eBook

Security and Networking Cost Savings in a Hybrid Work Environment

netskope

Security and Networking Cost Savings in a Hybrid Work Environment

The COVID-19 pandemic made remote work the modus operandi for white-collar employees around the world. In response, corporate networking and security teams scrambled to support newly remote staff. They needed to provide high-performance yet secure connections to data and applications, both on company premises and in the cloud. Now, as more and more businesses embrace hybrid work models, where employees can come back into the office for one or more days per week, networking and security teams are again scrambling—this time, to build out wide-area networks (WANs) and security capabilities that support hybrid work.

At the same time, the external climate of uncertainty has many companies in belt-tightening mode. These teams must continue to support the evolving work landscape, but do so cost-effectively. That's why it is time for them to rethink hybrid work, as networking and security teams should be looking to optimize their WAN connectivity and security capabilities.

Secure access service edge (SASE) architecture represents a way to bring both security service edge (SSE) and WAN edge, or SD-WAN, capabilities together in a unified platform. This eBook will show you how your organization can save by implementing these unified, consolidated capabilities in your hybrid work environment.

Security and Networking Cost Savings in a Hybrid Work Environment

Source of Savings #1 | Platform Consolidation

Source of Savings #2 | Streamlined Networking Infrastructure

Source of Savings #3 | VPN Infrastructure Replacement

Source of Savings #4 | Transition From CapEx to OpEx

netskope

01

Security Platform Consolidation

To secure remote users accessing web, cloud, and private applications, security teams have launched an assortment of solutions over the past few years, often including:

- A secure web gateway (SWG) designed to provide protection, visibility, and control of user traffic to websites, managed or unmanaged Software-as-a-Service (SaaS) solutions, cloud service providers, and public-facing custom apps.
- A cloud access security broker (CASB), which enables identification of risks in users' access to cloud applications and management of potentially problematic traffic, including inappropriate data exfiltration.
- A zero trust network access (ZTNA) solution, to securely connect users and devices over the internet to the servers and applications they need, either in the data center or public cloud.
- A data loss prevention (DLP) solution, to consistently secure sensitive data companywide.
- A cloud-based Firewall-as-a-Service (FWaaS) to secure all ports and protocols used by non-web traffic.

Each of these capabilities is crucial in protecting users, applications, and data. But deploying a separate solution in each category is highly inefficient.

01

Security Platform Consolidation

How SASE creates cost savings:

Harnessing multiple separate security and networking services is a costly approach to cloud security. Not only does each solution come with its own price tag, but ongoing management of the various products, via different consoles, consumes a lot of staff time. And integration of the different solutions is usually time-consuming and expensive.

Security teams want to avoid sending end-users through different security solutions as they access different types of resources—for example, one solution for web browsing, another solution with a different login for SaaS applications, a third for private apps, and so on. An infrastructure with this much friction would drive some users to bypass security altogether, leading to increased effort and cost dealing with data loss and security incidents. So, most IT teams stitch together security and networking solutions so that users can log in once and access everything they need. This integration improves the end-user experience but is a significant cost driver for cloud security. Compounding the cost of each solution's licensing fees, multisystem integration gets expensive fast.

That's where security service edge (SSE) capabilities, as part of a SASE architecture, can bring major cost benefits. SSE was developed to consolidate the stack of tools needed to secure companies' evolving cloud edge. The capabilities typically encompass SWG, CASB, DLP, and FWaaS technologies, among others, providing traffic and data inspection as close as possible to the user. From a pricing perspective, companies usually buy the various components of a unified SSE platform for a single fixed price and the capabilities are integrated as part of the converged platform, so the security team does not need to spend significant time and money tying the technologies together.

Moreover, an SSE platform enables staff to save time on ongoing management of the cloud security infrastructure. They can manage all threats—across the SWG, CASB, DLP, and firewall—from a single pane of glass, saving time on investigations and incident response. One configuration of data protection rules permeates the entire cloud security infrastructure, providing economies of scale from a management perspective. Furthermore, when integrated with SD-WAN, organizations can benefit from a full SASE architecture that meets the needs of both security and networking teams.

02

WAN Infrastructure Modernization

The typical WAN of the pre-cloud era had a hub-and-spoke architecture and companies made significant investments in security hardware that resided in a corporate data center. To ensure user communications were protected by this best-of-breed security infrastructure, the company backhauled traffic from every branch office to the data center. Whether the user wanted to access sensitive information in on-premises finance systems or just casually browse the web, all packets traveled through the data center before moving on to their final destination, a process often referred to as “hairpinning.”

Hairpinning made sense when the majority of corporate data and applications resided on-premises, but as the majority of these resources have migrated to the cloud, an inordinately high volume of traffic is traveling to and from the data center unnecessarily. Maintaining adequate network performance required large-bandwidth pipes, and even then, high latency costs would ensue. In addition, the connections from branch offices to the data center were generally multiprotocol label switching (MPLS) links, which are expensive and much slower than their modern broadband counterparts. The modern cloud security model not only improves this architecture, but leads to significant networking infrastructure cost savings.

WAN Infrastructure Modernization

Because SASE brings unified security and networking capabilities to the cloud, branch offices no longer need to connect to the data center before users can access websites, or cloud-based applications and data. Most companies still run a subset of their applications on-premises, and offsite traffic to those systems obviously needs to reach the data center. However, all other branch-office traffic can connect directly via the cloud-based SSE platform, which inspects and routes the traffic onward. This approach reduces the costly bandwidth required to route to and from the data center by as much as 50%, which provides significant savings for a tight IT budget.

Moreover, companies taking this direct-to-internet approach typically use technologies such as software-defined WAN (SD-WAN) to tie branch offices to the internet and the data center. This means they can provide connectivity via broadband links, which are much less expensive than leased MPLS connections. Consider the savings a company could achieve by replacing an MPLS that, for example, costs $6,000 per every gig of bandwidth to every remote office with commercial broadband at a fraction of that cost.

In addition, leveraging SASE as the on-ramp to the cloud can also deliver savings by leveraging the peering relationships that the SASE provider has established. Whereas many networking teams may need to invest in costly interconnects like Microsoft ExpressRoutes, AWS Direct Connect, or GCP Interconnect in order to provide their users with fast access to these cloud services, customers can now enjoy fast, optimized connections to these services by simply connecting to the SASE service and benefiting from their optimized peering relationships.

All told, a cloud-direct networking infrastructure can have a huge impact on WAN costs.

03

VPN Infrastructure Replacement

Just as organizations used a hub-and-spoke WAN to connect branch offices to the data center, many companies have long relied on virtual private networks (VPNs) to connect offsite individuals to the corporate networks. Remote workers might use an assortment of resources on the corporate network as a standard part of their day-to-day responsibilities. They might still be required to use VPN even for connections to cloud-based resources. And like MPLS backhauling, cloud access via VPN can be convoluted and lead to the same hairpinning problem. SSE offers a more efficient approach.

VPN Infrastructure Replacement

An SSE solution, as part of a SASE framework, can replace legacy VPN connections with zero trust network access (ZTNA). The SSE solution can verify a user's identity upon connection and then use contextual telemetry from ZTNA to limit access to resources based on that user's explicit permissions. This ensures that workers can utilize all the appropriate resources—SaaS solutions, websites, applications in the public cloud, etc.—no matter where they are physically located, while protecting those resources from anyone who doesn't need access.

Just as important as the improved zero trust security approach, ZTNA significantly improves the end-user experience by accelerating cloud connectivity, while also substantially reducing costs. A company providing remote users access to internal resources through VPN technologies must install VPN concentrator hardware in every location that houses those resources. If the user is trying to access the web or cloud resources, they first need to connect to the VPN concentrator and then hairpin back out to the internet. The pricey concentrators and end-user licensing place a drag on both network performance and the budget.

ZTNA capabilities, under the umbrella of an SSE solution, can integrate with the company's existing network. These zero trust capabilities reduce demands on security administrators, because they can be managed through the same console as the rest of the SSE technologies. They also eliminate the need for heavy VPN clients and concentrators. And by sending remote users directly to their cloud or web destinations, ZTNA can reduce traffic into and out of the data center, further reducing the cost of the organization's networking infrastructure.

04

Transition From CapEx to OpEx

Several years ago, as companies were considering the benefits of moving to the cloud for core back-office functionality, “cloud operationalization” was a major selling point. What were once large upfront capital expenditures (CapEx) could be turned into recurring monthly costs. SaaS and other cloud applications substitute predictable operating expenditures (OpEx) for the risk of one-off surprise spending that might result from, say, an onsite hardware failure. System maintenance and updates require less—if any—internal staff time. Plus, scalability and flexibility are far superior to what onsite systems can provide.

These selling points of every cloud application apply to cloud-based SSE solutions as well.

Risk-aware data protection, a zero trust-ready model

Shifting a robust security platform into the cloud means that a substantial segment of the organization's IT budget transitions from CapEx to OpEx. Instead of spending $1 million on a new box whenever software reaches end-of-life or hardware dies, a company might commit to paying $100 per user per month. The numbers vary widely depending on the product and capabilities, but the idea holds: SSE solutions achieve the same basic objectives as onsite security, yet they come at a steady, predictable, and easily budgeted cost.

Even more important than cost savings, in this day and age, is cost flexibility. With the traditional approach to security, a company that spends $1 million on legacy infrastructure is stuck with those technologies for several years or more. But like most cloud solutions, SSE platforms as part of a SASE architecture can expand or contract on short notice.

If a sizable proportion of a company's workforce were to immediately start working from home, the security team could rapidly ramp up the SSE capabilities. Conversely, if all remote workers suddenly returned to the office, the SSE platform could quickly scale down, as could its cost structure. Whichever direction hybrid work is headed, a company using an SSE platform can scale and optimize its cloud security environment to best suit their needs.

At a time of global uncertainty, being able to secure all cloud traffic—without carrying unnecessary buffers of bandwidth, hardware, or software licenses—is priceless.

To be truly effective, a zero trust data protection solution needs to monitor what's taking place and who's doing what across the entire corporate infrastructure, including clouds, remote users, and unmanaged devices.

Summary

Utilizing a SASE approach, with SSE and SD-WAN capabilities, improves network performance and worker productivity while reducing security risk, but the most important benefit in these uncertain times might be its substantial cost savings.

Hybrid work is here to stay. Many employees love the flexibility of remote work and saving time on their daily commute. Many executives feel that onsite staff are more productive and collaborative with other members of their teams. The compromise is a hybrid workforce, who regularly perform their jobs from both office and home. A recent Gartner® report predicted that 75% of workers will split time between home and traditional office locations by 2026.[1]

Thus, securing remote workers, as well as cloud applications and data, will remain core responsibilities for corporate security teams, for the foreseeable future. Cloud security technologies may seem challenging to implement cost-effectively, however, SSE capabilities provide a solution by substantially reducing costs while improving end-user performance and productivity.

[1] Gartner, "Top Network Practices to Support Hybrid Work," April 2022.

For More Information

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. The Netskope Intelligent Security Service Edge platform is fast, easy to use, and secures people, devices, and data anywhere they go.

Learn how Netskope helps customers be ready for anything on their SSE journey, **visit netskope.com.**

netskope