netskope

White Paper

Evolving Your Network Security From Today to Tomorrow

+ How To Transition To Cloud-Native Network and Web Security

Table of Contents

INTRODUCTION: THE PROBLEM WITH LEGACY NETWORK SECURITY

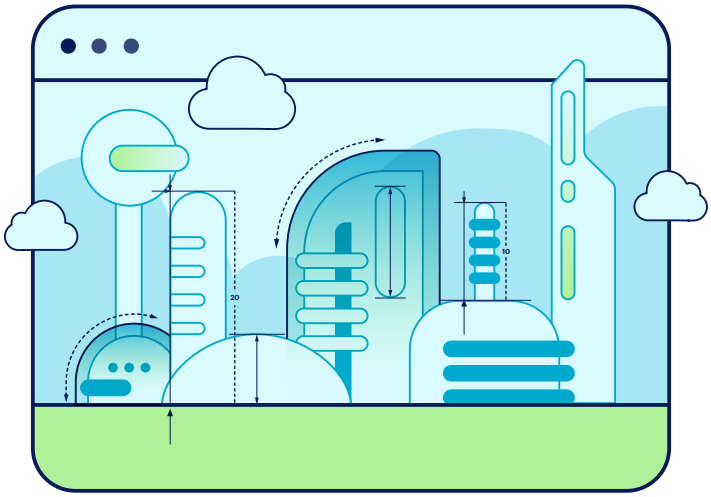
Networking teams and the wider infrastructure and operations (I&O) group are jointly responsible for the performance and security of an organization's network. A key aspect of that work is inline network security—monitoring and blocking potentially malicious data traffic in real time.

For many years, discussion about the best way to do this would focus on the merits of firewalls versus proxy gateways. While different practitioners preferred one or the other, depending on their organization's circumstances, this was the extent of their choice.

But recently that conversation has been completely overtaken by events. Hybrid work and cloud-based architectures have become the new reality for millions of organizations around the world, through a process accelerated by the COVID pandemic but with roots in long-term technological changes.

In this context, the inadequacies of legacy network security systems are clear. Traditional firewalls and proxy gateways struggle with scalability, performance, and visibility in cloud-first and remote work environments. That leads to inefficiency and security gaps. Legacy systems are simply not fit for purpose in our era of hybrid and remote working.

Today's organizations urgently need cloud-native security—such as security service edge (SSE) solutions—that provide scalability and flexibility, and align with zero trust principles. The technology answers are all there, but the challenge for the teams responsible is how to transition from legacy systems to modern solutions like SSE in a thoughtful way, without increasing ongoing investment, or leaving security gaps as they migrate to new ways of working.



AN OVERVIEW OF CLOUD-NATIVE NETWORK SECURITY SOLUTIONS

Cloud-native network security solutions such as SSE enable scalability, performance, and security for increasingly distributed organizations

Three elements of these modern network architectures are particularly important.

Zero Trust Network Access (ZTNA): Enforces the premise that no one is blindly trusted and the implementation of least-privilege access, selectively granting access only to resources that people or groups of people require, nothing more.

Secure Web Gateway (SWG): Provides fine-grained control and security for internet access, and addresses cloud-enabled threats and data risks for personal instances of managed applications, thousands of shadow IT applications, and cloud services.

Firewall-as-a-Service (FWaaS): Provides consistent network security for all outbound ports and protocols for safe, direct-to-internet access via an agent on managed devices or via Generic Routing Encapsulation (GRE) and Internet Protocol Security (IPsec) for offices. Often integrated components include DNS Security and Intrusion Prevention Systems (IPS) to detect and prevent DNS initiated attacks, and identify threats in real time, respectively.

Cloud-native network security solutions such as SSE enable scalability, performance, and security for increasingly distributed organizations.

REAL-WORLD BENEFITS

Four ways modern security infrastructure drives business value

Transitioning to cloud-native SSE enables organizations to strengthen their network security. But it brings other benefits too. By modernizing their infrastructure, SSE architectures actually reduce costs, streamline operational processes for efficiency, and improve network performance for improved user experiences. Taken together, these benefits better position organizations for success in our digital age.

