ML), to launch more targeted and effective attacks. As a result, enterprises must adopt advanced protection technologies and strategies to stay ahead of these threats.

2. **Zero Trust Adoption**

   Zero Trust adoption is driven by the need for a more secure and flexible approach to cybersecurity in the face of evolving threats and changing IT environments. This security model is based on the principle of "never trust, always verify," meaning that no one, whether inside or outside the network, is trusted by default. Instead, every access request is thoroughly verified, regardless of the user's location or whether the request originates from within the organization's network.

3. **Increased Connectivity, 5G, and IoT**

   The proliferation of IoT devices, which are often always on and connected, along with the expansion of 5G technology, increases potential entry points for cyber threats, necessitating robust security and network segmentation.

4. **Digital Transformation**

   Adopting cloud services and mobile technologies enhance operational efficiency, improve customer experiences, and drive innovation, but can also introduce new risks and vulnerabilities. It is essential to ensure that the new technologies are integrated securely.

5. **Regulatory Compliance**

   Adhering to stringent data protection regulations is critical to avoid fines and legal issues. Network security transformation helps enterprises implement the necessary security controls and processes to comply with these regulations and protect sensitive data.

6. **Business Agility and Innovation**

   In today's fast-paced business environment, agility and the ability to innovate are crucial for staying competitive. A modern, secure network infrastructure enables rapid adaptation to market changes, supports remote workforces, and fosters innovation.

7. **Customer Trust and Reputation**

   Data breaches and cyberattacks can severely damage enterprise reputations and erode customer trust. Ensuring robust network security helps build customer trust and protects enterprise reputations.

8. **Operational Efficiency and Cost Savings**

   Modernized network infrastructures lead to operational efficiencies. By automating security processes, reducing manual interventions, and optimizing resource allocation, enterprises can improve their overall security posture while reducing operational costs.

Network transformation with Secure Access Service Edge (SASE) incorporating the Security Service Edge (SSE) core component is revolutionizing how organizations secure and manage their networks. SASE integrates network and security functions into a unified, cloud-native service, providing seamless, secure access to applications and data from anywhere. This approach enhances performance, scalability, and security by reducing the complexity of traditional architectures and enabling a zero trust security model. Key benefits of SASE include ongoing verification via AI and integration with the entire security stack, contextual visibility of users, devices, applications, and data, reduced latency through efficient traffic inspection, and simplified management. These features are essential for meeting the demands of modern digital enterprises. However, challenges such as integration difficulties, change management, and workforce training remain significant.

Achieving a full Secure Access Service Edge (SASE) framework cannot be done overnight; it requires a phased, strategic approach. SASE can be effectively implemented through small, manageable projects that gradually build towards a comprehensive transformation. Following are a few strategies to achieve this objective:

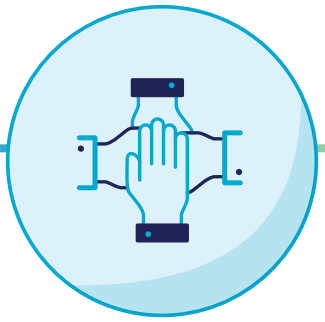
STRATEGY 1: ASSESS YOUR CURRENT NETWORK SECURITY POSTURE

Before embarking on a network security transformation journey, it's essential to understand where you currently stand. Assessing your current network security posture is the first crucial step in your security transformation journey. By conducting a comprehensive security audit, you can identify vulnerabilities, set baseline metrics, and develop a strategic plan to enhance your security infrastructure.

- **Step 1: Define the Scope of the Audit:** Identify the business priorities, along with the most sensitive data and most important applications. Define all assets, determine their criticality and set clear objectives for the audit, such as identifying vulnerabilities and business impact, ensuring compliance, or preparing for a transformation.
- **Step 2: Gather Information:** Create a detailed network map, maintain an up-to-date inventory of devices and software, and review user access levels to ensure they are appropriate and secure.
- **Step 3: Assess Security Controls:** Examine firewall, IDS/IPS, VPN, SWG, and CASB configurations, evaluate endpoint security measures (antivirus, encryption, etc), and analyze access control mechanisms.
- **Step 4: Identify Vulnerabilities:** Use vulnerability scanning and penetration testing to uncover weaknesses, and assess system configurations for best practices.
- **Step 5: Evaluate Compliance:** Ensure alignment with regulatory requirements (GDPR, HIPAA, industry-specific regulations) and internal policies, and verify adequate logging and monitoring to track and respond to security incidents.
- **Step 6: Analyze and Report Findings:** Document vulnerabilities, perform a risk assessment, and establish baseline metrics for future improvements to measure future improvements and the effectiveness of your security transformation efforts.
- **Step 7: Develop an Action Plan:** Create a remediation plan, allocate necessary resources including budget, personnel, and tools, and set a timeline for implementation.
- **Step 8: Continuous Improvement:** Schedule regular audits, conduct ongoing training, and stay updated with the latest security trends and technologies to adapt your security strategy as needed.

Apply the Zero Trust Maturity Model in your organization to your Identity, Devices, Networks, Applications and Workloads and Data. In the case of Networks:

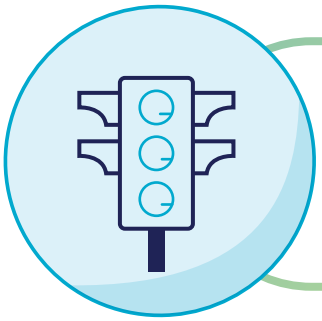
- **Application access:** Continuously authorize application access, incorporating real- time risk analytics and factors such as behavior or usage patterns.
- **Application Threat Protections:** Integrate advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.
- **Accessible Applications:** Make all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.
- **Secure Application Development and Deployment Workflow:** Leverage immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.
- **Application Security Testing:** Integrate application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.
- **Visibility and Analytics Capability:** Perform continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.
- **Automation and Orchestration Capability:** Automate application configurations to continuously optimize for security and performance.
- **Governance Capability:** Fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the Continuous Integration and Continuous Delivery (CI/CD) pipeline.



STRATEGY 2: SECURITY AND NETWORKING TEAMS WORKING IN TANDEM

The collaboration between security and networking teams is crucial for building a secure and efficient IT infrastructure. By working together, sharing knowledge, and integrating their efforts, these teams can create a more resilient network that is better equipped to handle the challenges of the modern digital landscape to not only enhance security but also improves the overall performance and reliability of the network. With this approach, professionals from both functions routinely collaborate to build a technology infrastructure rooted in a zero trust security model that is simultaneously high-performing and secure. Here's how security and networking teams can collaborate effectively:

- **Shared Goals and Objectives:** Establish common goals and involve both teams in network planning to ensure security is integrated from the start.
- **Regular Communication and Coordination:** Hold regular meetings, develop a coordinated incident response plan, and maintain clear communication channels.
- **Integrated Technologies and Tools:** Utilize unified monitoring and management systems that include granular Role-Based Access Control (RBAC), support for multiple identity providers (IDPs), and robust auditing. Implement automation tools to streamline processes and facilitate collaboration between teams.
- **Shared Knowledge and Training:** Encourage cross-training and joint workshops to foster mutual understanding and cooperation.
- **Policy and Procedure Alignment:** Develop aligned security policies and standard operating procedures that involve both teams.
- **Risk Management and Threat Intelligence:** Perform joint risk assessments and utilize shared threat intelligence resources for comprehensive risk mitigation.
- **Continuous Improvement and Feedback:** Conduct post-incident reviews and establish feedback mechanisms to continuously improve collaboration and processes.



STRATEGY 3: ACCELERATE AND SECURE WEB & SAAS TRAFFIC

Companies have long used web filtering to prevent users from visiting objectionable and unproductive websites. A traditional web filter deployed upon on-premises hardware means that all users' internet traffic is backhauled to the corporate data center. Backhauling remote users' web traffic to the data center negatively impacts performance and user experience. The practice of bypassing traffic inspection for trusted SaaS applications, such as those from Microsoft, is increasingly risky, with over 50% of malware infiltrating through these trusted SaaS application channels.

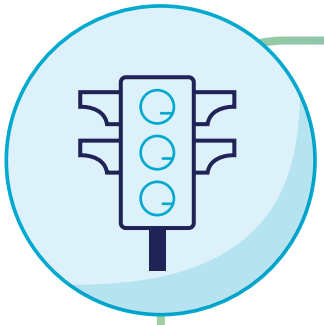
Consider steering traffic directly to a Security Service Edge (SSE) platform to secure web and SaaS traffic from distributed users going to distributed locations effectively balancing security measures against malware and data breaches, without compromising an optimal user experience.

This is a great first project for security and networking groups to collaborate and find efficient ways to protect against advanced and cloud-enabled threats with safeguards data across all vectors (any cloud, any app, any user).

> Remote enterprise assets should be able to access enterprise resources without needing to traverse enterprise network infrastructure first.
>
> NIST Special Publication 800-207

Effective Web and SaaS security solution must-haves

Traffic Inspection and Management	Implement Single-Pass SSL Inspection to decrypt and inspect all web and SaaS traffic, and TLS/SSL fingerprinting for undecryptable traffic, without impacting user experience, and Instance Awareness to identify unique SaaS app instances for policy enforcement. Use dedicated IPs to support IP-allow lists and filtering without backhauling traffic or limiting the number of PoPs
Adaptive Zero Trust Security and Access	Ensure protection that leverages AI for hybrid/remote users anywhere and continuous trust-based access to SaaS, evaluating identity, device, location, app trust score, behavior trust score, app instance, activity, and data.
Threat Protection	Provide comprehensive, real-time zero-day protection, global threat intelligence and protection against various types of cyber threats, plus continuous and committed effort to improve and maintain healthy threat efficacy scores. For new unknown and zero-day threats , ensure threat efficacy in real-time at time-zero (T+0) for the breadth of executable (PE files), non-executable (non-PE files), and phishing attacks.
User Experience and Compliance	Enhance security awareness across the workforce by implementing flexible coaching actions such as blocking, gentle warnings, redirection, and requiring justification. Use analytics to track the real-time effectiveness of these coaching measures.



Positive Impact of Netskope One Platform

- Deliver fast, reliable performance worldwide, scaling seamlessly to provide an enhanced user experience with widespread local coverage.
- Consolidate and automate your network and security stack into a unified platform, including a single console and policy framework, at a lower cost.
- Deploy Zero Trust principles by continuously evaluating every SaaS transaction
- Apply malware protection to all SaaS traffic and control sensitive data movement
- Provide fast and secure access for users connecting to any application from anywhere
- Real-time user coaching where users are guided on better security and digital practices.
- Safely enable generative AI applications

STRATEGY 4: MODERNIZING YOUR CONNECTIVITY WITH ZERO TRUST ARCHITECTURE

As companies strive to reduce the cost and complexity associated with traditional WAN connectivity, such as private MPLS circuits that require traffic backhauling, they are moving away from site-to-site VPNs and embracing zero trust architecture. This shift involves utilizing the public internet for network transport and transforming office networks into environments similar to 'internet cafes,' where the connectivity experience is seamless and consistent from any location.

Many existing SD-WAN solutions intended to facilitate this transition often fall short in providing the necessary security, efficient monitoring, and simplified management. Consider using next-generation SD-WAN solutions that not only reduce costs and complexity but also enable context-aware traffic routing, and implement zero trust principles, by enabling end-to-end integrated security for any user, anywhere. These solutions must enhance network performance, security, and operational efficiency, ensuring seamless connectivity and robust protection for modern enterprises.

SD-WAN Effective solution must-haves

Application Management: Support all apps	Automatically recognizes and prioritizes numerous cloud applications without manual QoS configuration, and supports web, non-web, and legacy applications with server-to-client, client-to-client, and bidirectional connectivity.
Performance and uniform resilience	Ensure protection that leverages AI for hybrid/remote users anywhere and continuous trust-based access to SaaS, evaluating identity, device, location, app trust score, behavior trust score, app instance, activity, and data.
Security and Compliance	Ensures consistent application performance and security policies across all locations, integrates advanced firewall and IPS in the SD-WAN gateway, and secures both managed and unmanaged devices by detecting and isolating threats
Operational Efficiency	Consolidates wireless, Wi-Fi, and switching products into a single AI-driven platform, streamlines operations, offers remote management, and provides a unified management interface for network and security.

Positive Impact of Netskope One SD-WAN component

- Enable secure and optimized access to 80k+ SaaS applications
- Deliver SD-WAN capabilities directly on a user's laptop through a unified SASE client
- Provide first class support for micro branches and instantly extend cellular reach (with wireless WAN)
- Support multi-cloud networking and intelligent access for IoT
- Ensure secure and optimized connectivity for hybrid working environments, enabling end-to-end integrated security for any user, anywhere
- Simplify operations with ML insights

STRATEGY 5: MODERNIZING FULL REMOTE ACCESS CONNECTIVITY

For two decades, organizations have used VPNs to connect remote workers to corporate networks under the castle-and-moat security model. However, with both the shift to hybrid work and the move of internal apps from data centers to public cloud, accessing private applications has become slow, cumbersome and a sub optimal user experience.

Prioritize this project by considering the proportion of users working outside corporate offices and the type of applications being used along with their performance requirements. Routing all traffic through the data center is inefficient, especially when most traffic is directed to the web from data centers to access private applications now residing in the cloud.

Consider steering traffic directly to its destination with proper security controls and replacing VPNs with a Zero Trust Network Access (ZTNA) solution, a component of most SASE platforms and a core part of SSE. This approach enhances application performance, improves security, and reduces unnecessary traffic through the data center, benefiting both users and the internal network.

Effective ZTNA solution must-haves

Continuous adaptive trust controls	To strictly enforce least privilege access, ZTNA should use extensive risk context from users, devices, applications, and data, to calculate the dynamic risk score of a user and continuously verify their trust level for every access request.
Coverage of all enterprise applications/use cases	Support any TCP and UDP web application, as well as non-web and legacy applications like VoIP and Remote Assistance that require server-to-client, client-to-client, and bidirectional connectivity.
Support for managed and unmanaged devices	Offer both agent and agentless deployment methods to support internal employee access from corporate managed devices as well as third-party access and employee BYOD.
Universal ZTNA	Extend beyond remote access and provide local enforcement in on-premises campus and branch environments without the need to be forwarded to the cloud for inspection.
Optimize voice & video traffic	Process and optimize more demanding (i.e., high bandwidth) voice/video application traffic, and not bypass it, while maintaining quality of service (QoS) capabilities.
Integrated SD-WAN capabilities	Integrate SD-WAN capabilities to ZTNA with a single client for enabling secure and optimized connectivity to all private applications, including on-premises hosted VoIP, video, and remote assistance, allowing organizations to completely replace their remote access VPN solutions.

Positive Impact of Netskope One Private Access component

- Completely replace remote access VPN solutions (legacy VPNs)
- Improve productivity and Secure hybrid work with faster and safer zero trust–based connectivity for remote users
- Enhance the user experience and reduce helpdesk and network ops tickets related to connectivity
- Lower costs and simplify management by consolidating solutions for accessing legacy and modern applications
- Improve app discovery and rationalization to support business objectives
- Integrate VoIP & remote assistance (apps using server-initiated connections)
- Secure third-party and BYOD and achieve M&A acceleration for quicker time to value

STRATEGY 6: ACHIEVE OPERATIONAL EXCELLENCE WITH A CLOUD-NATIVE PLATFORM AND DIGITAL EXPERIENCE MONITORING (DEM)

The shift to a more distributed and dynamic digital infrastructure based on hybrid workforces, SaaS applications, and cloud hosting has created a visibility gap, making user experience and performance management more challenging for IT organizations.

Achieving operational excellence involves consolidating and automating your network and security stack into a unified platform with a single console and policy framework, reducing costs and enhancing efficiency. Emphasizing convergence and adopting a cloud-native platform simplifies operations, providing end-to-end visibility, scalability, and improved performance.

Additionally, an integrated digital experience monitoring (DEM) provides end-to-end visibility that overcomes the limitations of legacy tools, mapping out the full path and infrastructure between endpoints and applications to detect and diagnose any bottlenecks along the way.

Together, these approaches streamline management and significantly improve network performance and user experience, creating a modern, efficient enterprise network.

As per Gartner® "By 2027, DEM will use synthetic and real user monitoring to enhance the user journey and better understand user interactions of SaaS applications and services."

Gartner, Market Guide for Digital Experience Monitoring, By Mrudula Bangera, Gregg Siegfried, Padraig Byrne, 20 November 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Effective DEM solution must-haves

Full Observability	True real user experience monitoring that combines real-user monitoring with synthetic traffic to provide a unified view across network, application, endpoint–and security–management domains.
Transparent Insight into SASE	Provide complete transparency into and beyond the SASE platform reveals how user activity, risk profile, activated security policies, and protection contribute to the user experience.
Proactive remediation	Provide actionable insights to the SASE cloud to proactively preempt issues, continuously optimize performance, and consistently deliver a first-rate user experience.
Intelligent Insights	Leverage AI-powered analytics to diagnose, predict and prioritize events impacting user experience, application performance and availability.

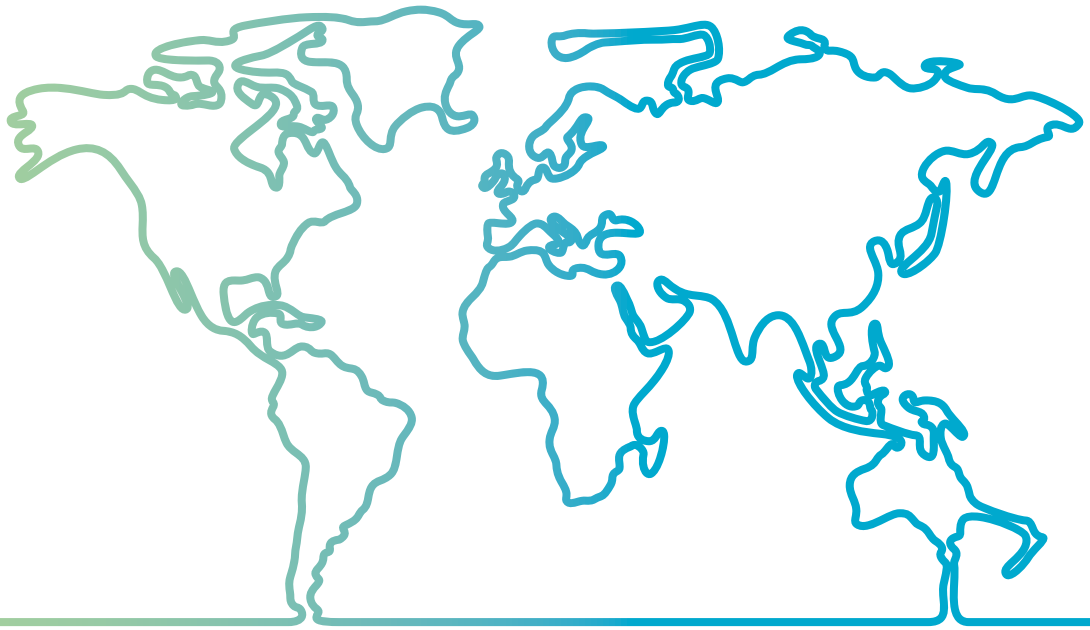
Positive Impact of Netskope One Digital Experience Management (DEM)

- Enable comprehensive visibility into real user experience using real and synthetic traffic.
- Implement Zero-touch monitoring for the top 40+ business critical applications.
- Provide performance transparency across all domains
- Improve operations with role-centric dashboards including tailored analytics for IT, NetOps and SecOps teams
- Accelerate problem detection, diagnosis, and resolution with AI insights and alerts
- Integrate seamlessly with existing management systems

STRATEGY 7: ENHANCE PERFORMANCE WITH THE RIGHT UNDERLYING SASE ARCHITECTURE

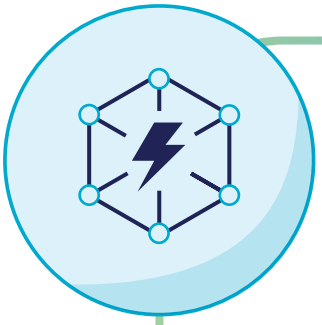
Often times, the need for speed and performance is on a collision course with the need for more security. The network can't be insecure, but neither can the necessary security slow down the network. In reality, both security and a phenomenal user experience could be simultaneously and seamlessly delivered—without any tradeoffs.

When evaluating SASE, it's crucial to note that not all solutions are created equal. By choosing a high-performance SASE cloud infrastructure, organizations can significantly enhance network performance while maintaining robust security. An optimized, purpose-built private cloud infrastructure and network with ultra-fast full-compute data center coverage in every country for users, devices, and branches, as well as extensive peering relationships with tier one cloud providers can truly deliver unmatched latency and availability. This strategic approach ensures that the network is prepared to meet current demands and future challenges effectively.



Effective SASE Cloud Architecture solution must-haves

Global Presence	Offers global access from anywhere, powered by data centers with full compute and all the security services available in every region, eliminating reliance on virtual PoP or backhauling.
Speed & Performance	Minimizes the latency of traffic processing/inspection from user to the destination by optimizing the connectivity and leveraging single-pass architecture.
Scalability & Flexibility	Ability to handle all the data traffic and scale with the organization's growth and evolving IT strategies. All SASE services should be available at each PoP to truly embody a distributed service edge.
Interconnect strategy	Control where and who to peer with and how the traffic is route. By combining direct peering with multiple and varied transport providers we can provide market leading resiliency and performance.
Reliability	Include over provisioned data centers for maximum reliability. Adapt both inbound and outbound routing to mitigate issues caused by third party networks, Internet, or weather events.
Connectivity Options	Provide options for connecting to the SASE cloud, including client, clientless, IPSec/GRE tunnels, SD-WAN, private network interconnect (direct routing to the SASE cloud), Dedicated Egress IP (to restrict access to critical applications and cloud services without backhauling traffic).



Positive Impact of Netskope NewEdge Network

- Provide fast & reliable performance with a global footprint (75+ regions including China) and extensive peering relationships (+4K network adjacencies)
- Ensure peak speed and resilience with Industry-best SLAs for latency, decryption, and single-pass inspection
- Provide transparent End-To-End Visibility and a local user experience regardless of location
- Scale to handle growing user and traffic volumes without performance trade-offs
- Simplify your network and reduce cost and management overhead
- Ensure data sovereignty and compliance by controlling your traffic and data in motion and at rest

CALL TO ACTION

Begin your network security transformation journey today by assessing your current infrastructure, setting clear objectives, and partnering with a technology provider like Netskope that can help navigate the complexities of modern networking solutions. Netskope offers advanced tools and expertise that can streamline your transformation process, from planning and implementation to ongoing management and optimization.

Discover how Netskope can accelerate your Network Security Transformation journey with the ideal SASE architecture, visit **netskope.com/netskope-one**

Interested in learning more?

Request a demo

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.