Brought to you by:

netskope

SASE Architecture

for dummies

A Wiley Brand

Master cloud and SaaS security

Modernize your network and security architecture

Improve and maintain network performance

Netskope 2nd Special Edition

Steve Riley

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 trade-offs. Learn more at netskope.com.

We would like to thank a number of individuals that made publication of this book possible:

From Netskope: Amanda Anderson, Mike Anderson, Robert Arandjelovic, Chad Berndtson, James Christiansen, Tom Clare, Trevia Clark, Rich Davis, Mark Day, David Fairman, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Mariesa Milan, Krishna Narayanaswamy, Kate Reid

From Evolved Media: Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

SASE Architecture

Netskope 2nd Special Edition

by Steve Riley

for dummies®
A Wiley Brand

SASE Architecture For Dummies®, Netskope 2nd Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-26428-5 (pbk); ISBN 978-1-394-26429-2 (ebk); 978-1-394-30421-9 (ebk)

Publisher’s Acknowledgments

Some of the people who helped bring this book to market include the following:

Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Account Manager: Jeremith Coward

Production Editor: Saikarthick Kumarasamy

Special Help: Chad Sievers

Table of Contents

Introduction

Your employees, partners, and customers increasingly use the cloud instead of private networks and data centers. This shift toward work-from-anywhere models and a greater reliance on cloud services has been ongoing and was inevitable. This evolution is now the standard. Remote work and cloud integration are intertwined. Each drives and reinforces the other, establishing a new norm in how organizations operate and secure their environments.

But security can't inhibit people's ability to do their work. Balancing security, user experience, and complexity was always challenging. The challenge is compounded now that you must realign security for an environment that, if you're still using traditional security tools, is outside your control.

The widespread distribution of remote employees, applications, and data across the cloud — the new normal — eliminates the viability of traditional castle-and-moat security methods, exposing organizations to new risks. The complexity of this new security landscape has challenged even the best security teams and increased the chance of misconfigurations and breaches.

The fundamental issue is that traditional security and data center architectures are misaligned with today's digital transformation where the majority of users and applications operate remotely. We've reached a breaking point where maintaining security through a centralized data center approach is impractical and unsafe. Conflicting products, services, and industry messaging further challenge security decision-makers trying to support opportunities for business innovation while refactoring security to suit their needs.

The architecture called *secure access service edge* (SASE; pronounced "sassy") is the proven way forward. It has completely reshaped how we approach networking and security. There are two tightly integrated halves to SASE:

- **Security service edge (SSE):** This aspect of SASE focuses on minimizing security risks and protecting business elements in the cloud. SSE converges critical elements like secure web gateways (SWGs), cloud access security brokers (CASBs), zero trust network access (ZTNA), data loss prevention (DLP), threat protection, firewalls, and remote browser isolation (RBI).

- **Software-defined wide area network (SD-WAN):** The networking half of SASE, SD-WAN, ensures optimized and reliable connectivity, complementing the security measures of SSE by efficiently moving and managing network traffic to and from resources.

SASE represents a unified system that combines key network and network security services. But how to architect it all the right way and in the right sequence? That's where this book comes in.

About This Book

This book can help you develop a road map for implementing networking and security projects that will deliver positive, incremental results in the near term while paving the way for a resilient, secure future that's cloud-first. It cuts through the marketing blather you receive from purported SASE vendors, giving you a practical understanding of what SASE is — and isn't — and enabling you to future-proof your investments in security and networking to ensure that adapting to inevitable changes is as easy and cost-effective as possible.

Foolish Assumptions

We make the following assumptions about you, our reader:

- You aren't a stranger to the internet.
- You know the internet is home to a wide variety of cloud-based digital tools that people use for both work and personal needs — tools that are in use without the involvement, let alone the approval, of security and IT teams.
- You're aware that the cloud can be a dangerous place where the credentials and data of both individuals and companies have been attacked, mostly because of poor customer configurations.

- You're interested in fixing that challenge for your company, employees, shareholders, customers, and business partners.
- You acknowledge the need to balance security with user experience, understanding that the traditional separation of networking and security roles is no longer viable.

Icons Used in This Book

We use icons in the margins to call attention to important information. Here's what you can expect:

TIP

Anything marked with the Tip icon is a shortcut to make a specific task easier.

REMEMBER

The Remember icon flags facts that are especially important to know.

TECHNICAL STUFF

When we offer up highly technical info that you can safely skip, we use the Technical Stuff icon.

WARNING

Heed anything marked with the Warning icon to save yourself some headaches.

Beyond This Book

Although this book is chock-full of information, if you find yourself at the end of it thinking, "Where can I learn more?," just head to `www.netskope.com`.

IN THIS CHAPTER

- Recognizing how the nature of security has changed in the cloud era
- Identifying how pre-cloud security practices create new problems
- Getting to know SASE and how it enables the cloud for business
- Creating lasting business value with a SASE architecture that works
- Separating SASE value from marketing noise

Chapter 1
Understanding the SASE Vision for Securing Cloud-First Enterprises

The term *cloud* is tossed around so frequently that it can be hard to figure out just what it means. Generally, cloud refers to:

- **Public cloud:** A broad term that refers to multiple delivery styles, including:
  - **Infrastructure as a service (IaaS):** Consists of virtualized components like compute, storage, and networking. Instantiated to create an environment for hosting applications.
  - **Platform as a service (PaaS):** Abstracted services that eliminate managing IaaS components. They're created and manipulated by software application programming interface (API) calls.

  - **Software as a service (SaaS):** Applications hosted by a third-party vendor and accessed over the internet.
- **Virtual private cloud:** Private applications that run from the public cloud but are accessible only by the organization.
- **Private cloud:** This is not simply applications in a data center but an internal environment that offers self-service, on-demand components and services similar to public IaaS and PaaS.

That casual application of the word *cloud* can make it difficult to evaluate options and their relationship to your specific needs. Start by understanding what you need security to do. Because you need these capabilities across every cloud interaction, that understanding will help clarify the issues.

In this chapter, you discover how the cloud has changed security, why pre-cloud security no longer works in the cloud era, why traditional network approaches like hairpinning don't work, how secure access service edge (SASE) can enable your workers to work securely and productively in the cloud, and the defining factors of best-in-class SASE.

NICHE NO MORE

In 2024, hybrid, digitally transformed environments, SaaS applications, and distributed data architectures are the norm. Therefore, addressing cloud-centric vulnerabilities is the priority. According to Netskope Threat Labs research:

- The number of cloud apps the enterprise accesses has continued to increase between 15 percent and 20 percent every year, with the number of different apps employed by the typical user jumping from 14 to 20 in just two years.
- Half of all enterprise users now interact with between 11 and 33 cloud apps each month, with the top 1 percent using more than 96 apps per month. Interactions with these cloud apps are increasing at an even faster rate, from just over 1,000 activities per month two years ago to nearly 2,000 activities per month today.

- Most enterprise users generate between 600 and 5,000 activities per month, while the top 1 percent of users generate more than 50,000 activities per month.
- To also underscore the prevalence of generative artificial intelligence (GenAI) as a newer ingredient into this security mix, more than 10 percent of enterprise employees access at least one GenAI application every month, compared to just 2 percent a year ago.

Eyeing How the Cloud Changed Security and Networking

Once upon a time, corporate data centers were the mighty fortresses of the business world. Companies erected these digital citadels and then built and deployed business applications within their walls. Inside the fortress, companies established private networks that connected people to data, including staff at headquarters, employees in far-flung branch offices, and road warriors traveling the globe.

Like all great castles, there was an obvious perimeter: a wall with a guarded gate. Access to and from the wilds of the internet beyond the gate was strictly regulated. Gatekeepers could keep a vigilant eye over traffic along their few protected network roads, letting in the righteous, keeping out anything suspicious, and leaping into action at the first sign of trouble. Every exchange with that outside world was forced to travel back and forth along the narrow confines of the private network's internet connection.

Things changed when new, powerful applications became available in the cloud. First, a trickle, then a torrent of business users gravitated to apps based in the cloud. Cloud-based apps — for social media and communication, collaboration, and crunching the details of sales, finance, marketing, and customer relationships — were simply better than anything offered in-house.

Then enterprises and even slow-to-evolve government agencies got on board. Today's organizations favor SaaS applications and have adopted sweeping cloud-first policies that mandate solving business challenges with cloud solutions and moving critical enterprise systems to the cloud. SaaS products provide fantastic capabilities to companies faster and better than previous approaches that required long development times and the acquisition of hardware and software.

As the last decade ended, spending on cloud activities increased significantly to far outstrip the pace of all other parts of IT budgets. But the transition to cloud hasn't been easy or seamless. Many of these cloud-based tools remain outside the visibility and control of IT departments. From a security perspective, that's troubling. But security isn't just about protecting cloud apps.

Security is also about providing all the protection needed when your entire workforce has gone remote. Wherever they are, your users need to be protected from attacks and provided guardrails to keep data and applications safe. And from a networking point of view, the experience needs to be not only safe, but also functional. Security can't be a bottleneck to the undeniable productivity users realize when they can use the cloud to get more stuff done faster, from wherever they are.

Then there's information. Data (everything from intellectual property and sales figures to customer credit card numbers) is valuable treasure possessed by your business — perhaps more valuable than the products you sell. Because of that value, the fact that IT security is the stuff of front-page headlines is not surprising; when it is, the news is rarely good. The world has seen a rising wave of attacks from a variety of criminals using sophisticated techniques to wreak havoc and exploit vulnerabilities in cloud applications and how they're accessed.

Old security techniques developed for primarily on-premises data centers have struggled to keep up. The old roads running through the data center network are littered with obstacles, annoyances, and inefficiencies that slow productivity, frustrate users, and compromise security. Applications based in the data center pale in comparison to SaaS apps in terms of productivity, user experience, and convenience. The much-needed improvements brought by SaaS have empowered salespeople to sell more, marketers to amplify their messages, HR departments to find the best job candidates, and product developers to work faster. Giving up SaaS would mean letting go of unprecedented productivity. No business wants that.

The catch was that these SaaS applications required data from inside the walls to be useful, and yet the applications were outside the walls. Corporate IT security, assuming it had very little control over things "out there" in the cloud, had two choices: Say no or pretend not to notice. This is what's now described as *shadow IT,* where users and even whole departments circumvent IT and security to use SaaS tools, including large file-sharing tools that are convenient but not approved for business use. Shadow IT has existed for many years, but its use (and danger) accelerated thanks to cloud adoption. Security professionals, with their toolkits built for enterprise data centers and the old style of how to keep track of and control applications, find themselves in a real bind.

REMEMBER

Old security always forces compromises: Choices that raise some standards, such as speed or flexibility, come at the cost of others, namely security. SASE, done right, is enabling. It enables the people closest to the problem to innovate and solve problems with technology in a secure and governed way — all while helping IT leaders better understand their business.

Noting the Problems of Pre-Cloud-Era Security

Pre-cloud-era security tools, techniques, and technologies are still in use everywhere, likely within your own company's IT infrastructure. This creates a situation in which a lot of security "stuff" is out there, but the result is anything but secure or efficient. The lingering problems usually fall into one of two categories: the wrong approach or no strategic approach at all.

The wrong approach

One of the perceived benefits of an enterprise data center and the efficacy of its security was that it kept a company's digital assets in a single, safe location. A company could then build its own private network to connect workers at headquarters, as well as those at branch offices, and control their access to the bits that they needed within the data center.

REMEMBER

Although data centers still exist, forward-thinking companies are increasingly cloud-only and are shutting down their data centers. Regardless, a data center is just one of many places users and data go. It's no longer at the center of anything, either for business needs or as a single security control point.

Security systems for data centers are usually appliances — physical boxes plugged into the data center network to serve specific, narrow functions. Over the years, enterprises may have purchased security systems from hundreds of vendors. According to the Panaseer 2022 Security Leaders Peer Report (`https://panaseer.com/reports-papers/report/2022-security-leaders-peer-report`), security teams from big enterprises now have an average of 76 security tools. In the majority of cases, those products were not designed to work together. It's all but impossible for security staff to integrate all these systems into an orchestrated, adaptive security platform that can enforce policies that support cloud applications and remote workers.

WARNING

Having diverse systems often results in console chaos (and perhaps arguments over who gets to sit at which consoles). Your security and network personnel may face dozens of different management windows, each with its own priorities and all competing for attention. Making sense of the big picture or a single situation may be impossible when you're in the crunch of diagnosing an issue.

REMEMBER

The role of security isn't just to shout "no." You want to say "yes" to things that enable your business to work more quickly and effectively, especially with a distributed workforce. Security must prioritize protecting users and data, but it also must adapt in real time to keep pace with fast-changing requirements. That means providing users with a smooth, productive work experience wherever they happen to be by letting them access the data they need using whatever tools enable them to be the most productive and successful.

No approach at all

Your users are everywhere, and today's network needs to be designed with that in mind. Instead of a proactive strategy, "no approach at all" is a conscious decision to do nothing, allowing cloud complexities to overwhelm the IT department until it collapses. Such neglect results in users constantly slowing down and changing course due to *hairpinning* (forcing all user traffic through the data center's outdated "security stack" and back out to the internet, stifling productivity). This approach makes business systems less usable, reduces performance dramatically, and frustrates users.

The range of controls you have for people and services within your network isn't available for your SaaS applications. Your strategy must be to secure a far broader landscape, in real time, and do it all using just three control points:

- The data, which you own, that flows in and out of the SaaS applications
- The identity of each user who's accessing those apps
- Approval based on whether your business conducts business with the provider

REMEMBER

The key to successful cloud security lies in readjusting your focus. Past security systems were largely based on controlling access — a castle-and-moat approach. For cloud security to succeed, you should focus not on access but on activity: who's doing what, how applications are being used, what data is going where.

TECHNICAL STUFF

Older security systems typically know where on the internet a user is headed. But the SaaS application they're using may itself rely on tens, hundreds, or even thousands of additional resources to populate the web page your user sees. To secure the cloud, you need to know those details. Your legacy tools don't do things like decrypting Transport Layer Security (TLS), which would let them see what's happening inside the traffic of the user's communication with that application. Those tools also can't spot certain API connections that the SaaS application uses to exchange information with other, unknown resources to build a rich environment for the user. Without that type of detail, you can never be certain that your data is safe or that what your user is seeing has been legitimately sourced.

Defining and Adopting SASE

SASE moves network security perimeter controls to the cloud, while at the same time making those controls faster, more application- and user-aware, and data-centric.

SASE is also a new architecture strategy for security and networking that your organization, like others, will find valuable. It addresses the fact that a cloud-centric world needs an updated model for security and networking — and outlines fundamental ways in which security, networks, applications, and data protection have all transformed.

Functionally, SASE combines suites of integrated security and networking services. These are not only designed to grant users cloud access but also to monitor the activities, devices, and applications they use continuously. This ensures data security at all times and at every access point, without compromising user experience. The good news is that the foundation of your SASE security architecture can be deployed today, in deliberate, incremental steps (see Chapter 5). The following sections discuss what SASE is and how your organization can implement it.

Making sense of SASE Math 101

Welcome to the world of SASE Math, where we combine essential tech elements like snapping together colorful building blocks. When clicked together in the right combination, they create a robust, secure, and efficient architecture. Our foundation is built on the following:

- **Secure web gateways (SWGs):** When you try to visit a website, SWGs stand in between you and the web. They check out the site first, scan the content to ensure it's safe, and then welcome you into the water. Like a good friend who is also an expert surfer, they test out the waves to make sure the water's not too rough, so you can surf in peace.
- **Cloud access security brokers (CASBs):** The digital world's hall monitors for cloud apps stand guard, making sure only the right people can access the right cloud applications and data. They scrutinize who's trying to get in, what they're bringing with them, and what they're doing, ensuring everything and everyone is safe and sound. It's like a personal security detail for cloud adventures, ensuring you're always in the right place with the right access.
- **Zero trust network access (ZTNA):** Picture ZTNA as the bouncer for your company's private apps. Unlike the old days of using a bulky, one-key-fits-all virtual private network (VPN), ZTNA uses a smart key approach. Before anyone can

get in, the ZTNA cloud bouncer checks their ID and makes sure they're dressed right (their security posture). Only then does it let them into exactly where they need to go — no wandering around the entire place. This smart bouncer is great for remote work. It doesn't matter where you are or what device you're using; you get a smooth, direct line to your work apps, just as if you were in the office. And because it lets you into only the apps you need, there's no chance of your sneaking around where you shouldn't be. It's like having invisible walls that keep the bad guys out and the good guys on the right path, making your digital space safer than ever.

- **Data loss prevention (DLP):** These tools detect and prevent potential data breaches or data exfiltration, safeguarding sensitive information like a meticulous librarian who makes sure no book (your data) gets lost, destroyed, misplaced, or into the wrong hands.

Now, start snapping these blocks together:

- **SWG + CASB = Next-gen SWG:** Combine the gatekeeper and the bouncer, and you get an even mightier, all-seeing gatekeeper who's also got an eye on the cloud.
- **Next-gen SWG + ZTNA = Security service edge (SSE):** Add the super-skeptical bodyguard to the mix, and — voilà! — you've got a powerhouse protecting all of your data pathways.
- **SSE + Software-defined wide area network (SD-WAN) = SASE:** If you snap an SD-WAN onto your SSE, you've got yourself a digital traffic cop who's not just smart but also buffed up with some security muscles. SASE is an omniscient, omnipresent tool that's not just secure but also super-smart in handling your data traffic.

But wait, there's more! SD-WAN is like the ultimate road-trip planner for your data. It knows all the shortcuts and can reroute you in real time to avoid congestion, making sure your digital journey is smooth and swift. Plus, it's got a few security tricks up its sleeve to keep the bad guys at bay. It shines in three major areas:

- **Optimization:** Think of it as always having a green light. It ensures that your data traffic flows fast and without sputtering, which is especially important for branch offices.

- **Resilience:** Even if one internet lane is closed (think of it as a roadblock), SD-WAN finds another route instantly, keeping your connection up without a hitch.
- **Security:** Although SD-WAN isn't a full-blown bodyguard, it does a decent job of keeping the riffraff out with basic security checks.

For finishing touches on our architectural masterpiece, add

- **Firewall as a service (FWaaS):** A barrier between a trusted network and untrusted networks, monitoring and controlling incoming and outgoing network traffic.
- **Threat protection:** Technologies and practices that protect against cyber threats like malware, ransomware, and phishing attacks. Threat protection looks at all content going in or out of your organization and ensures that it's not disguising an attack.
- **Remote browser isolation (RBI):** Like a chaperone for web browsing, RBI visits websites for you. Instead of grabbing files that may be risky, it sends back a safe rendering of the site. It's like browsing inside a protective bubble — seeing everything but touching nothing harmful.

There you have it — SASE Math, where combining the right tech elements equals a secure, streamlined, and savvy digital ecosystem. It's like playing with your favorite blocks, but these blocks protect your entire digital world!

One of the defining characteristics of SASE is that every aspect of this security architecture is purpose-built for use in and with the cloud. It doesn't repurpose devices or code intended for data centers. You already know the reason why: Security services for the data centers primarily seek to control access. They don't speak the native language of the cloud, which is rich with nuance and information describing connections between points and the data contained in the flow of traffic between points. Keep this in mind as you evaluate security and networking options.

Understanding the role of context in SASE

We talk about context throughout this book. For now, just recognize that context is the lifeblood of SASE. It offers an informative guide to just how deep and rich this new security architecture intends to be. Here is a sampling of the contextual factors that are intrinsic to SASE and that reveal the sophistication of its workings:

- The identity of the user
- The identity and posture of the user's device
- The location from which access is being attempted, plus the day and time
- The type of and identity of the applications being accessed
- The data being requested — what it is and where it's stored
- The user's behavior patterns
- The application interaction — what the user is specifically trying to do

Then, while continuously reevaluating that dynamic stream of information, SASE applies security based on policies that determine the following:

- The service level and type of network services to apply
- The use of appropriate types of traffic encryption
- The level of data protection to apply to prevent misuse
- The level of authentication to apply
- Whether the application requires the use of specific, specialized security services such as a CASB to further intermediate in the activity

Yes, a lot's going on in a SASE architecture. But when it's truly functional and properly implemented, SASE dramatically simplifies and improves the quality of your security and your network connectivity. When SASE is done right, all these things happen in real time, including continuous risk management.

REMEMBER

By moving security services out of your data center and into the cloud, closer to both your points of vulnerability and your users, you gain greater visibility and firmer control over what's going on, with whom, at all times. SASE helps network and security teams transition to enable new applications and a new way of doing business while at the same time protecting access to older, on-premises applications.

Comparing dual-vendor and single-vendor SASE

You may encounter a dual vendor versus single vendor debate as you explore SASE implementation in the wild. It sounds technical, but let's break it down.

Imagine you're hosting a huge party (your company's network) and need both a DJ (security features) and a caterer (networking capabilities). Do you hire two separate specialists or do you go with one company that promises to handle both? That's the crux of the dual vendor versus single vendor debate in SASE.

Dual vendor: The specialist duo

As SASE evolved, it became clear that this massive party may need specialists. Initially, SASE was this big blob of security and networking functions with little distinction. Real-world use showed that the DJ and caterer had to be different entities in some cases to offer the best experience. So, Gartner updated its advice: Hiring separately is cool, but make sure they can play nice together, aiming for no more than two vendors to avoid a logistical nightmare.

Single vendor: The one-stop shop

Some experts, like those from Gartner, initially viewed the single-vendor approach as a jack-of-all-trades but master of none. However, companies like Netskope beg to differ, showing that it's possible to have your cake and music, too — offering advanced SASE products that don't skimp on quality or functionality. When we talk about single-vendor SASE in this book, we're talking about a powerhouse that can handle everything SASE requires without compromise. It's like finding a caterer who is also a world-class DJ.

A popular narrative suggests that a single-vendor approach — where both security (SSE) and networking (SD-WAN) come from the same provider — is only viable for simpler, smaller-scale operations. Critics argue that such products may not meet the complex demands of larger, global enterprises. However, at Netskope, we challenge this notion head-on.

Our comprehensive SASE offerings, including both Netskope Intelligent Security Service Edge (SSE) and Borderless SD-WAN, are designed to scale and adapt to the needs of even the largest global enterprises. Whether these components are deployed together or separately, they stand ready to tackle the sophisticated requirements of any organization, without compromise. This commitment underscores our belief that a single-vendor platform can indeed offer the depth, breadth, and scalability necessary for modern enterprises, debunking the myth that such approaches are only suited for the mid-market.

The bottom line

The choice between single- and dual-vendor approaches to SASE is about more than just technical capabilities. It's about ensuring seamless collaboration toward the ultimate goal: a secure, efficient, and user-friendly network environment. Whether you choose a single vendor that can do it all or two specialists that work in harmony, the key is integration and cooperation.

REMEMBER

When choosing vendors, remember that they need to be in sync, just like the DJ and caterer at your party who need to work together to ensure that everyone has a good time, no one's stepping on toes, and your party is the talk of the town (or industry).

Examining the Business Benefits of SASE

What does your business stand to gain from embracing SASE? Why go through all this effort? SASE offers three primary business benefits: reducing cost and complexity, mitigating security risk, and enhancing agility. Together, this triad helps you effectively navigate the complexities of modern cybersecurity, streamline processes, bolster security, and foster a more agile business environment.

Reducing cost and complexity

Imagine trying to run a relay race while juggling 76 tennis balls. Sounds impossible, right? That's a bit of what managing a company's cybersecurity has been like. Back in 2021, the average company was spinning 76 different security tools just to keep the digital bad guys at bay. Each tool needed its own special care and feeding — different interfaces, licenses, and endless updates. Plus, they didn't talk amongst themselves much, if at all. It was a lot.

Now, enter the world of SASE, your all-in-one tool combining critical cybersecurity and networking capabilities. SASE pulls together all those scattered security and connectivity needs into one streamlined, easier-to-manage package. Your relay team, spanning parties from infrastructure and infosec, can focus their collective efforts much more effectively.

Why does this matter? For starters, it's a huge relief for the IT folks. No more hopping among dozens of platforms to tweak settings or update passwords. SASE means fewer tools but more power, simplifying those daily tasks that used to eat up hours. And for the company, it means spending less cash on a mishmash of licenses and getting more bang for their cybersecurity buck.

Adopting SASE simplifies security and cost management, replacing a complex, expensive setup with a streamlined solution that efficiently protects the company. It's designed to meet the needs of modern businesses in a complex digital environment.

Mitigating security risk

In the digital world, keeping safe is like being in a never-ending game of tag. You're always trying to stay one step ahead of the "it" player, who, in this case, is a cyberattacker. This game gets tricky because the rules keep changing, and the "it" player keeps getting smarter. (And there's more than one "it.") SASE is like getting to choose all the best players for your game of digital tag, ensuring you stay safe while running around the internet.

SASE is all about being prepared. It's like a team where each member has a unique gadget designed for different kinds of trouble. But instead of your having to run around trying to figure out which gadget to use, SASE integrates all these tools, ensuring they function together as a well-oiled machine. This means you're always ready, no matter what new trick the "it" player comes up with.

Now, imagine a world where, upon entering a building, everyone's ID is checked — not just once at the front door but every time they want to go anywhere else within the building. That's what SASE does through zero trust. It's like having a strict bouncer at every door, ensuring only the right people can get in. It's much harder for the "bad guys" to sneak into places they shouldn't be.

So, why does all this matter to you? With SASE, you can keep playing the game — browsing the internet, working online, sharing with coworkers — without worrying about getting tagged. It's like having an invisible shield around you so you can focus on what you love doing, knowing you're being protected by the best team out there.

Enhancing agility

In business, agility is like competing in an obstacle course race. Here, the goal is to swiftly navigate challenges, jump over hurdles, and reach the finish line faster than the competition. Agility is the heartbeat of digital transformation, allowing businesses to harness technology to stay ahead, empower their workforce, and provide them with the tools and data they need to excel.

However, this race has a unique twist: Although speed is essential, safety cannot be compromised. Imagine having to wear protective gear that shields you without slowing you down. This is where cybersecurity steps in. It's crucial, yet it must not add unnecessary weight or *friction* that could slow your pace. *Friction* refers to any security measure that becomes more of a hindrance than a help, making accessing the tools and information that drive productivity more challenging.

SASE is the game changer in this scenario. Think of SASE as the ultimate gear for our obstacle course: It's lightweight, it doesn't slow you down, and it offers protection so seamlessly integrated that you barely notice it's there. It's about implementing security that effectively protects without disrupting the flow of work, ensuring that employees can navigate digital spaces swiftly and safely.

In essence, embracing agility in today's digital age means leveraging IT to its fullest, enabling your team to perform at their best with minimal security-induced delays. SASE represents a strategy that balances robust security with the need for speed. It ensures that businesses can race through their digital transformation journey without unnecessary barriers. With SASE, companies are equipped to tackle the obstacle course of the digital world, ensuring both security and agility as they aim for success.

Busting SASE Myths

This probably isn't the first *For Dummies* book you've read on SASE, and it probably won't be the last, though it's our job to make it the best! Joking aside, as with any emerging technology or trend, SASE is ripe for misinformation. Just as slapping an *i* before a product name doesn't automatically confer design elegance and adding an *e* doesn't translate into power and efficiency, the SASE moniker is already being co-opted, over-marketed, and misinterpreted. In the following sections, we dispel several common myths.

Myth: SASE can be supported by legacy technology

Today's network security infrastructure is the product of years (in some cases, decades) of development and deployment efforts. But no amount of patching, tweaking, and upselling magically turns legacy appliances into cloud-native security products. The cloud demands a fresh approach.

Myth: SASE can be achieved through a patchwork of multi-vendor products

Relying on a patchwork of products from multiple vendors to assemble a customized SASE fails to capture its essence. The power of SASE lies not just in having a set of tools (like a SWG, a CASB, and a ZTNA) but in their cohesive integration and unified management. Guidance from leading industry analysts to favor minimal vendor diversity underscores a critical insight: SASE is about simplicity and consolidation, not merely collecting independently managed products and branding them as a unified system.

Myth: SASE lets you keep your network architecture

SASE can be effective only when its policies and enforcement are out at the edge, close to where your users, devices, and applications meet. This proximity is what gives SASE its dynamic security characteristics and provides the performance and reliability users require to be their most productive (and least frustrated!).

Myth: SASE doesn't need to see all your network traffic

SASE is effective precisely because it's an all-in approach to security. Its power, simplicity, and impact derive from its ability to develop context about users, data, and applications, including underlying APIs. SASE offers the visibility that security and networking teams crave. That rich context is what makes SASE so effective in a landscape that offers far fewer control points than the old data center ever had.

Myth: SASE adds to complexity

Complexity is the bane of your and every security or networking person's existence, and it's the common denominator among the majority of headline-grabbing failures of security. SASE replaces disparate tools with a single, integrated platform of security capabilities that operate under a unified policy framework and shared reporting/analytics functions. Network security cobbled together piecemeal can never deliver on the SASE vision of a single, integrated cloud security architecture in which policy and enforcement are perfectly orchestrated and adaptable to rapidly changing requirements.

Myth: SASE requires a "rip and replace" approach

It's all but impossible for companies to fully unburden themselves of their past — old products, biases, beliefs, and investments. Contrary to the myth that transitioning to SASE requires a complete overhaul of existing infrastructures, SASE allows for a gradual evolution, accommodating and potentially replacing legacy technologies over time without demanding an immediate wholesale replacement, ensuring a smoother transition to a more consolidated, efficient, and secure network architecture.

IN THIS CHAPTER

- **Understanding how SASE makes modern cloud security possible**
- **Identifying how SASE creates security fit for the cloud**
- **Defining the key principles that describe SSE and SD-WAN**
- **Architecting for SASE**

Chapter 2
Bringing SASE to Life with SSE and SD-WAN

Imagine embarking on a grand digital adventure with the cloud as your destination and your digital identity as your passport. In this scenario, secure access service edge (SASE) is like the ideal security agency of every traveler's dreams, one that ensures that your journey through the vast online realms is safe *and* efficient. SASE goes beyond traditional security checks, representing a fusion of networking and security, like some perfect airport where security and flight operations are integrated to deliver a smooth, more secure travel experience (we travelers can dream!).

Just as our fantasy security agency would work to ensure passengers and their belongings are safe without slowing operations, SASE integrates software-defined wide area network (SD-WAN) and security service edge (SSE) to create a dynamic, secure networking infrastructure. This integration allows fluid data movement across networks, like passengers being simultaneously securely checked and efficiently routed to their flights without unnecessary delays.

Within the SASE framework, SD-WAN determines the most efficient pathways for data to travel. This would be like our idealized airport making the effort to direct passengers to the fastest security lines or the most direct routes to their gates. At the same time, SSE scrutinizes every bit of data (or every passenger) for potential threats, ensuring that only safe, authorized access is granted — similar to how airport security ensures that only cleared passengers board their flights.

By weaving SD-WAN and SSE together, SASE creates an experience where security and network performance enhance each other instead of existing as separate checkpoints. Security measures are applied precisely where and when needed without slowing down the network's performance, ensuring that data travels through the most optimal routes while being safeguarded against threats.

This chapter dives into a set of guiding principles outlining the essentials of a comprehensive SASE architecture. Our focus is on helping you identify the SASE platform that best meets your needs, ensuring that your digital journey is both secure and efficient. Through the seamless integration of SD-WAN and SSE, we navigate the complexities of the modern digital landscape where every measure is taken to ensure your passage is both swift and protected.

REMEMBER

SASE isn't just technology — it's about enabling people. It empowers individuals and teams to work from anywhere, on any device, without compromising security or performance. It breaks down old barriers that hold back innovation and productivity.

Enabling True Cloud Security

SASE, done well, has two key jobs:

- **To deliver security services throughout the global edge network so that these services are close to users:** This ensures that users and organizations can always rely on this security network to get work done safely. This configuration makes it feasible to apply security policies and control users' online interactions based on context, such as who the person is and where they are, and to do so while optimizing the security, reliability, and performance of those activities. Implemented through SSE, this capability is like ensuring a secure and efficient journey from the parking lot through the airport security checkpoint.

- **To provide a global edge network that grants users access to cloud services, no matter where those users are:** This global edge network authenticates users and then optimizes their connections to software as a service (SaaS) applications, your data center, and other services, ensuring a seamless continuation of their journey to their final destination, much like guiding passengers from the airport security checkpoint to their departure gate. This job, which ensures a smooth transition and optimized path through our digital airport, is implemented through both the SASE cloud architecture and SD-WAN.

REMEMBER

Properly implemented, SASE is effective because it acknowledges that applications and workloads have moved to the cloud, and therefore, security services must follow.

For your users, SASE done right means they don't have to worry about jumping through hoops to use an application. When they go to a coffee shop, getting access to what they need is as easy as ordering a latte. For you, the security pro, having context and shared, integrated security services makes it possible to create sophisticated policies that can be applied automatically and appropriately based on who needs access, what they're trying to access, and where all the pieces of the interaction are located. In a digital world that has left the restrictive confines of the data center for the wide-open possibilities of the cloud, SASE is the only security and networking architecture that makes sense.

WHAT ABOUT THE DATA CENTER?

The data center still has a role to play in enterprise IT for the foreseeable future. Large applications like enterprise resource planning (ERP) were built to last for decades, so such applications in the data center will likely coexist with public clouds of all styles — infrastructure as a service (IaaS), platform as a service (PaaS), and SaaS — for a long time. More broadly, organizations have invested a lot over many years to create and nurture their enterprise data centers. Letting go of that momentum may be hard. Be patient.

When you accept the data center as just one of many places your users go to do their jobs, routing all your cloud-bound traffic through

(continued)

it starts to make less sense. Forcing a remote user's traffic to constantly detour back through your organization's private network to then be crunched through a succession of separate security black boxes — a process known to security people as *hairpinning* or *backhauling* — is cumbersome and inefficient. After all, you wouldn't plan to drive from Los Angeles to San Francisco by way of Cairo unless you had a lot of spare time (and a ship). The same logic applies to linking your users to their SaaS applications.

Note: SASE isn't just about SaaS applications. It can and should be used to provide access to and protect all your applications, including the ones in the data center, regardless of whether a user is on- or off-premises. We talk more about this subject in Chapters 3 and 4.

Examining the SSE Side of SASE

SSE is where all your security measures start to work together intelligently. Implementing SSE is like setting up the brain of your security operations, ensuring that every action is coordinated and every security service is in sync.

SSE consists of smaller, manageable, specialized, yet integrated services. Like the smart, interconnected devices in a modern home, each service has a specific role to play, but by working together, they create an efficient and even more capable environment. The various components of SSE make your security system flexible, scalable, and capable of adapting to new challenges.

Furthermore, SSE is both the central point where security policies are defined and the distributed points where those policies are enforced consistently and intelligently regardless of where your data or users are. This design — centralized decision and distributed enforcement — is crucial in managing complex security tasks, ensuring that every part of your network is protected without manual intervention.

One of the transformative aspects of SSE is its ability to consolidate and enhance your security posture. Moving away from isolated security appliances and toward integrated services within SSE makes your security infrastructure less complex and more effective. This transition simplifies management and improves your ability to respond to threats with the combined intelligence of integrated services. Here are the core principles to remember.

Context and zero trust

The concept of trust within network and security architectures has undergone a significant transformation. The traditional model, which operated on an implicit trust basis — assuming that everything inside the network is safe — is inadequate for today's dynamic and boundary-less digital environments.

REMEMBER

Zero trust is a security model that insists on explicit verification for every access request, regardless of where the request originates. This model operates on the principle of least privileged access, ensuring users can only reach the resources necessary for their roles — nothing more, nothing less.

By integrating zero trust into SASE, organizations can navigate the complexities of modern cybersecurity, transitioning from a state of implicit trust to continuous, adaptive evaluation based on identity and context.

Context is the foundation of zero trust

The ability to measure signals and gather context is at the heart of the zero trust model. This goes beyond just recognizing a user's identity. It encompasses a comprehensive understanding of the user's device, their location, the applications they're accessing, and the nature or sensitivity of the data involved. By weaving together these strands of rich metadata, a detailed picture emerges — one that allows for real-time, informed decision-making about access permissions tailored to the specific circumstances of each request.

Visibility is the key to contextual awareness

To implement zero trust effectively, visibility across all network traffic is paramount. Traditional security systems primarily monitor web traffic, and a few can identify types of web applications; both are blind to the many other channels through which modern business operates, such as SaaS applications (personal and corporate), corporate applications running from IaaS/PaaS cloud services, and even on-premises custom applications. This comprehensive visibility is crucial; it's the foundation upon which context is built, enabling security systems to see and understand every interaction in the digital landscape.

The dynamics of context and policy enforcement

Because digital interactions are constantly evolving, context is inherently dynamic. A security system that can adapt to these changes in real time, adjusting policies and protections as needed, is essential. For instance, if a user's behavior suddenly deviates from the norm, this could trigger additional authentication steps or other security measures. This agility ensures that security responses are always tailored to the current risk level, providing robust protection without hindering legitimate business activities.

WARNING

Legacy security systems typically operate on a binary yes/no decision framework. They lack the flexibility to adapt to the fluid nature of digital interactions.

The modern approach is characterized by its dynamic, ongoing assessment of each access request, with security measures that evolve in response to the shifting digital landscape to provide just the right access at just the right time.

Adopting zero trust within a SASE framework marks a significant leap forward in cybersecurity strategy. By grounding security decisions in context, organizations can ensure that a responsive, adaptive security posture protects their digital assets. This is about more than just keeping up with the times. It's about setting a new standard for digital security equipped to handle the complexities of the modern world.

Best-in-class enterprise security

Achieving unparalleled enterprise security means equipping your network with the most effective tools and strategies to safeguard against cyber threats. This principle centers on adopting a comprehensive approach to security and fortifying every layer of your network with top-tier protection mechanisms.

Just as airports use a variety of security measures — from passenger screenings to secure access controls for staff — enterprises require a multifaceted security strategy. This strategy should be holistic, encompassing everything from endpoint protection to secure web gateways (SWGs), cloud access security brokers (CASBs), and zero trust network access (ZTNA). Implementing advanced threat protection (ATP) techniques, firewall as a service (FWaaS), and remote browser isolation (RBI) is crucial. (We touch on these subjects in Chapter 1; also see Table 2-2 later in this chapter.) Each component is vital in a robust system that covers all potential vulnerabilities.

Integration is essential

For security measures to be effective, they must work in concert. Integration is key, allowing various tools and platforms to operate as a unified system. This cohesion enables real-time threat detection and response, significantly reducing the risk of breaches and ensuring rapid recovery from security incidents.

With single-pass inspection, a user's traffic is analyzed in one seamless operation when connected to a global edge network. This method channels all traffic through the inspection engine for real-time scrutiny, in contrast to older systems that segment inspections through multiple, disjointed checkpoints.

This approach encompasses websites, approved and unapproved SaaS applications, and IaaS/PaaS cloud services, creating a unified security posture. It simplifies the process by first eliminating explicit threats, and then progressively scrutinizing the remaining data with finer detail, optimizing the enforcement of security policies across all network interactions.

Integrating SWG, CASB, and ZTNA into a cohesive security strategy also ensures that data is protected regardless of where it resides or travels. By leveraging threat intelligence, enterprises can anticipate and neutralize potential threats before they impact the network. FWaaS and RBI serve as essential layers of defense, controlling access to network resources and isolating browsing activities to prevent malware entry.

Selecting security products that can seamlessly integrate is crucial. The goal is to create a security ecosystem that supports swift, automated responses to threats, leveraging the strengths of each component — whether it's endpoint detection and response (EDR), intrusion prevention system (IPS), or ATP products. This integrated approach streamlines security operations and enhances the effectiveness of each security measure.

The role of advanced threat protection

ATP is a critical component of a well-implemented SASE framework, offering broader and more effective security measures. Traditional threat protection tools shielded users from common threats like malicious files. However, as attacks become more sophisticated, advanced forms of threat protection become necessary. In addition to malicious files, these threats encompass risky applications, systems, and attack vectors such as:

- **Endpoints:** Devices like laptops, tablets, phones, and Internet of Things (IoT) sensors that connect to your network from the outside world.
- **Cloud-dwelling services:** This includes SaaS applications you subscribe to, IaaS/PaaS applications you own, and websites your people visit — which can range from secure to compromised by malicious actors.
- **Users:** Verifying the identity and legitimacy of individuals accessing your systems in your company's name.

To effectively counter these threats, ATP in the cloud must be proactive, preventing threats before they start and quickly detecting any that do emerge. Netskope enhances this process by incorporating artificial intelligence (AI) and machine learning (ML) to significantly improve threat recognition.

As part of an overall SASE platform called Netskope One, Netskope's Intelligent SSE leads the way in addressing these complex challenges using what's known as the Cloud Threat Exchange. The Cloud Threat Exchange provides continuous, real-time threat intelligence to your SASE, sourced from a wide range of contributors, including identity providers (IdPs), endpoint protection platforms (EPPs), and security information and event management (SIEM) services. This collaborative approach ensures that your security measures are as comprehensive and up-to-date as possible, leveraging the collective expertise of all integrated services.

REMEMBER

Demanding best-in-class enterprise security is about more than just adopting the latest tools. It's about ensuring these tools fit your unique needs and working together seamlessly to protect your digital assets. By following this principle, enterprises can achieve a level of security that defends against today's threats and is prepared for tomorrow's challenges (see Table 2-1).

TABLE 2-1 Key Security Services Delivered by SSE

Security Service	What the Service Did in a Traditional Setup	How Netskope Intelligent SSE Supercharges the Service
SWG	Protected users against web threats and objectionable content.	Adds app and data context (who's using the app or data, where they're using it, and why). Stops inappropriate use of data (preventing data from being used or sent where it's not intended).
Data loss prevention (DLP)	Protected only the data stored in the data center and being moved beyond the data center's firewall via the web.	Protects all data in motion, including data distributed on the web, in SaaS apps, and in custom apps running from IaaS/PaaS clouds.
CASB	Monitored and controlled the usage of all SaaS apps via inline inspection (as proxy). Reported on the usage of approved SaaS apps via application programming interfaces (APIs) they published for that purpose. Its focus was on data at rest in approved SaaS apps and data in motion from and to all SaaS apps. Not all products support both modes.	Differentiates between corporate and personal instances of approved SaaS apps. Provides controls over specific activities within all SaaS apps by decoding JavaScript Object Notation (JSON). Incorporates several context signals into access policies, thus allowing customers to apply zero trust principles to SaaS app usage. Offers high-fidelity data protection with hundreds of prebuilt rules and dozens of file types. Includes strong app risk insights to inform SaaS selection and deployment.

(continued)

TABLE 2-1 ***(continued)***

Security Service	What the Service Did in a Traditional Setup	How Netskope Intelligent SSE Supercharges the Service
ATP	Protected against web-based threats using methods such as *sandboxing* (detonating executables safely to detect malicious intent and hyperlinks) and threat intelligence (shared indicators of compromise [IOCs] from public and paid sources).	Protects against cloud-enabled threats, including malware delivery and phishing attacks from Transport Layer Security (TLS)–encrypted cloud services such as Microsoft 365 and Google Docs. Blocks rogue accounts within approved cloud services. Isolates unknown apps and websites to enable safe interaction and protect against potential threats.

Advanced data protection

Securing data is more than a technical challenge; it's a strategic imperative. The concept of advanced data protection recognizes that effective security isn't just about preventing unauthorized access. It's about creating a comprehensive, easy-to-use system that safeguards data across all channels and touchpoints. This principle emphasizes the need for unified data protection that extends across email, web, private applications, clouds, and endpoints and embodies the essence of the zero trust approach — trust nothing, verify everything — with a keen focus on data.

TIP

An integrated DLP capability is at the core of advanced data protection. Traditional DLP systems often fall short because they can be cumbersome to implement and manage, hindering user productivity. A modern DLP capability should be as seamless to operationalize as it is comprehensive, covering every conceivable data interaction within the organization's digital ecosystem. This means protecting data in transit, at rest, and in use, from cloud services to on-premises networks, without complicating the user experience.

However, enterprises need more than just DLP to protect their data fully. They require layered security that includes ATP, SWGs, and context-aware policies. These elements work together to prevent data leaks and ensure that security measures adapt in real time to the context of each transaction. In many cases, the results that come from evaluating other signals can yield correct access control decisions without invoking DLP. This reduces the pressure on DLP and the risks of false positives and false negatives. Now, organizations can apply the most effective protection mechanisms based on the identified risks.

One of the key challenges in data protection is making powerful tools accessible and manageable. An effective DLP system should provide clear visibility into data movements and security incidents, enabling swift, informed responses to potential threats. This operational ease is crucial for maintaining a robust security posture without overwhelming IT teams or end users.

Zero trust principles guide the deployment of DLP and other security measures, ensuring that they're comprehensive and adaptable. By continuously verifying every access request and adjusting protections based on the sensitivity of the data and the context of the interaction, organizations can create a dynamic, resilient defense against the evolving threat landscape.

Such comprehensive data protection creates a secure, adaptable, and user-friendly environment that protects data wherever it resides or travels. By integrating advanced DLP products with a broader security strategy informed by zero trust principles, organizations can balance robust protection and operational efficiency. This approach ensures that their most valuable asset — data — remains secure against all threats.

Looking at the Networking Side of SASE

Gone are the days when most employees were tethered to corporate offices and routing traffic through a central data center was the norm. With the widespread acceptance of remote and hybrid work models, the demand for direct, efficient access to cloud services has skyrocketed.

This shift underscores the need for security measures that can adapt to this dispersed, dynamic landscape without compromising on protection or user experience. In the modern work environment, balancing swift, hassle-free access to apps and data from anywhere and ensuring top-notch security might seem like a tightrope. Users expect quick and easy connections to their digital workplaces without hitting security snags, reflecting a shift from traditional office-centric models to a more flexible, anywhere-access approach.

The concept of rerouting user traffic through a data center — known as *hairpinning* — has also become outdated. It introduces unnecessary delays and stands in the way of productivity for the modern, mobile workforce. To tackle this, the focus has shifted toward leveraging the cloud to securely follow users wherever they work, ensuring data protection is always in lockstep with their needs.

Moreover, the reliance on traditional virtual private networks (VPNs) is waning as users seek faster, more reliable connections. This change highlights the importance of a global edge network, allowing seamless cloud access from any location and eliminating the need for cumbersome detours through the data center. This approach enhances user satisfaction and maintains a robust security posture, ensuring that users and data remain protected across all fronts. The following sections address principles to the networking side.

Optimal end-to-end user experience

The expectation for seamless online experiences has never been higher. This principle delves into the heart of ensuring a seamless experience through the power of Netskope Proactive Digital Experience Management (P-DEM) and the innovation of Netskope Borderless SD-WAN.

Proactive digital experience management

What you may know as *digital experience monitoring* — a passive approach of merely observing — has been revolutionized into an active principle we now refer to as proactive digital experience management (P-DEM). Instead of simply spotting and reacting to issues, P-DEM anticipates issues and ensures that they're addressed before they impact your experience. The technology provides a comprehensive end-to-end view of the digital pathway from client to app, akin to having X-ray vision, allowing for real-time adjustments and ensuring smooth, uninterrupted access. P-DEM allows your company to close help desk tickets faster, which directly influences your company's bottom line.

The role of borderless SD-WAN

In tandem with P-DEM, Borderless SD-WAN acts like the world's most advanced navigation system for your data, intelligently charting the course it takes through the vast expanse of the internet. This technology ensures that data takes not only the fastest route but also the most reliable one, dynamically adjusting to avoid digital traffic jams and potential disruptions.

Integrating these technologies delivers several benefits:

- **Latency and efficiency:** By intelligently managing and routing data, P-DEM and Borderless SD-WAN significantly cut down on delays, making digital interactions instantaneous. This efficiency is crucial not just for the user's satisfaction but also for the productivity and agility of the modern workforce.
- **Unwavering reliability:** The digital world waits for no one. Hence, the reliability offered by these technologies ensures that the tools and resources you depend on are always at your fingertips, ready when you need them, without fear of unexpected downtime or interruptions.
- **Simplified security:** In the intricate dance of digital access and protection, simplicity plays a pivotal role. These technologies not only secure your digital journey but do so in a way that enhances, rather than complicates, user experience. They provide security that operates seamlessly in the background, enabling safe access to the digital resources essential for job performance.
- **Streamlined user experience:** Integrating P-DEM and Borderless SD-WAN requires a commitment to simplifying the digital experience. This approach eliminates the all-too-common digital hurdles, streamlining interactions to ensure effortless and secure navigating of the digital world.

Combining P-DEM with NewEdge and Borderless SD-WAN makes it possible to provide an exceptional digital experience, ensuring that every digital journey is as enjoyable as it is efficient. This principle isn't just about connecting points A and B. It's about enriching the journey and making every digital interaction a pleasure.

The strategic advantage of purpose-built private cloud

The foundation upon which a SASE provider's infrastructure is built is critical to the provider's effectiveness and efficiency. A purpose-built private cloud represents a strategic choice to optimize data flow between users and applications through a secure and efficient pathway. This approach addresses several key considerations:

- **Global network design for seamless connectivity:** A well-architected network ensures minimal latency and optimal performance by facilitating direct and secure connections from users to applications. The infrastructure must span the globe, with strategically located points of presence (PoPs) that act as conduits between users and the digital resources they access. This global footprint, an embodiment of the global edge network concept, is essential for swift, secure user access to the security cloud, which securely guides them onward to their destinations. By integrating a global edge network into the private cloud infrastructure, organizations ensure that security functions are close to the user, enhancing the efficiency of single-pass traffic inspection and improving the user experience while maintaining high-security standards.
- **Ownership and control over infrastructure:** Choosing between leveraging existing public hyperscaler infrastructures and building a dedicated, private cloud infrastructure is pivotal. Hyperscaler infrastructure offers scale, but it also introduces dependencies on third-party capacities, priorities, and contracts, potentially affecting performance and control. In contrast, owning a purpose-built private cloud allows for end-to-end control over the network. End-to-end control reduces latency through better management of traffic routing, essential for supporting single-pass inspection. It also allows for direct peering with more than 650 providers (as of July 2024), which further reduces latency by eliminating the multiple hops otherwise required for users to reach cloud services and applications..
- **Customization and compliance flexibility:** A private infrastructure uniquely enables tailoring network paths and security measures to individual customer requirements. Whether compliance-driven demands, such as avoiding data transit through specific regions, adhering to specific data residency and flow regulations, or optimizing performance, a purpose-built network offers agility that's unconstrained by the limitations or priorities of a third-party infrastructure, thereby enhancing technical and operational benefits such as data sovereignty and reduced compliance risks.

- **Innovation made possible by direct control:** Direct oversight of the network infrastructure paves the way for introducing advanced features and services, such as P-DEM and specialized packet capture capabilities. These innovations require granular control and visibility across the network, something inherently limited when relying on public cloud infrastructures. The ability to implement cutting-edge security measures tailored to specific organizational needs illustrates the unique advantages of a purpose-built private cloud infrastructure.

TIP

The decision to develop a purpose-built private cloud for SASE implementations reflects a SASE vendor's commitment to providing unparalleled security, performance, and adaptability.

This approach ensures that the infrastructure meets the immediate demands of users and applications and is poised to address future challenges and opportunities in the ever-evolving digital landscape. Integrating a global edge network within this infrastructure amplifies these benefits, making it a cornerstone for achieving the seamless connectivity, security, and efficiency that modern organizations require. Table 2-2 shows how Netskope One and the Netskope NewEdge Network meet SASE networking requirements.

TABLE 2-2 How Netskope Fulfills SASE Networking Requirements

SASE Requirement	Netskope One
PoPs, with service-level agreements (SLAs) for low latency and high availability	The Netskope NewEdge network, a high-performance security private cloud, hosts security services and provides abundant access points worldwide. With low single-digit millisecond latency for the best experience, NewEdge is backed by five nines (99.999%) availability, an inline services SLA, plus a Trust Portal for real-time service/data center status (`https://trust.netskope.com`).
Traffic inspection with forward proxy of five types of user traffic	Analyzes all lanes of user traffic, including web, approved and unapproved SaaS, IaaS/PaaS cloud services, and custom apps everywhere, unlike legacy SWGs that analyze only web traffic. Consistent security inspection policies are applied across all lanes.

(continued)

TABLE 2-2 ***(continued)***

SASE Requirement	Netskope One
Zero trust security principles	Enables zero trust security principles by evaluating context for identity, behavior, device posture, app, app instance, app risk rating, category, activity, content, and action to apply risk-based adaptive access control. As user behavior and anomalies are monitored, adaptive policy actions dynamically enforce the right access at the right times, including step-up authentication, constraining activities, stopping data movement, or terminating access altogether.
Security operations center (SOC) enablement	Provides sharing of indicators of compromise and rich metadata to work seamlessly with SIEM; security orchestration, automation, and response (SOAR); and other dashboards used by security personnel to investigate alerts and respond to incidents.

The Right SASE Architecture

Juggling myriad intricate security rules across countless appliances is the old, inefficient way. With SSE at the core of top-tier SASE products, you can craft overarching policies that articulate your security aspirations for every byte of data coursing through your network. From web activity and both the managed and shadowy corners of SaaS to the vast expanses of public IaaS/PaaS clouds and the bespoke applications you host there, SSE is your policy conductor. It not only commands the symphony of security services to safeguard these digital territories but does so with finesse — offering user guidance and risk-adjusted responses when necessary.

In this section, we look at architecting a robust, resilient, smart, and adaptive SASE framework that leverages the cloud's expansive reach and agility. This framework ensures that your security posture is not a static set of barriers but a dynamic, context-aware guardian that adapts to the ebb and flow of your digital ecosystem.

Cloud-native foundations for effective security

One of the fundamental principles for achieving effective SASE is recognizing that the most efficient way to secure cloud environments is from within the cloud itself. As workloads increasingly migrate to the cloud and workforces become more dispersed and mobile, traditional security models centered around a fixed corporate network and perimeter-based defenses are no longer sufficient.

Historically, the transition to cloud-centric operations revealed a significant shift in security paradigms. During the early 2010s, when the transition to the cloud began to accelerate, many established security vendors, heavily invested in appliances, were slow to adapt. Their initial response to the cloud's rise was to virtualize their existing offerings, repackaging old methods within a new context. Industry analysts cautioned against this approach, highlighting the challenges legacy vendors would face in truly embracing cloud-native and cloud-based service delivery models.

WARNING

Simply transplanting traditional security tools to the cloud will not fully exploit the cloud's capabilities or meet the evolving security needs of modern, distributed enterprises.

In contrast to retrofitting old products, the principle of cloud-native security emphasizes building new security architectures that are specifically designed for the cloud. Such architectures leverage scalable, cloud-native platforms, enabling the seamless addition and integration of services over time. This approach ensures that security measures are inherently flexible and capable of adapting to the dynamic nature of cloud services and the evolving landscape of cyber threats.

This is why all SASE implementations are cloud-based and cloud-delivered. This approach ensures that an organization's security posture is aligned with the current state of cloud adoption and poised to evolve alongside the cloud's ongoing development. This principle underscores the importance of agility, scalability, and integration in building a security framework that can effectively protect distributed networks and mobile workforces in a cloud-centric world.

Full platform convergence: The essence of SASE

Gathering a collection of security products and hoping to achieve a degree of interoperability isn't enough. True convergence results from building a unified platform that combines various functionalities into a coherent and integrated whole. This principle ensures that an organization's security and networking fabric operates as a harmonious system in four ways:

- **Unified client experience:** A converged client serves as the one-stop interface for all user interactions with web, SaaS, and private applications. This convergence goes beyond the traditional security capabilities by also providing optimized SD-WAN connectivity. This approach to endpoint-based SASE and SD-WAN simplifies access by presenting the user with a single agent that goes with them everywhere, simplifying desktop administration and the user experience.
- **Consolidated network devices:** In the physical realm, convergence manifests as a single device that anchors the office's security and networking architecture. This "one box" approach combines SD-WAN connectivity with comprehensive security enforcement, offering a streamlined outcome that effectively addresses access and protection.
- **Centralized management console:** The heart of a converged SASE platform is a unified console that offers a panoramic view of the organization's security posture. It enables administrators to craft and enforce policies across all areas, ensuring consistency, simplifying management, and enhancing the agility of security responses.
- **Integrated network infrastructure:** The final cornerstone of convergence is a unified network infrastructure that spans the globe. Each node in this network is a full-compute entity equipped with an identical suite of security and networking capabilities. This ensures that no matter where data flows, it's afforded the same level of protection and performance optimization.

WARNING

Some vendors may have the pieces necessary for a SASE product, but their offerings often resemble a disjointed collection of projects and acquisitions rather than a cohesive platform. Others may present partial portfolios, relying on third-party integrations to fill the gaps. Gartner critiqued this piecemeal approach for its inconsistent management, subpar performance, and costly deployments (`www.gartner.com/en/documents/3957375`). It also smacks of what's sometimes known as a "price list platform," in which a vendor has a number of capabilities on a price list and calls it a platform. But that's no integrated platform — it's a price list with the right things on it.

REMEMBER

True convergence in a SASE framework starts by creating a new, evolving platform that seamlessly integrates new technologies and capabilities. This approach emphasizes integration, scalability, and future-proofing the network and security infrastructure, setting the stage for an agile, secure digital enterprise.

AI/ML across the platform

Incorporating AI and ML into a SASE platform is fundamental for automating tasks on a massive scale, offering deep insights through analysis and correlation, and providing ATP capabilities far beyond the reach of traditional methods.

Here are some examples of AI and ML in SASE:

- **Automated data classification:** Data classification is one of the most time-consuming aspects of deploying DLP products. AI and ML streamline this process by automating the identification and categorization of sensitive data, reducing manual effort and accelerating the implementation of DLP measures.
- **ATP:** The dynamic nature of cyber threats demands a proactive and predictive approach to security. AI and ML excel in identifying patterns and anomalies that signify new types of malware, especially those designed to evade traditional signature- and heuristics-based detection methods. They uncover and neutralize previously unknown threats through sophisticated correlation analysis, safeguarding against polymorphic malware, phishing attempts, and zero-day vulnerabilities.
- **Behavioral analysis for insider threats:** Understanding and mitigating insider threats requires a thorough analysis of user behavior. AI and ML can analyze a vast array of activities to detect irregularities that may indicate risky behavior, compromised accounts, or potential data exfiltration attempts. This capability is crucial for identifying and responding to internal threats before they cause significant damage.
- **Optimizing SD-WAN operations:** SD-WAN network management also greatly benefits from AI and ML, which can help predict potential issues, streamline network management, reduce the need for manual support interventions, and enhance overall operational efficiency.

- **Securing IoT and device intelligence:** As the IoT continues to expand, so does the complexity of securing a myriad of connected devices. AI and ML provide a deeper understanding of device behavior, enabling real-time detection of anomalies, threats, and vulnerabilities in the IoT ecosystem.

These examples underscore the versatility and power of AI and ML across a SASE platform. From fortifying data protection to ensuring a secure and efficient network infrastructure, the integration of these technologies is indispensable. As we look to the future, the role of AI and ML in SASE will continue to grow, enabling organizations to adapt to the evolving digital threatscape with agility and confidence.

Single-vendor or multi-vendor SASE products

The SASE model was initially envisioned as a comprehensive service merging numerous security and networking functions. Over time, the capabilities of single-vendor products (like Netskope) have significantly evolved, offering robust security features that cater to the sophisticated needs of larger enterprises. Some single-vendor products also integrate seamlessly with other vendors for organizations preferring a multi-vendor approach. This flexibility ensures that enterprises can achieve optimal security and network performance through Netskope's all-in-one SASE offering or a tailored combination that leverages its compatibility with leading SD-WAN products.

The choice hinges on several factors — organizational size, technological maturity, existing investments, and the dynamics between security and network teams. For many, the multi-vendor approach represents a pragmatic path to enhanced security without compromising network performance. However, less siloed organizations may lean toward the simplicity of single-vendor products.

IN THIS CHAPTER

- **Enhancing productivity and safety with real-time, context-aware security measures**
- **Educating and guiding users on secure practices without impeding their work**
- **Optimizing performance and access across all environments**
- **Ensuring security is a facilitator, not a barrier**

Chapter 3
Empowering People through SASE

So much of security is about people — protecting and enabling them to work safely and productively without the burdens of traditional security measures. The practical scenarios for enterprise security and networking teams extend beyond guarding your organization's personnel and digital assets from those with bad intentions. It's equally about empowering your employees and customers to be productive without navigating through or even thinking about the security frameworks protecting them.

When correctly designed, secure access service edge (SASE) provides your security team with the insights and tools to effectively and intelligently address these broad challenges and apply protections in a way almost invisible to the end users. This approach allows for:

- **Protecting your systems from unauthorized access:** Ensuring that security seamlessly extends across your data centers and the cloud, applying consistent standards at all times.

- **Enabling your people:** Equipping them with access to the resources and performance they need, wherever they are, without compromising on security or user experience. The SASE framework does this not by saying "no" but by implementing intelligent guardrails that guide safe and productive work.

But security is also about shielding your staff from themselves — guarding against the mistakes, temptations, negligence, and errors of judgment that can do irreparable harm. This is critical in a landscape where more than 85 percent to 95 percent of cybersecurity incidents are attributable to human error, according to research from Tessian and IBM (`https://securitytoday.com/Articles/2022/07/30/Just-Why-Are-So-Many-Cyber-Breaches-Due-to-Human-Error.aspx`). SASE is a powerful tool for navigating these waters, removing restrictions on your people while empowering them to work safely in new ways.

This empowerment comes from SASE's ability to blend robust security measures with a seamless user experience. This ensures that your workforce is protected in a manner that allows them to remain agile without being overly burdened by security protocols. Security is no longer a barrier — it's transformed into a business facilitator.

The Road to SASE Is Paved with Context

SASE extends beyond adding layers of security. SASE redefines how we approach protection and productivity. Just as every traveler's journey is unique, requiring different routes, preparations, and safeguards, the digital journey of each user in a SASE framework is distinct. This diversity demands a security approach that's robust, smart, and adaptable.

The essence of this adaptability lies in context — the understanding that no two access scenarios are alike. For instance, accessing sensitive data from a secured office network during business hours poses a different risk than accessing the same data from a public café in another country. This variance in context requires adaptive trust and adjusting security measures in real time to fit the situation.

The backbone of any effective SASE strategy is the principle of zero trust (never assume trust, always verify!). But achieving this without a nuanced understanding of context is a tall order. Through adaptive trust, a security system discerns between a routine access request and a potential threat, leveraging insights from each user's unique interaction with the network.

The road toward a secure and efficient digital environment is also paved with a winning user experience. We must ensure that security measures appear so seamless they're virtually invisible, allowing users to work without friction or frustration, and preserving network performance.

This is the essence of SASE — a world where security and performance coexist without compromise, driven by the recognition that context is everything.

A QUICK ZERO TRUST PRIMER

Zero trust isn't a new concept in enterprise security circles, but SASE expands the scope of how the principles of zero trust are applied. Before zero trust, after a user was allowed inside the data center's services, they might be further limited to a specific set of allowable activities. But within those confines, they were essentially free to do whatever they wanted.

With zero trust, the assumption is users and devices working in your system can't be trusted — at all — until the context surrounding their interaction can be evaluated. Even then, the user is confined to only the set of resources for which they were just approved. If they try to do something else, the context must be evaluated again. Zero trust principles ensure that the right users gain the right access to the right resources at the right times for the right reasons.

Zero trust principles are fundamental to SASE architectures and are another key to properly implementing SASE. It's the idea that with all network traffic, regardless of whether you recognize the user, their device, and so on, you always assume the user may be up to no good.

Remember: If you can't see what's happening inside your traffic — the interactions and transactions inside the connections that have been allowed — your security is weak.

By moving the protection close to the users wherever they are accessing data and distributing services to those edges, your security can see inside the flow of traffic without forcing users to hairpin back to your data center. People can work from anywhere, and security policy is enforced everywhere.

Context: Changing the game for security

Effective SASE is driven by context, and the generator for that rich background is the Netskope Zero Trust Engine, which is the heart of the Netskope One platform. The Zero Trust Engine is a context service that transforms web traffic, infrastructure as a service (IaaS)/platform as a service (PaaS) interactions, and software as a service (SaaS) application activity into intelligible, actionable insight.

The Zero Trust Engine captures and decodes details inside the traffic that make it possible to identify users, their devices, applications being used, and specific activities within those applications. This decoded information is shared with all security services, making it possible to enforce detailed security policies based on cues provided by the Zero Trust Engine.

Answering basic questions

The contextual awareness delivered by the Zero Trust Engine is wide and varied, itself dependent on the specific transaction underway. That detail may include information such as the following:

- Is the user uploading or downloading something?
- If so, does that "something" include sensitive data?
- How many bytes is the user uploading or downloading?
- What application is being used?
- Is the person using a corporate or personal instance of an application?

Those examples are simple, but it may surprise you to learn that, until recently, such basic, high-level data wasn't effectively available to security teams, and not anywhere close to an aggregated, coherent presentation that could be applied across the entire security landscape.

These newly available details make it possible to construct a narrative about a user's activity that may sound something like this:

> Lauren is using her corporate instance of Gmail and has been granted access using her business login credentials: a username that she knows, a password that was verified, and a two-factor authentication (2FA) code that was accepted. You know that Lauren may have a personal Gmail account, so you'll keep track of what instance she's working with because Gmail allows her to switch accounts within her browser window readily.

This, in practice, is how adaptive trust works. It's the practical application of the zero trust principle, which states that no user or device is trusted by default, and resource access is carefully calibrated based on real-time context. This nuanced understanding of each transaction — factoring in user behavior, device status, application type, and data sensitivity — enables a tailored security posture that's both robust and flexible.

Adaptive trust operates on a spectrum. At one end, stringent controls and additional authentication steps may be applied to higher-risk scenarios. This could mean granting read-only access to certain data or requiring users to verify their identity further. Conversely, when all signals indicate low risk — trusted applications, nonsensitive data, and verified corporate use — access can be freely granted, ensuring that productivity isn't hampered by unnecessary barriers.

This approach is a departure from the traditional all-or-nothing security measures. It acknowledges that the digital workplace is vast and varied, with each user's journey presenting unique risks and requirements. By intelligently adapting security policies in real time, adaptive trust ensures that protections are proportionate to the perceived risk, enabling a seamless yet secure user experience.

Adaptive trust is, therefore, an improvement over the original notions of zero trust. It's made possible only through deep contextual awareness that spans users, devices, applications, and data. This insight is necessary for security measures to avoid being too lax (exposing the organization to potential threats) or too restrictive (stifling user productivity and satisfaction). With it, organizations can achieve the delicate balance between staying secure and getting work done, a balance that modern enterprises require.

WARNING

Context, in the sense of modern, sophisticated security, requires that your security services have their eyes open for change and anomalies at all times. Attackers have become skilled at capturing credentials by phishing SaaS application login pages and launching other cloud-oriented attacks, making it easier for them to evade legacy web defenses. When access is granted to a user, security's job is just getting started!

Examining behavior

Valuable context further expands beyond the basic questions (which we reference in the previous section) by detecting and evaluating behavior patterns after a user has access. The Zero Trust Engine applies sophisticated analytics looking for clues that an account has been compromised or a user may be an insider threat, revealing when an authorized user (or what looks like one) engages in activity outside their usual behavior or assigned role. The Zero Trust Engine looks for signs of suspicious behavior to answer questions such as the following:

- Is this user doing things they don't normally do, such as moving data?
- Is the user accessing applications or content that are different from usual?
- How much data is the user uploading or downloading, and is that activity or amount of data unusual?
- Is the user interacting with their device in an atypical manner?

REMEMBER

People may seem unpredictable, but their routines and patterns of work are recognizable. Netskope's capabilities can develop a user profile over time and use that profile to detect actions outside the norm, such as unusual data movement, attempts to misuse credentials, and many other anomalies.

Digging into rich external context

This overall context-driven approach makes security cloud-smart — very smart. You know more not only about internal context — the user, device, network, and applications that are all inside the company network — but also about what's outside the company network. Netskope makes it possible for a SASE architecture to better understand all of what makes the cloud go, such as application programming interfaces (APIs), which are how applications talk to each other, and JavaScript Object Notation (JSON), which allows data to have a flexible structure. Additional services provide contextual information about specific websites and cloud services to paint a complete picture of the cloud environment in which the user is working.

Taken together, this context makes security services more effective. Because the security services now know more, they can act more intelligently. Services can be controlled by policies that define exactly what's allowed and what isn't — down to very specific details and ever-changing context.

SASE services are greater than the sum of their parts

In the past, security appliances often functioned separately from each other, performing their individual jobs in sequence and isolation. In contrast, the architecture enabled by Netskope and required for effective SASE means that services can help each other as needed, making the entire architecture smarter. DLP can work together with user and entity behavior analytics (UEBA) to apply extra levels of data protection when a user exhibits behavior that indicates risk. For example, optical character recognition (OCR) can be used to detect what's contained in a document that a user is uploading and then determine if the document is safe to share. A team approach for the win!

The user profile further informs the process, permitting, for example, your chief financial officer (CFO) to share information with the company's accountant but preventing a business-line manager with access from sharing a subset of the same information with a stockbroker pal.

Enhancing Security with Rich User Profiles

Before SASE, user security primarily meant one thing: knowing who the person is. After you identified the user, access was granted past the perimeter into the so-called castle (the data, applications, and services the individual was allowed to use). Beyond that, the person may have had specific permissions and restrictions dictating what things they were allowed to work with, with no deeper granular understanding and certainly no protections for errant behaviors inside those permitted entitlements.

SASE still begins with identity and access management — the usual username, password, and multifactor authentication processes we all encounter daily in our digital lives. But in a SASE architecture, that's just the beginning of verifying a user's identity. Your security services now have a rich, detailed, and continuously updated user profile on which they can rely. All that other "stuff" — including what device they're using, the time of day, where they're located, applications they're using, and existing risk scores (see Chapter 4) — provide a lot more information to confirm that the user is who they say they are. Even if a user's basic credentials are compromised, your SASE is still working to protect your enterprise and its data.

Empowering Users Rather Than Just Protecting Them

SASE architecture is about much more than keeping your users safe. It's about giving them the ability to be in control of their own safety. The following sections explain in plain English what it means to empower your users rather than just protecting them.

Providing guardrails

Instead of acting as the "Department of No" — a gatekeeper that hinders access — IT security teams should strive to become the "Department of Yes You Can, with Conditions" by enabling secure, safe access by operating subtly in the background and basing access on context.

Imagine you're on a mission that requires navigating through the digital equivalent of a dense forest known for its risky paths. Traditionally, you may have encountered a gate preventing you from proceeding, halted by a security system's stern warning of potential danger. This old-guard method stops you in your tracks, perhaps suggesting a lengthy detour through IT for special permissions — a route fraught with delays and productivity pitfalls.

In contrast, today's security products recognize that your mission is vital. Instead of blocking your path, they provide protective gear so you can safely navigate the risky landscape. Visiting a website flagged for risks doesn't result in a dead end. Instead, technologies like browser isolation create a protective barrier that allows you to access the site without directly exposing your system to potential threats.

This is the essence of providing guardrails in cybersecurity: enabling safe access to necessary resources, no matter the risks they may carry. It's a nuanced approach that empowers you to do your job effectively without the cumbersome restrictions of traditional security measures. Safety is given, which allows you to focus on your tasks with the confidence that the security framework has your back.

By redefining security as an enabler rather than a blocker, we open up a world of possibilities for users. They're empowered to explore, investigate, and perform their roles to the fullest, shielded by a security approach that adapts to the context of their activities.

Coaching

To empower people, we need to teach them to navigate the digital landscape safely. Instead of monolithic security measures that block access, we want to mentor users by providing just the right access while educating them on navigating risks.

Imagine security not as a barrier but as a coach in your corner, whispering the best moves to keep you safe while you're in the ring. This coaching involves teaching users to avoid risky behavior and to perform their jobs more securely and efficiently. This approach brings users into the security solution, making them active participants in their protection.

Security is filled with gray areas that require nuanced decisions. You may find yourself needing to access a website flagged as risky. Again, traditional security may block this access outright. But with the right coaching, you're provided a safer way to proceed — perhaps through browser isolation that allows access without direct risk to your system.

This coaching approach uses these gray areas as teachable moments. Say you're about to use an unsecured cloud application for file sharing. The system may suggest, "Yes, you can proceed, but did you know we offer a secure, corporate-approved alternative?" It's about informing and guiding, not just restricting.

REMEMBER

Coaching fosters a culture of security that encourages everyone to think: Is there a safer way? Instead of heavy-handed, technology-driven rules enforcement, users are empowered to make intelligent, informed decisions. It's turning potential security risks into opportunities for learning and improvement. Sharing data may prompt a gentle nudge: "You're about to share this file externally. Are you sure?" It's not a warning. It's an invitation to consider the implications and explore safer alternatives.

By integrating coaching into our security strategy, we empower users to avoid, understand, and safely navigate danger. This approach doesn't dilute the rigor of our security measures — it enhances them by involving users in their own protection, making security a shared responsibility and an integral part of daily work.

Bettering the user experience

SASE isn't just about transforming security. The goal is to enhance the user experience within an environment that is inherently safer than anything before. Netskope is redefining the user experience to let people achieve more quickly and with better access to data. SASE does this by:

- **Accelerating performance:** The NewEdge network is purpose-built for unmatched speed and direct connectivity. It's the digital express lane that ensures that users reach their cloud services and applications swiftly, avoiding digital congestion that can impede productivity.
- **Optimizing user experience:** Beyond speed, SASE focuses on optimizing network performance to prevent potential disruptions. Through SD-WAN, NewEdge, and digital experience management, the network actively navigates the best routes, ensuring a smooth digital journey. This optimization is about more than avoiding slowdowns. The solution proactively ensures each step in the user's path is as efficient as possible.

- **Reducing friction:** Security processes are integrated seamlessly, minimizing disruptions without compromising protection. SASE streamlines these processes to be as unobtrusive as possible. The approach extends to controls and policies that support users' workflow, enhancing productivity.
- **Empowering through technology:** SASE empowers users by securing their digital environments and then leveraging this secure foundation to unlock new performance levels and user experiences. It enables users to navigate the digital landscape easily, reducing friction, optimizing their journey, and ensuring their safety.

Using AI safely

Artificial intelligence (AI) has clearly emerged as the next monumental technology shaping our future. Much like social media redefined communication in the early 2000s, AI promises to revolutionize how we work, offering unparalleled benefits to those who harness its power effectively. Yet, AI also brings significant security challenges.

Here's how SASE helps empower users to engage with AI safely:

- **Providing exploration and utilization:** Security shouldn't be about restricting access. This means ensuring that only appropriate data is fed into AI tools and controlling data exfiltration — by using the DLP capabilities already present in Netskope SASE. Guardrails surround not just the data, though: Just as we verify the legitimacy of websites to guard against phishing, we must validate the legitimacy of public AI applications to protect against spoofing. SASE-enabled guardrails make it possible to leverage AI's transformative potential safely.
- **Guiding users for safe navigation:** Restricting AI usage isn't the goal. Instead, we aim to guide users in safely leveraging these powerful tools. Education and awareness are essential to helping users recognize when they're entering risky territory. For instance, using a generative AI (GenAI) tool (for example, ChatGPT or Gemini) to generate code could be incredibly efficient. However, users must be cautioned against supplying sensitive or proprietary information to

public tools. The prompts people supply and the responses they receive become public, and the GenAI model retains a history of that information for training purposes. Anything that's gained from an interaction could appear in subsequent interactions with other people. When possible, coach users toward approved GenAI tools obtained under an enterprise license. This ensures that data remains secure while fostering an environment of informed decision-making.

- **Accelerating performance:** Access to AI tools must be swift and reliable. Through the NewEdge network, Netskope provides a resilient and redundant fabric that ensures fast, uninterrupted access to AI services. This seamless connectivity enables users to interact with AI applications efficiently, enhancing productivity without sacrificing security.
- **Reducing friction in AI utilization:** The ultimate aim is to minimize any obstacles that may deter users from leveraging AI in their work. We significantly mitigate friction by establishing secure guardrails and ensuring rapid access, making AI tools readily accessible. This approach ensures that safety measures do not impede innovation but facilitate secure, efficient use of AI technologies.

SASE is an ideal foundation for safely integrating transformative technologies like AI into our daily operations. By providing guardrails, coaching for safe usage, ensuring fast and reliable access, and reducing friction, we empower users to harness AI's potential safely. This boosts organizational productivity and positions companies at the forefront of innovation while maintaining a steadfast commitment to security.

When you get SASE right, embracing all the principles that we describe in Chapter 2 and applying them as we describe in this chapter, your users are safer and more empowered to be effective at their jobs. Your people are protected. Your organization benefits when employees are free to be productive without compromising valuable assets or running afoul of compliance and governance concerns.

IN THIS CHAPTER

- » Changing the security game by setting high-level policies
- » Using Netskope SSE superpowers to control data whenever it's accessed
- » Overcoming the challenge of unmanaged cloud apps and services
- » Getting a look at single-pass inspection in action
- » Understanding why zero trust is essential for effective data protection

Chapter 4 Protecting Data and Applications

In the past, protection meant keeping everything safely inside the perimeter of your data center. Today, data and applications are outside your data center fortress and in the cloud. It's time to leave some outdated concepts of data protection permanently behind.

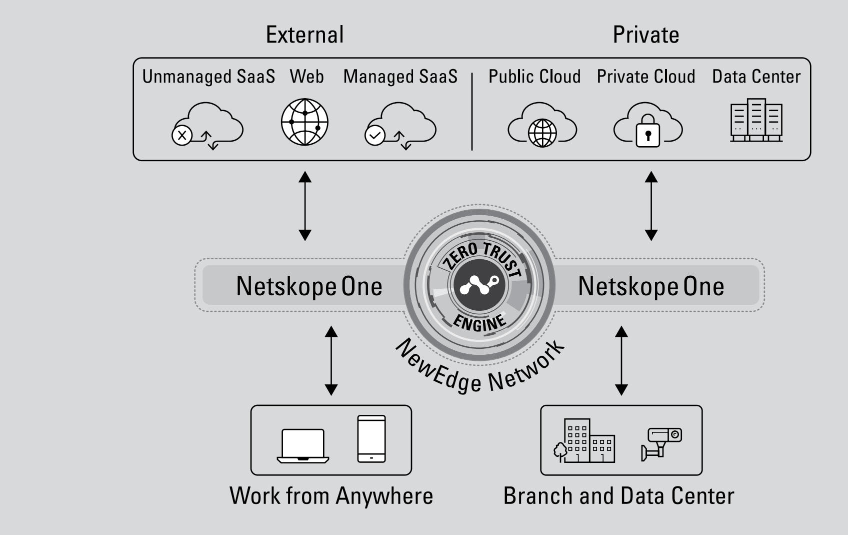
This chapter examines how data protection must evolve to be successful and how Netskope SASE technology helps you ensure that your organization's sensitive data isn't misused or vulnerable.

NETSKOPE ONE: THE CONVERGED SASE PLATFORM FROM NETSKOPE

Instead of a sprawling collection of multiple independent tools, Netskope One provides organizations with a single coherent platform with one console, policy engine, inspection point, cloud network, client, and gateway.

Netskope One (see the following figure):

- **Simplifies administration by offering a unified policy that spans all channels, reducing operational cost and complexity and better safeguarding the business.** This unified approach frees teams from the inefficiencies of switching between multiple consoles and depending on error-prone integrations typical in cobbled-together portfolios. This simplicity streamlines operations and ensures more effective and consistent application of security practices across the business.
- **Decrypts and inspects all internet traffic efficiently and without compromising the user experience, including major cloud applications such as Microsoft 365.** This thorough inspection ensures comprehensive visibility and strengthens the overall security posture. Thanks to Netskope's extensive network peering and close proximity to user locations, users frequently experience faster performance compared to direct-to-net.
- **Integrates with and extends a company's existing investments, simplifying and strengthening an organization's overall security posture while improving operational efficiency and effectiveness.**
- **Offers a practical and nondisruptive solution for enhancing security and efficiency.** Netskope One enables the consolidation of tools and capabilities within an existing network and security architecture aligned with a company's business needs, priorities, and operational timelines. This approach avoids the risks and costs associated with complete system overhauls or purchases of unnecessary products.



Conquering Complexity with the Power of Policies

In the past, security teams have been limited not only by their skill, but also in their reach. Their primary defenses were stacks of disparate security appliances — firewalls, secure web gateways (SWGs), cloud access security brokers (CASBs), and so on. Disjointed security environments and specialized appliances are inherently limited. Worst, after enduring the micromanagement needed to tell each of those specialized boxes how to do its job, these systems don't have the visibility, reach, or power to properly secure the cloud or to work together to prevent and respond to threats. The only choice is to block access even when that policy doesn't make sense because the user context is available.

Netskope fixes the problem by replacing that disjointed mess. It enables your security team to set broad macro-level policies — a consistent set of instructions that describe the outcome you want. Netskope Intelligent Security Service Edge (SSE) helps transform those instructions into action, coordinating and directing security services to achieve your desired results.

This builds on what we describe in Chapter 3, moving beyond the rudimentary block-or-allow strategy by incorporating context-aware policies, nuanced controls, and coaching, to enhance user engagement and productivity without compromising security. This approach simplifies life for your security team. Fewer devices to control and fewer rules to write means less potential for errors. Maintaining and modifying this system as needs change is easier. Even when underlying systems are updated and improved, policies stay the same. Services can evolve quickly to address new threats because changes don't disrupt the security framework.

Protecting Data

In the era before secure access service edge (SASE), data loss prevention (DLP) systems tracked data moving out of your enterprise network to meet compliance requirements and to prevent that data from being used or shared in unauthorized ways. Now company data increasingly lives outside the enterprise among cloud services and applications; it also moves within and across cloud apps, sometimes without ever touching the endpoint.

Netskope watches web traffic, infrastructure as a service (IaaS)/platform as a service (PaaS) cloud activity, SaaS applications, private application sessions, and even traffic directly flowing from the endpoint to secure all that data. Netskope SSE remembers what it has learned to continuously enhance security services. Specialized controls give it awareness no matter what managed or unmanaged cloud service is used and whether users are in your offices or remote. Netskope SSE recognizes what users do within each service and what happens between and among services (for example, if an employee downloads sensitive data within a managed service and then tries to upload that data to their personal Gmail account).

Netskope SSE implements your security policies automatically to protect data. When you set a policy to prohibit the sharing of confidential information, Netskope SSE uses its DLP service and image classifiers to notice if a user captures, for example, a screenshot of a confidential Microsoft PowerPoint slide or a photograph of a whiteboard image with confidential text and prevents that user from emailing or uploading the screenshot or photo to unmanaged or personal shared drives or sharing the data in a web form.

REMEMBER

Artificial intelligence (AI) and machine learning (ML) boost data protection.

Netskope SSE uses AI and ML as extra firepower to detect nuanced contextual details with greater accuracy. These technologies enable specialized capabilities, including the following:

- **Pattern and image detection:** Using algorithms that help categorize information to provide a dynamic web page risk rating and to detect malicious documents and images of confidential information
- **Anomaly detection:** Recognizing occurrences in data or behavior that are rare, unusual, or otherwise out of place

Specialized AI/ML classifiers do things like determine what types of pictures are being moved around to recognize confidential content such as passports, whiteboard images, driver's licenses, and screenshots. Other classifiers analyze document types to detect source code, résumés, and other sources of protected data. This capability is a powerful enhancement to the accuracy and efficiency of data security, important to securing the volume of data being created today.

Protecting Applications

Today's organization relies on several categories of applications, including managed applications, unmanaged SaaS applications, public IaaS/PaaS cloud services, and custom apps hosted in the public IaaS/PaaS clouds or in legacy data centers.

Security teams were once able to protect applications from external threats just by keeping firewalls up to date. Later, web application firewalls added more protection. But that protection was limited to web applications running inside the data center.

When cloud applications first arrived, cloud application vendors were asked to provide management application programming interfaces (APIs) that allowed IT departments visibility into what users were doing with the applications and gave them a bit of control. These apps (common examples include, such as Salesforce, ServiceNow, and Workday) became under company management and were known as managed or approved for employee use apps. It was at this time that the need for the advanced single-pass inspection method became apparent (refer to the next section). This innovative approach, channeling all traffic through a global edge network for real-time scrutiny, represents a leap in securing web content, SaaS applications, unsanctioned IT, and public cloud services with a unified security posture.

Netskope provided one of the first tools used for this management with its cloud access security broker (CASB), which utilizes the APIs provided by Google, Microsoft, Salesforce, and others to give access to whatever monitoring and control capabilities those app developers had included.

WARNING

Many valuable applications don't have published management APIs. Sometimes these unmanaged apps can be evaluated by IT staff for reliability, security, and safety. But as we discuss in earlier chapters, employees often use whatever app they want — resulting in that unauthorized, unmonitored shadow IT.

With Netskope SSE, however — and unlike traditional SWG — CASB functionality expands dramatically. Deep inspection capabilities distributed throughout the Netskope platform monitor the HTTP/S and API traffic of all web and cloud-based apps your employees use. That includes both your managed and unmanaged apps and services previously invisible to CASB. Shadow IT steps into the light!

Netskope can discover tens of thousands of cloud apps and services, assigning a risk rating to each. That risk rating is based on Netskope's Cloud Confidence Index, an objective measure of a cloud service's risk readiness derived from Netskope resources and a variety of industry threat intelligence services. Netskope SSE uses that rating to inform users and security teams and to steer enforcement of your security policies. When a user is logged into your organization's cloud services, such as Microsoft Office 365, their activity is monitored so they can't download data in that instance and then upload it to an unmanaged, risky cloud app.

Seeing Netskope in Action

Chapter 2 describes the Netskope SSE single-pass inspection approach. Here's a deeper look at how Netskope SSE applies that approach to secure data and applications:

- **Stage 1:** Netskope SSE identifies multiple instances of cloud services and applications to differentiate personal, third-party, and corporate instances of email and/or productivity applications. Netskope SSE uses the Netskope Cloud Confidence Index rating system to block access to malicious websites, risky software as a service (SaaS) applications, and unsafe cloud services. It also actively works to stop malware and other sophisticated web threats from spreading.
- **Stage 2:** Using metadata about the user's identity, location, device, and network, Netskope SSE adjusts the level of access for each session based on that context. For example, if Netskope SSE determines that a fully authenticated employee is using a personal tablet on a public Wi-Fi hotspot, they can be prevented from accessing a critical, managed cloud application.
- **Stage 3:** Netskope SSE enforces control over users' specific activities to reduce the risk of data being leaked and exposed. Rules about uploading and downloading documents, sharing screenshots, filling in web forms, and creating, posting, and publishing to services such as social media are enforced in each application and instance.
- **Stage 4:** Netskope SSE continuously monitors all activities allowed by the previous steps, watching for anomalies and threats. It recognizes sensitive data moving around and reacts on the fly based on the sensitivity of the data, type of action, and other relevant parameters. ML-enhanced image classifiers and pattern detection techniques kick in. Netskope SSE may block certain specific actions, trigger an alert, query the user about their objectives, ask for step-up authentication, or quarantine data for further inspection by security teams. Netskope SSE offers very detailed context, so false positives are rare.

Netskope SSE expansively implements the guiding principles of properly implemented SASE so data and apps are protected, wherever they are and wherever or however they're accessed.

The Importance of Zero Trust Principles to Data Protection

No honest discussion of data protection is complete without referring back to our good friend zero trust. The idea is that no users accessing data should be inherently trusted, and access to applications and data should be kept to as little as possible. Products built with zero trust principles such as zero trust network access (ZTNA) are well known in security and networking circles. But what does zero trust mean for data protection?

REMEMBER

Like other pre-cloud frameworks, DLP was founded on the idea that everything of importance is inside a data center, protected by a network perimeter. In the old days, the job of data protection was to prevent data from leaking out in unauthorized ways and to stop unauthorized individuals from getting inside the perimeter to access that data.

That approach doesn't work in the modern cloud era. Some crucial data is in the data center — behind the traditional perimeter — but at least as much (and increasingly more) data is in SaaS apps and in apps hosted in IaaS/PaaS, the public clouds. Organizations must rethink data protection in response to the way users work these days in order to protect a much wider, much more dynamic attack surface. You need a way to grant users access to just the data they need, at the time they need it, and nothing more.

Netskope was first to describe the term *zero trust data protection* as a security approach that provides continuous, real-time access and policy control based on risk and context. Context helps you understand what's happening between users and apps and informs how to provide the correct level of control to allow and prevent data access based on a deep understanding of who the user is, what they're trying to do, and why. It's what allows security teams to define and enforce adaptive access conditional controls based on data sensitivity, app risk, user behavior risk, and other factors — and to do all that in real time. The result is more effective security, thanks to continuous risk management.

A continuous risk management approach is the only effective way to manage risk dynamically across a mix of third-party applications when you have a remote-first workforce that needs always-on access to cloud apps and data to stay productive.

REMEMBER

Zero trust data protection isn't just a new way to think about DLP or another speculative marketing idea that hitches itself to the popularity of the *zero trust* term. Zero trust data protection gets to the heart of what best-in-class SASE is all about, which is to transform security and networking for the access-from-anywhere era of the cloud and ensure that data is protected everywhere. A unified, comprehensive approach to SASE and zero trust data protection separates true SASE technology providers from the pretenders.

IN THIS CHAPTER

- **Developing a full understanding of your organization's cloud security**
- **Improving risk assessments by seeing activity outside your data center**
- **Gaining control over who's moving what data and where**
- **Fully enabling and securing your remote workforce at scale**
- **Refactoring your data center to work securely with the cloud**

Chapter 5 Ten (or So) Steps to Get to SASE

This chapter provides a step-by-step approach to implementing secure access service edge (SASE), from knowing your starting point and where you're going to optimizing everything in between. It also provides an overview of how to achieve success by deploying SASE in a series of nine steps. At each phase, you'll make big strides toward significantly increasing your organization's security posture, managing risks, and providing your employees and customers with the experience they require.

Step 1: Determine Where You're Going

When undertaking a new project, the need to deliver quantifiable results today (or at least very quickly!) is a significant challenge facing a chief information officer (CIO), chief information security officer (CISO), or anyone with high-level responsibility for enterprise networking and security. Unlike typical IT projects where long development cycles may be tolerated, security must demonstrate value right away and deliver quick wins. Vulnerability is scary.

SASE addresses that vulnerability using an architecture that reflects the way security must be delivered now and the increasing (and favorable) convergence of security and networking. But true SASE is a long-term evolutionary process — a journey. Your organization will grow into SASE. The key to your success is to deliver a succession of tangible victories — deliberate leaps forward — that repeatedly expand and strengthen your organization's security in demonstrably meaningful ways.

REMEMBER

But to do that, you must know where you're starting from and where you're going.

By approaching SASE in a gradual, considered way (remember, it's a journey!), you can deliver continuous, dramatic results as you steer your enterprise away from its parochial data center–centric worldview to one that can fully and securely reap the many benefits of the cloud.

Step 2: Gain Awareness and Visibility

Before you can solve any problem, you have to admit that the problem exists. This book explains how enterprise security has remained rooted in the traditional data center and, thus, hasn't kept up with the security and access needs of today.

More than half of enterprise app traffic and users are getting work done on networks the organization doesn't control. Work from home is the new norm (see Chapter 1).

You and your organization need to come to grips with the severity and breadth of what has escaped your control and the reality that the stuff outside your control is how your business does business today. Implementing the Netskope One SASE platform in a basic way, even for just one service, will turn the lights on and show you what's happening and what's not protected.

TIP

At a minimum, you need thorough visibility into user activity in the cloud if you want to be confident in any product you implement. You also need your organization's decision-makers on board. You get buy-in when those decision-makers understand that SASE will protect critical things they value but don't realize are dangerously exposed. Millions, even billions, of dollars in value is derived from the work being done "out there."

Step 3: Choose between Single- and Multi-Vendor SASE Strategies

This decision, which we explore in Chapter 1 and 2, requires thoughtful consideration of your organization's needs, technological maturity, and existing infrastructure. Choosing between a versatile all-in-one provider and specialized separate vendors can significantly influence the outcome:

- **Consider your organization's scale and complexity.** Large enterprises with extensive security investments may lean toward a multi-vendor approach to maintain certain security features. Smaller entities, without siloed network and security teams, may find a single-vendor product that meets their needs. However, a single vendor like Netskope addresses any scenario.
- **Evaluate integration and cooperation.** The essence of SASE lies in seamless integration. Whether you're opting for a comprehensive offering from a single vendor or harmonizing capabilities of two, the focus should be on ensuring these components work in synergy, as highlighted in our discussion in Chapter 1.
- **Assess the evolution of SASE platforms.** Recognize that the SASE landscape is rapidly evolving. Netskope's journey from a cloud access security broker (CASB) to a unified SASE platform exemplifies the progression toward more integrated offerings. Keep abreast of these developments to make an informed choice that aligns with your long-term security and networking goals.

Making this choice is a strategic decision that influences your organization's agility, security posture, and operational efficiency. Revisit the insights from Chapter 1 to guide you through this pivotal step toward a secure, efficient, and user-friendly network environment under the SASE framework.

Step 4: Place Core Inspection Points between Users and Apps

With the Netskope One SASE platform firmly in place and visibility into all your traffic dramatically increased, one thing is certain: You may not like what you see next.

Are your people using Microsoft 365? Salesforce? Workday? Box? The answer is almost certainly yes. But how big and how mature is that cloud environment beyond your security perimeter and outside of what you can easily see? Just how much of your organization's data is running around out there, unchecked?

For the first time, your organization will be aware of just how at risk it has been. You'll see the flow of data, some of which may be particularly sensitive, among unsecured sites, services, and apps.

Now you have a truthful, and likely worrying, picture of where your organization stands with respect to its dependence on the cloud. So many apps and services, so few effective security controls. Until now.

Netskope Intelligent Security Service Edge (SSE) establishes a single-pass, funnel-like, core inspection point for all your traffic in the cloud and in the data center (see Chapter 2). That core inspection point is better than your old perimeter — way, way better.

REMEMBER

Whether it's the result of shadow IT that has been knowingly ignored or a more deliberate process of business digitalization, your old and outmoded security systems have been blind to the details.

By replacing old secure web gateway (SWG) and similar appliances, you'll finally have complete visibility into who's using non-enterprise-grade applications and services and what enterprise data is being sent "out there" beyond your control. As shown in Table 5-1, Netskope One and its new inspection points in the cloud let you see what's going on inside all that traffic: web, managed and unmanaged software as a service (SaaS), infrastructure as a service (IaaS)/platform as a service (PaaS) activity, and custom apps in IaaS/PaaS clouds.

TABLE 5-1 Using Inspection Points to Monitor Traffic

Out with the Old	In with Netskope
Legacy SWG — only yes or no to web traffic	Deep inspection of all traffic: web, managed and unmanaged SaaS, IaaS/PaaS activity, and custom apps in IaaS/PaaS clouds.
Secure Sockets Layer (SSL) appliance	Transport Layer Security (TLS) decryption is performed in the cloud at cloud-scale with no appliances required.
Legacy CASB reports usage details of only managed SaaS apps that provided application programming interfaces (APIs)	Monitors all traffic to and from managed and unmanaged apps, regardless of whether they offer APIs; also sees what data is being used with apps, services, and websites.

Step 5: Introduce Zero Trust Principles to Web, Cloud, and Activity Access

This is when you'll really begin to put your SASE to work as you lay its foundation. Fortunately, the capabilities needed to set things right are built into the Netskope platform. You have everything you need to reestablish control over your enterprise data, not only on your own network but also, ultimately, everywhere in the cloud.

In Step 5, as shown in Table 5-2, you'll leverage expanded security controls to apply context, going beyond the simple yes-or-no options of your old appliances. Netskope One also performs deep inspections of both your web traffic and your cloud traffic. And now that you've established a new inspection point, its functionality is expanded to exert fine control over the movement of and access to data to manage risk according to policies that make sense for your business.

TABLE 5-2 Setting Policies to Manage Risk

Out with the Old	In with Netskope
Legacy data loss prevention (DLP) — protects only stuff in the data center	Intelligent DLP protects all data being moved anywhere.
Basic user and entity behavior analytics (UEBA)	Expanded behavior anomaly detection and user risk scoring.
Various signature- and heuristics-based scanning tools	Advanced threat protection, including sandboxing and machine learning–based anomaly detection.

Step 6: Optimize Network Performance

Optimizing network performance is crucial to transcending traditional networking limitations and providing secure, high-performance, seamless global access to cloud services. The following features help you optimize network performance:

- **Architectural mastery and global infrastructure:** Built by industry-leading networking experts, Netskope NewEdge has evolved into one of the world's most expansive cloud networks, offering secure and optimized connectivity to facilitate access to essential services from anywhere. Netskope's strategic selection of data center locations and widespread peering arrangements are designed to meet the unique demands of its global customer base, ensuring minimal latency and maximum uptime.
- **Innovative networking solutions:** Netskope's ownership of the cloud infrastructure allows us to pioneer features like proactive digital experience management (P-DEM), cloud packet capture, and direct peering with hundreds of popular providers setting Netskope apart from our competitors. These innovations, born from our end-to-end control and visibility, offer our customers capabilities that are not feasible in an IaaS/PaaS cloud network.
- **Superior user experience:** Integrating the NewEdge infrastructure with the single-pass security architecture and P-DEM results in a user experience unmatched in the market. Netskope's industry-leading performance metrics are underpinned by comprehensive service-level agreements (SLAs), affirming the commitment to delivering the best possible service.

- **Visibility and automation:** The drive to build this infrastructure was fueled by the necessity for end-to-end visibility. Unlike conventional approaches that treat the network journey as a black box, Netskope P-DEM presents a detailed view of every step within the NewEdge infrastructure. Beyond visibility, the use of actionable insights enables data-driven automation across the Netskope products, reducing the total cost of ownership for customers and ensuring that they can use the Netskope service more effectively to secure their end-user traffic without performance trade-offs.

Access to a robust, high-performance network is a cornerstone of SASE. Organizations can prioritize network optimization through Netskope NewEdge to ensure a secure, efficient path to digital transformation, where security and network performance enhance rather than inhibit business operations. This is integral to achieving the holistic security and networking harmony that SASE promises, enabling enterprises to thrive in the cloud era.

Step 7: Extend Zero Trust to Data Protection and Private Access

Now that your organization is smarter about its traffic, able to see what's going on, and able to enforce policies to secure its data, you can realize the promise of a remote-first workforce. You're going to make it possible for people to work from anywhere and make it a great, fluid, productive experience that is highly protective of your data, your applications, and your employees.

The most noticeable change is to move away from your legacy virtual private network (VPN) — that long, inefficient hairpinning route that forced all your remote users' traffic to detour back to the data center on its way to the internet. With Netskope NewEdge, you can efficiently route that traffic to its destination while enforcing your security policies to protect data.

Zero trust means enforcing the assumption that any user may be up to no good at any time and ensuring that data is always protected no matter where it needs to go. The Netskope platform's deep contextual knowledge about the user, device, network, behavior, and hundreds of other details is used to limit activity only to what has been allowed by policy and to ensure that any claims, such as a user's identity, are verified.

After it's in place, your security and networking will be transformed to suit the needs of cloud workers and to satisfy the board-level demands for zero trust strategies (see Table 5-3).

TABLE 5-3 Security and Networking That Meet the Remote Workforce's Needs

Out with the Old	In with Netskope
Legacy VPN	Security cloud to route and protect traffic as dictated by policy.
	Netskope One Private Access to combine award-winning zero trust network access (ZTNA) with the power of software-only Endpoint SD-WAN.
	Zero trust data protection.

Step 8: Refactor Internal Data Center Controls to Closed-Loop Risk Management

The data center is just one more place people and data have to go — it's no longer the center of attention. When you're far along in your SASE architecture, it's time to reconsider the data center.

Perhaps a few applications that are too unwieldy to move or too precious to let out of your sight remain in the data center. To access these apps, you could use Netskope One Private Access which replaces VPNs while providing secure access worldwide.

As for all those other boxes and bits that have been replaced by Netskope platform services in a SASE architecture, this is your opportunity to dramatically reduce the complexity and upkeep cost of your network, with those old systems depreciating out of existence and receding into the past while you and your enterprise look forward.

Table 5-4 indicates which older systems or technologies can be replaced using Netskope's platform.

TABLE 5-4 Providing Secure Access to the Data Center

Out with the Old	In with Netskope
Firewalls, intrusion prevention system (IPS), unprotected Domain Name System (DNS)	Firewall as a service (FWaaS) provides control over outbound non-HTTP(S) traffic, including, for example, steering DNS traffic to the Netskope cloud to protect against DNS abuse.

True SASE yields ongoing operational cost savings. Table 5-5 shows a snapshot of what that can look like with a successful SASE deployment. Your finance people will be among the many stakeholders to thank you!

TABLE 5-5 Ongoing Operational Expenditure Savings

Domain	What Happens	Estimated Average Savings
Multi-cloud access	Enable multi-cloud strategy Improve user experience Streamline procurement and adoption Enable business unit–led apps Close help desk tickets faster	30% on connection and infrastructure 20% on future cloud costs
VPN replacement	Remove VPN appliances Direct-to-net traffic for bandwidth-heavy apps Reduce virtual local area network (VLAN) and firewall policy changes	80% on hardware 50% on security changes and admin
Business partners	Manage third-party access Direct access to published apps Apply granular controls for activity Constrain lateral movement	Varies
Mergers and acquisitions	Make onboarding and integration more efficient Consolidate current and future network and security costs Synchronize policy	40% on hardware Onboarding is five times more efficient

Step 9: Monitor, Assess, and Optimize

Traveling the road to SASE will take time, but it offers huge, transformative benefits to your security and infrastructure teams and your organization at every step along the way. Security certainly improves throughout the journey, but the impact reaches much farther than that. You'll quickly begin to realize cost savings as over-provisioned, capital expenditure (CapEx)–intensive legacy security appliances no longer need to be maintained, upgraded, and replaced. The network experience also improves journey, as fast, optimal paths replace inefficient and slow routing.

However, even though the principles behind SASE are the same, the way SASE works at your company will be different from that at another company. To keep SASE alive and healthy, you must monitor its effectiveness, assess where improvements are needed, and take steps to optimize your implementation.

Taking the time to continuously improve will protect your gains. It's difficult to overstate the benefits that Netskope One, as a platform approach, brings to enterprise security and networking:

- Where your security team had been overwhelmed, trying to make sense and correlate what a dozen or more complex and independent security applications were trying to tell them in the heat of the moment, they'll now have a unified, automated platform working in real time. All the security services will deliver a shared, coherent message resulting in fewer errors and making it possible to act decisively — and immediately. Every person on your team will be able to get more done to enhance security further and enable your business to run smoothly.
- Where your networking team had been stuck in the past, trying to force all traffic through a suboptimal internet architecture with little visibility into connectivity problems, they'll now have a network infrastructure designed for modern ways of work. All traffic flows directly to its destinations, and performance or access problems are clearly surfaced for immediate resolution.

Most important, however, properly architected SASE will transform business operations and the relationship between employees and technology and among your networking and security teams. Shadow IT can emerge into the light, enabling true digital transformation where best-in-class applications and tools can quickly and securely be adopted, fueling efficiency and driving opportunity. User experience will be preserved, and your users will be happy and productive. This is possible only when security can confidently support digital innovation, facilitate the widespread adoption of cloud services, and align with networking and all parts of the business on digital transformation priorities. That's what you get with true SASE.

Create a SASE architecture that protects data and drives lasting business value

In a digital world that has left the restrictive confines of the data center for the wide-open possibilities of the cloud, a secure access service edge (SASE) architecture is the only architecture that makes sense. Empower your users, protect your data anywhere it moves, preserve network performance, and grow your business with a well-designed SASE architecture that combines advanced security capabilities with modern SD-WAN and zero trust principles as catalysts for success.

Inside...

- Learn about the evolution of data, applications, networks, and security
- Understand the roles of advanced security capabilities, SD-WAN, and zero trust in a SASE architecture
- Secure your remote workforce at scale and improve the overall experience for your users
- Build a confident plan for security and network convergence

netskope

Having worked at the intersection of cloud and security for pretty much as long as that's been an actual topic, **Steve Riley** is Field CTO at Netskope and a widely-renowned expert speaker, author, researcher, and analyst. His decades of experience also include Gartner, Riverbed, Amazon Web Services, and Microsoft.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-26428-5
Not For Resale

9 781394 264285

for dummies®
A Wiley Brand