BENEFIT	IMPACT
Consolidate Infrastructure By consolidating network security infrastructure into a modern cloud-based system, organizations can sunset legacy systems and solutions.	Organizations benefit from reducing costs related to physical servers, networking equipment, and associated upkeep. Forrester estimates that shifting from legacy security to Netskope's Security Service Edge (SSE) solutions generates a 109% ROI over three years for a typical organization, with a break-even point of less than six months, and infrastructure consolidation savings alone of $5.4m.*
Simplify Security Operations and Management With streamlined workflows and automated processes, teams can focus on strategic initiatives rather than day-to-day technical issues.	Organizations can save time, for their network and broader I&O teams, and among their wider workforce, thanks to simpler processes. Forrester estimates that Netskope's SSE solutions help security teams regain more than 35,000 work hours, valued at $1.5m, allowing them to focus on more impactful activity. Meanwhile, nearly 30,000 hours of remote user effort is avoided across the organization, as users no longer need to continually engage in time-consuming VPN processes.*
Improve Network Performance Modern cloud infrastructure is faster and more reliable, with less downtime, fewer disruptions, and higher detection rates.	With modern and agile systems in place, organizations can achieve an 80% reduction in help desk volumes and a 60% reduction in mean time to resolve (MTTR) incidents with Netskope's SSE solution, according to Forrester. Netskope's SSE provides greater visibility into the user environment, ultimately improving network protection and data loss prevention. Netskope also delivers a 15% reduction in unplanned downtime.
Strengthen Defenses Cloud-native solutions are more effective at understanding and blocking cyber threats	Netskope's modern SSE solutions can deliver an 80% reduction in the risk of a severe breach caused by an external attack, according to Forrester.

*Based on a composite organization that is a multibillion-dollar firm with 60,000 employees (full-time equivalents) worldwide, half of whom require remote access to private corporate apps.

How cloud-native solutions support modern working habits

Changing behavior drives new security approaches.

In the years before the COVID pandemic, on average fewer than 20% of an organization's employees and workers were remote. Now there are many organizations where that's anywhere from 50% to 100% on certain days of the week, as hybrid working policies become mainstream.

This means that remote, web, and SaaS access—and their associated security functions—have fundamentally changed. Organizations increasingly rely on cloud-hosted secure web gateway (SWG) and Firewall-as-a-Service (FWaaS) components, delivered within security service edge (SSE) platforms. While edge firewalls remain necessary for managing inbound access requirements (in data centers and public cloud, where applications reside), they are no longer needed at branch locations: stores, branch or regional offices.

Zero trust network access (ZTNA) is also replacing VPNs as the standard approach for securely giving access to public-facing exploitable services remotely and enabling lateral movement once inside. The more secure "inside-out" connection model of ZTNA gives users direct access to desired applications or resources only, limiting the reach of any malicious actors.

Content and context are now essential for real-time adaptive access control

Modern networks, built around ZTNA principles, take a more contextual and real-time approach to analyzing content and making security decisions than their legacy counterparts. These more adaptive and intelligent networks are appropriate for our new generation of business agility, remote working, and cloud-based access.

Inline inspection of Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) content and context in real time is the future of access control for SSE solutions. In previous technological eras, firewalls perfected the inspection for network traffic and SWGs did the same for web traffic. Now SSE brings these controls together with inline cloud access security broker (CASB) content and context inspection.

Based on application risk, behavior risk, device posture, activity, data sensitivity, or other variables, adaptive access control is applied to every business transaction for its content and context.

If a user desires to delete 100 files of company sensitive data, adaptive access can request a step-up authentication or request a justification from the user. If another user wants to access an unmanaged risky cloud storage application to move files, adaptive access can warn them and provide safer company-approved cloud storage options.

This "real-time coaching" approach is much like satellite navigation (or GPS) when driving today: alerting users to potential wrong turns and redirecting them to safer alternatives when appropriate. Modern enterprise users can benefit from this sort of guidance as they move around their networks.

MIGRATING WITH CONFIDENCE

A framework for phased SSE implementation

Moving from legacy network security systems to modern SSE solutions doesn't have to be done all at once. In fact, it shouldn't be. A phased approach, transitioning over time and building methodically on successful implementations, provides the best way to deliver improved results without risking performance, while also maximizing existing investment.

KEY STEPS	BEST PRACTICE
Initial Assessment and Planning Begin by assessing your current security posture and identifying gaps that SSE can address. Evaluate your network architecture, existing security solutions, and specific business needs to understand where SSE can be most beneficial.	Develop a clear strategy for SSE deployment that includes defining objectives, expected outcomes, and key performance indicators (KPIs).
Choosing the Right SSE Provider Evaluate potential SSE vendors based on their ability to meet your specific requirements and use cases. Consider factors such as the comprehensiveness of their security services, underlying architecture, ease of integration with existing systems, customer support, and cost-effectiveness.	Conduct a pilot test with short-listed vendors in your environment to see how the SSE solution can handle your specific security needs, network traffic patterns, and visibility requirements.
Deployment in Phases Work with your chosen vendor to configure the SSE solution to meet your specific security policies and compliance requirements. Customization may involve setting up security rules, configuring data loss prevention (DLP) settings, and defining access controls.	Integrate the SSE solution with existing IT infrastructure, such as identity management systems, network infrastructure, and other security tools. Proper integration is vital for seamless operation and maximizing the value of your SSE solution, so assess vendors on the basis of their partner ecosystem and integrations.
Focus on User Experience Provide comprehensive training before each phase of deployment. Communicate changes well in advance, and monitor user feedback to address friction points quickly.	Use analytics to track security effectiveness and user adoption. Maintain audit trails to demonstrate security improvement over time.

The foundations for long-term success

Why zero trust frameworks matter

As the traditional network perimeter has dissolved, with the rise of remote work and cloud services, the zero trust approach has become fundamental to effective network security. Zero trust principles seek to remove implicit access, refine least-privilege access, and continuously monitor. This reflects the escalating sophistication of cyber threats, and provides better visibility and control for security practitioners.

The average organization uses more than three times the number of genAI apps—and has nearly three times the number of users actively using those apps—in 2024, compared to the prior year.

However, the zero trust approach is often misunderstood, with many explanations focusing solely on secure access for zero trust and missing the fact that data flows through all the other zero trust components (users, applications, devices, and networks).

SSE solutions combine CASB and SWG capabilities into a core inline proxy with FWaaS and ZTNA, redefining the traditional NGFW and VPN roles to support zero trust principles. As a result, your infrastructure is more resilient and secure. Importantly, SSE has the scale and performance for any user, device, or location to provide a great user experience, removing the trade-off of performance versus security for content visibility.

Proprietary source code sharing with genAI apps accounts for 46% of all data policy violations.

With a zero trust framework and modern SSE solution, enterprises have a solid foundation for sustainable security that can scale and adapt as the enterprise grows and transforms, while maintaining consistent security controls across all environments and use cases.

The impact of AI

Artificial intelligence (AI) and machine learning (ML) have been used in the background for many years for threat defense engines, data classification, URL dynamic ratings, and IT operation planning, among other areas. Now AI and ML-based defenses are moving inline to work in real time to detect new unknown zero day threats and identify sensitive data in documents and images.

Regulated data, driven by industry regulations or compliance requirements, accounts for 35% of all data policy violations, and intellectual property for 15%.

The AI boom itself enables both good and bad actors to quickly develop new code and content, and learn quickly. In this sense, AI is both a boon and lure, with the potential to expose sensitive data. For example, the most popular content supplied to AI applications like ChatGPT has been source code.

Legacy defenses are not in a position to allow company instances of AI versus controlling public and personal instances for users. Nor can they provide the ability to identify content like source code being fed into AI applications.

In contrast, inline AI/ML-based defenses are detecting malicious executable files and phishing attacks, and classifying dozens of documents and images, including source code, today. As AI applications and use cases rapidly gain adoption across enterprises, any future-proofed network security strategy must be able to respond to these kinds of risks.

CONCLUSION: THE SECURITY EVOLUTION IMPERATIVE

Enterprise technology and individual behavior constantly evolve. We've seen the reality of that up close in recent years, as the shift to the cloud, the explosion in remote and hybrid working, and the rise of AI have all transformed our daily lives.

For networking and infrastructure and operations professionals, the urgent requirement now is to modernize architectures in alignment with the changes happening around them. There are two sides to that process.

First, teams should carefully analyze their legacy systems. There's an ongoing shift to SaaS and IaaS inline inspection, more inline AI/ML defenses, and providing adaptive access with real-time coaching to users. In this context, renewing NGFW, SWG, and VPN solutions could be costly mistakes.

Second, organizations should map out a migration to modern SSE solutions. Breaking this into phases is the best way to make it manageable and effective. It avoids simply abandoning existing systems and helps networking teams build confidence in new ways of doing things across the business.

As the IT landscape continues to evolve, what will likely define an organization's success is how quickly it can adapt to those ongoing changes and capitalize on their impact. For networking and infrastructure and operations practitioners, while it can seem like a complicated shift to navigate, it can be made simpler, and ultimately promises significant rewards in performance, productivity, and cost savings.

Interested in learning more?

Request a demo

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs.