Brought to you by:

netskope

Security Service Edge (SSE)

for dummies®
A Wiley Brand

Design your IT for the future of cloud security

Deliver CASB, SWG, ZTNA, and firewall from one platform

Master SSE as part of a SASE and Zero Trust architecture

Netskope Special Edition

Jason Clark
Steve Riley

About Netskope

Netskope, the SASE leader, safely and quickly connects users directly to the Internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, firewall as a service, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing Zero Trust principles across data protection and threat prevention everywhere. Unlike others who force tradeoffs between security and networking, Netskope's global security private cloud provides full compute capabilities at the edge.

Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total cost of ownership. Learn more at www.netskope.com.

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

From Netskope: Amanda Anderson, Lauren Baker, Chad Berndtson, Jeff Brainard, Tim Chiu, Tom Clare, Catie Halliday, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Sasi Murthy, Shamla Naidoo, Lauren Polito, Zoe Revis, James Robinson, James Yokota, Svetlana Rubin

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

Security Service Edge (SSE)

for dummies®
A Wiley Brand

Security Service Edge (SSE)

Netskope Special Edition

by Jason Clark and Steve Riley

for dummies®
A Wiley Brand

Security Service Edge (SSE) For Dummies®, Netskope Special Edition

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

ISBN 978-1-119-87700-4 (pbk); ISBN 978-1-119-87701-1 (ebk)

Publisher's Acknowledgments

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

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Senior Managing Editor: Rev Mengle

Business Development Representative: Jeremith Coward

Production Editor: Tamilmani Varadharaj

Special Help: Nicole Sholly

Table of Contents

Introduction

The overall business transition to the cloud is happening far faster than many experts predicted. That speed has left most companies reliant on security platforms built for a bygone world dominated by on-premises data centers. The COVID-19 pandemic further accelerated and complicated the situation, stressing CISOs who are responsible for protecting a work-from-home staff that may not ever fully return to the office.

The good news is that Secure Access Service Edge (SASE), a security architecture framework, points the way to a cloud-based solution that provides the protection every business needs, wherever its staff members are located. Even better is the news that Security Service Edge (SSE), which is the fundamental set of security services in SASE, provides the capabilities necessary for implementing security services to protect remote workers, cloud-based technology, and existing on-premises applications and infrastructure.

SASE is a framework. SSE is a set of services you can purchase today. This book explains SSE and explores its foundation, which is constructed from innovative ideas like Zero Trust; adaptive, context-based security; and novel approaches to network design. The book then shows how familiar services are knit together inside SSE, alongside new, advanced technologies that can dramatically enhance security.

About This Book

It's time to reshape the modern security landscape. Learning about SSE will help security and business staff prepare themselves for the steps necessary to remake enterprise security — currently a bottleneck — as an amplifier and enabler of digital transformation. The book sets the stage with explanations of SASE and SSE, then offers a road map to how you can bring this new security to life. Use of the cloud requires every company to transform its security. This book advises you on how to prepare.

Foolish Assumptions

You aren't a stranger to the Internet or to security. You know that the traditional security model we all use is being stretched to its limit. You're also aware that the cloud is both a productivity booster and a dangerous place where the credentials and data of individuals and companies are under attack. Lastly, you have an interest in ameliorating that challenge for your company, employees, shareholders, customers, and business partners using the powerful evolution represented by SASE and SSE.

Icons Used in This Book

We use icons throughout the book to highlight important information.


TIP

The Tip icon offers shortcuts and other information that can make your life easier.


REMEMBER

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


WARNING

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

Beyond the Book

For more information on Netskope solutions, visit `www.netskope.com`. For a continued deep-dive on SSE, visit `www.netskope.com/security-defined/security-service-edge-sse`.

IN THIS CHAPTER

- Exploring the future of security
- Understanding how digital transformations affect security
- Discovering how to create the security nirvana we all want

Chapter 1
How Context and Integration Accelerate Security Transformation

Organizations shift to cloud applications to realize the clear business benefits of speed, efficiency, and insight that cloud provides. To really protect data, people, and applications in the cloud, security can no longer consist of the simple binary, accept/deny decisions that applied in the days when the network was supreme and most workers were in one place. Security must be made smarter by using detailed context to craft just the right protection for your organization, no matter where your workers are located. Security must follow the data wherever it goes, and it must be easy to apply so it doesn't slow down the business.

Where Security Is Headed

Now is a profound time to be immersed in security. The power and quality of cybersecurity technology are making astonishing strides. Never have security professionals had to grapple with so much change so quickly, and never have they had an opportunity

like the present to revamp security into a strategic business enabler. Data, applications, and workers have migrated into the cloud. Security must follow.

Companies that adopt a cloud-based security posture to enable digital transformation will innovate faster and more safely than companies whose security posture is entrenched in yesterday's ideas. We foresee a new era in which security professionals finally leap ahead of attackers and support their businesses as cloud-powered digital transformation goes into overdrive.

Efforts to force legacy security systems onto the cloud aren't succeeding. Under a framework called Secure Access Service Edge (SASE), security is transforming to address the cloud-based, hybrid workplace.

WARNING

Best-of-breed security products and services of the past won't succeed in the cloud. Nor will retrofitting or relabeling old security technology as "cloud enabled."

Security technology vendors are instead offering new cloud-native products and services to provide protection when data is stored and applications are run on infrastructure that companies themselves don't control. New security technology must protect not just *access* to data, but also the *use* of that data.

It's helpful to look at cloud-ready security in terms of four fundamental ideas:

- **SASE** is the framework for implementing a cloud-based, converged infrastructure for networking and security functions. SASE combines concepts such as Zero Trust, software-defined wide area networking (SD-WAN), and Security Service Edge (SSE) to guide us to a security and networking posture that protects and governs the cloud and the new work-from-anywhere environment. Analysts recognize that this new architecture provides comprehensive security for a cloud-centric world. (See Netskope's *Designing a SASE Architecture For Dummies* for a complete introduction.)
- **SSE** is how all the security services necessary for SASE — which were previously separate applications, products, or services, often from different vendors — come together in a unified, integrated form that provides greater capability and efficiency and reduces complexity and cost. SSE represents

deeply integrated security capabilities that are aware of each other, work well together, and are sourced from a single vendor. Netskope further defines a set of extended capabilities that we call *proper SSE* (see Chapter 3).

- **Context** determines how the integrated security capabilities of SSE are applied as the control mechanism for keeping data, applications, and people safe at all times. Context — a deep comprehension of *who* the person is, *what* they're trying to do, and *why* they're trying to do it (plus, when, why, and how) — also makes it possible to apply adaptive security policies to mitigate risk in real time. Previously, "allow" or "block" were the only options. Now, rich context supports shades of access control, such as "allow, with conditions," to provide security that is safe without disrupting productivity. The quality and breadth of context is a critical differentiator among security vendors.
- **Zero Trust** principles differentiate truly adaptive policies from simple conditional authentication based on familiarity. The goal is not only to provide just the access and authorization each person needs to perform a given task, according to the confidence level derived from a real-time assessment of worker identity and access method. Adaptive access requires insight into what happens *after* the login — environmental signals that vary over time, historical and current behavior, and the characteristics of the data itself. At Netskope, we view Zero Trust as the starting point (no trust at the beginning of every interaction) and aim for the goal of *continuous adaptive trust,* where the amount of trust is commensurate with the determined confidence level and environmental signals.

This book explains how these concepts coalesce in effectively implemented SSE to create a new security nirvana (see Chapter 3). Companies will finally enjoy cloud-based security with everything necessary to protect a cloud-centric world of data and applications accessed by workers who are — and will remain — distributed and often far from a central office location.

Forcing Security Transformation

Explosions in several areas of digital transformation are reshaping the business world. Security transformation is vital to achieve and sustain the success of digital transformation efforts.

REMEMBER

Technologies like the cloud, Internet of Things (IoT), machine learning/artificial intelligence (ML/AI), and analytics substantially improve business outcomes. If security can't keep up, then that progress is at risk.

- **The data explosion:** By 2025, IDC anticipates there will be 175 zettabytes (ZB) of data worldwide (up 25x since 2010). As you can see from headlines, attackers are stealing company data for nefarious purposes — to sell it, to maliciously modify it, or to extract ransom. Netskope Threat Labs discovered that the cloud is an attacker playground, with 68 percent of malware delivered through the cloud in 2021 (as opposed to less than half as recently as 2020). The explosion of data accessed from the cloud generates more targets for attackers and more challenges for defenders.
- **The cloud explosion:** Businesses are adopting cloud-based infrastructure and applications to gain speed, flexibility, and agility. According to Netskope Threat Labs, the average enterprise company subscribes to more than 800 distinct software-as-a-service (SaaS) applications. A whopping 97 percent of those are so-called "shadow IT," meaning not managed by (and, in many cases, not visible to) in-house IT. Furthermore, the default security settings of many cloud applications are wide open — another reason attackers find the cloud a particularly juicy target.
- **The device explosion:** Estimates vary widely on the volume of Internet-connected devices on the horizon, from 25 billion in 2030 to an astounding 75 billion perhaps by 2025. More devices and more connectivity create a larger technology estate — and a larger attack surface. Nevertheless, device explosions often lead to accelerated innovation.

REMEMBER

Security transformation is about creating a new way to handle all these explosions so the business can do what it needs to succeed.

Companies that fail to engage in cloud-based security transformation face increasing risk. The current security landscape has become too complex, costing companies large sums in capital expenditures (CapEx), operational expenditures (OpEx), and people hours, even as its efficacy declines. Vendors must, therefore, reconstruct functions into systems that collaborate.

Creating Security Nirvana

Companies that are planning their security future must envision what security nirvana looks like, both in broad strokes and in fine detail. Practical advice — not marketing or (is there a difference?!) hype — should guide their decisions.

From a high level, here's how this transition might occur:

1. **Transform the network.**

   The network must move data as efficiently as possible among all points, including cloud services and the data center, without trading performance and worker experience for security. Traffic is routed through a network built to support SSE consisting of globally distributed points of presence (PoPs). Staff at the office, home, or coffee shop receive high-level security and performance, and company data remains protected.

2. **Consolidate security services.**

   A unified, single vendor suite offering a comprehensive SSE replaces the patchwork of legacy security appliances. Merged capabilities simplify management and administration, ensure consistent policy enforcement, and streamline traffic processing.

3. **Extend SSE usage and implement advanced security services.**

   With SSE in place, security teams can introduce powerful functions, such as remote browser isolation (RBI), cloud security posture management (CSPM), and SaaS security posture management (SSPM). Advanced capabilities such as data loss prevention (DLP) and advanced threat protection (ATP) perform better than in old models hampered by minimal integration and restricted visibility.

4. **Protect data in the cloud and company devices.**

   The same SSE vendor should also provide a firewall as a service (FWaaS) to protect cloud-based applications, company-owned devices, and data repositories.

5. **Treat the data center as just another destination.**

   The traditional corporate data center, once the sole destination through which all traffic was backhauled, becomes one more destination that the SSE routes traffic to and from. Eliminating hairpinning decreases cost, reduces complexity, and increases performance.

6. **Apply Zero Trust principles to achieve a state of continuous adaptive trust.**

   Because SSE constantly monitors traffic after access is granted, security professionals can conduct thorough contextual analysis of the session, make decisions informed by third-party risk intelligence, detect changes in risk profiles, and neutralize dangerous actions. Notifications can coach workers to improve their security habits.

7. **Improve risk management across the business with increased visibility.**

   The ability to see, guide, and control the activity of everyone in the business dramatically improves risk awareness and detection. The security team can focus on high-risk areas and more quickly deploy enhanced policies in the SSE to reduce risk. Security leaders can engage in risk and business strategy conversations that elevate them to vital positions at the decision-makers' table.

A security transformation is no small undertaking. Chapter 4 shows how Zero Trust principles enable an incremental move to full implementation of cloud-based security. Chapter 5 highlights common mistakes and principles of success and describes a representative journey many enterprises will follow if they approach SSE, Zero Trust, and, ultimately, SASE the right way.

IN THIS CHAPTER

- Reviewing the history of the firewall
- Delving into why the cloud is here to stay
- Accepting limitations of point products
- Exploring how security must be integrated and follow the data
- Appreciating the role SSE plays in security needs

Chapter 2
How the Cloud Broke the Traditional Security Model

A decade ago, few leaders predicted how quickly all forms of cloud would take hold in business. Enterprises now subscribe to, on average, more than 800 software-as-a-service (SaaS) applications, according to Netskope Threat Labs.

Cloud and edge computing are pushing more and more business workloads outside the data center. Work-from-anywhere initiatives, accelerated by the COVID-19 pandemic, inspired more people, devices, applications, services, and data to escape the traditional confines of the enterprise data center. The cloud is now critical to enterprise productivity. But as new risks materialize, the cloud is also forcing people to rethink security.

Consider how parents protect children while they're babies and toddlers. Inside their homes, they add childproofing to stairs, electrical outlets, cabinets, and toilet seats. Parents protect the interior perimeter with an alarm that alerts whenever a door opens. They protect the external perimeter with a fence in the

backyard. After they send their children to daycare, to school, and later (yikes!) to college, the goal to protect their children remains the same, but the role of the parents has changed.

Similarly, the goal of securing the cloud means acknowledging that the goal of security — to protect data, applications, and individuals — hasn't changed. What has changed is that the data, applications, and individuals have left the house, reducing the role of the firewall and relegating it far behind. Meanwhile, the fastest-growing threats are in the cloud, not in your data center. The result: Security tactics must change.

Remembering When the Firewall Ruled Security

In an earlier era, the firewall was your most important central security control point and probably the most expensive line item in your security budget. Most enterprises designed their network security architectures around the data center, surrounded by a well-defined perimeter. Being secure meant securing your network.

In the pre-cloud world, that approach made sense. The data center was, after all, a single location where a company housed its valuable digital assets. Like a well-alarmed home today, a company erected a (mostly) impenetrable perimeter around its data center. A mighty gate built of security appliances tightly constrained access. Like a parent with alarms on doors and windows, you had substantial control of your enterprise security in that pre-cloud world.

Workers traveled an exclusive, private network that connected them to the areas they needed for their work. Those in far-flung branch offices or working remotely traveled the private network, typed in the alarm code, and gained permission to access not only the applications and data inside but also all external connected destinations. Backhauling remote worker traffic through this centralized data center inside the perimeter and then back out added cost and complexity and crippled performance.

Old-school firewall security was a simple matter of allowing or denying access. After they were granted access, an individual's

presence and good intentions were taken for granted. As part of perimeter-based security, businesses adopted security designed to thwart individual threats or categories of threats as they emerged. See a threat, buy another piece of equipment. In the on-premises model, an enterprise might have a line of ten security boxes connected by a wire.

Each box performed its own particular inspection. It applied its own "Hey, I want to detect malware . . . I want to compare signatures and block intrusions . . . I want to filter email, or I want to scan for sensitive data . . . I want to guard against name resolution attacks . . . I want to provide port and protocol blocking with access control lists." Every function did its job and then routed packets to the next function in the line, which added latency and complexity.

The cloud has changed all the assumptions.

Understanding How the Cloud Enables Business

Cloud computing offers such profound flexibility and business value that, at this stage, there's no going back. (And you can ignore blustery claims of "repatriation" into enterprise data centers. Except for rare and specific scenarios, it just isn't a thing.) The cloud is appealing to CEOs, CFOs, CIOs, and businesses in general because the bulk of the infrastructure is commoditized and turnkey. The cloud eliminates spending lots of time and money investing in your own infrastructure. You subscribe to a cloud, turn it on, customize it to meet your unique business requirements, and use it. As businesses seek to accelerate revenue generation and become more profitable, moving to the cloud is part of the answer.

The cloud is appealing to your busy workers, too. They're attracted to the widely available SaaS applications that offer modern and sometimes enjoyable platforms to collaborate, communicate, handle finance, close sales, and manage customer relationships. These third-party applications in the cloud feel better, faster, and more effective than anything offered by old clunky corporate applications in the rigid confines of an organization's data center.

WARNING

But therein lies the catch — and the danger: The majority of these cloud applications are not approved, let alone controlled, by the corporate IT department — and are hardly secure. You still have the duty of protection, but you no longer have the kinds of control you're accustomed to. Adopting the cloud is like sending your children off to school or even to college — you can no longer see them and know what they're doing.

In the era of cloud, the firewall is no longer your most important security control because it doesn't comprehensively protect your enterprise from threats in the cloud. Without adequate security to protect and cover our digital processes, employees, customers, and (ahem) assets, in this new, wide-open landscape, digital acceleration efforts will be risky. In the cloud era, security's job is to enable the business value created by the cloud by managing the liability that is also created by the cloud.

Point Products Help at Points But Don't Solve the Big Problems

As workers moved out of offices and data and applications moved into the cloud, legacy security tools ensconced in the data center became blind to activities transpiring beyond the perimeter. SaaS applications required data that originated from *inside* the walls to be useful. Yet the applications themselves were *outside* the walls, rendering the data that migrated to them uncontrolled and unprotected by enterprise security.

Change was needed if businesses were to take safe advantage of cloud-based applications. Enterprises configured new narrowly focused point products across their private networks and the cloud to address the most pressing security problems and weaknesses related to using the cloud. Those tools included the following:

- **Cloud access security brokers (CASBs):** CASBs help govern and protect enterprise data stored in someone else's computer, which is an honest way to conceptualize the cloud.
- **Secure web gateways (SWGs):** SWGs protect workers and organizations from threats on the web — that is, the pages a worker visits when they're online and browsing public sites.

- **Zero Trust network access (ZTNA):** ZTNA products simultaneously shield a business's private applications from the public and make the applications available to a set of known workers.

These tools represented an early generation of cloud security. But that early generation also lacked something critical: integration.

Integrating Security Is a Must

Earlier-generation cloud security products often came from different vendors and, as a result, didn't work together. Each offered its own console and required configuring duplicate and overlapping policies (think data loss prevention [DLP] here). Each might have required a dedicated agent, creating deployment and traffic routing challenges. And each required separate contract negotiations and purchase agreements.

Imagine if your senses of sound, smell, taste, sight, and touch all were connected to different brains. Without integration, when you see a fire, smell a fire, or hear a fire, you don't know what to do because your seeing brain, smelling brain, and hearing brain aren't sharing information. They aren't correlating the inputs of all your senses.

In such a security infrastructure, you have many different systems, each with its own brain skilled in its particular domain. For example, CASB is a brain focused mainly on "I have a worker trying to get to a SaaS application."

REMEMBER

Just like your actual single brain acquires information from all your senses to make decisions about comporting yourself in the world, your security services must be fully integrated to make effective decisions that support your cloud strategy. Security Service Edge (SSE) is the brain that integrates disparate security categories. Instead of operating separately in sequence, SSE enables all these security "senses" to activate in parallel. The result: security that's both faster and more efficient. Plus, SSE is much easier to acquire, because all capabilities (CASB, SWG, ZTNA, and related) are purchased together in a single transaction.

Security Must Follow the Data

As we explain in Chapter 1, Secure Access Service Edge (SASE) describes a vision in which the traditional enterprise perimeter no longer exists. Instead, the entire portfolio of network functions and security capabilities moves to the cloud where it's immediately adjacent to workers, to data stored in the cloud, and to SaaS applications.

SASE provides a way to adjust our perspective in a cloud-first, work-from-anywhere world, where the old notion of a physical perimeter has faded away. In this new world, security must reach far beyond the boundaries of the data center. Security must now follow a company's most important asset — its data — with a level of contextual awareness sufficient to protect that data everywhere it resides and however it's accessed.

To provide security that addresses the cloud, new security assumptions and capabilities must be in place. Security must

- Follow the data.
- Be based on a rich context.
- Adapt to the specific characteristics of a worker's context.

The other key consideration a SASE model solves for is the balance of security and network performance. We can't trade one for the other — we need both. People are most productive when their experience of technology is effortless and smooth. When security tools slow down networks, performance degrades and productivity suffers. Or, even worse, workers try to bypass security controls altogether, which creates tremendous risk and exposure.

The crucial step toward achieving that balance is for an enterprise to move its essential networking and security capabilities to the cloud while eliminating perimeter-based appliances and (get ready for pushback) all legacy products.

Such an approach will provide safe and reliable access to web services, applications, and data, with Zero Trust principles applied throughout to achieve continuous adaptive trust during every interaction.

SSE: Guiding the Security Needs of the SASE Journey

SASE and SSE are how security moves to the cloud and becomes more effective than anything we've had before.

SASE is an overall vision for transitioning networking and security capabilities to the cloud. SSE is the brain that integrates, identifies, and executes a specific set of security services needed to achieve SASE. The set of integrated services becomes the primary inspection point where consistent security inspection and control are applied to all traffic. SSE doesn't replace the firewall — you'll still have one — but it does supplant the firewall's position as your central security feature.

There is certainly value, individually, from CASB, SWG, ZTNA, and other related services. Most companies have deployed one or two of these already. However, to harness the full value of the cloud, these services must be integrated and work together.

Netskope believes essential SSE functions can be augmented with many capabilities currently missing from enterprise security but crucial for reliably securing digital assets beyond the confines of the data center. These include

- **Classification:** Identifies and labels sensitive information, ideally when it's created but also through periodic scans of data stores
- **DLP:** Actively monitors and controls the movement of sensitive information
- **Threat awareness and neutralization (also known as advanced threat protection [ATP]):** Identifies indications that an environment has been compromised and performs actions to reduce or eliminate the likelihood of future attack
- **Cloud security posture management (CSPM):** Evaluates the configuration of infrastructure and platform clouds and takes steps to remediate misconfigurations that could result in compromise
- **SaaS security posture management (SSPM):** Evaluates the configuration of SaaS applications and eliminates

misconfigurations that might allow exfiltration, impersonation, or other kinds of attack

- **Digital experience management (DEM):** Analyzes data collected for security purposes along with other availability and performance signals to measure worker experience and help quickly resolve problems

REMEMBER

By combining all these capabilities as a single, integrated security product deployed in the cloud where it's nearest to people, data, and applications, SSE becomes the most important inspection point protecting your enterprise. (We look at SSE in detail in Chapter 3.)

We Need Security for Tomorrow, Not Yesterday

We must deploy tools that support the cloud, the key factor in creating business value and revenue. We must deploy tools that resist disruption by adversaries. Finally, we must deploy tools that don't impede operations. Compare the concept to sending an invisible bodyguard with your child to daycare, school, and college. That portable bodyguard is SSE.

IN THIS CHAPTER

- Understanding the need for SSE
- Exploring SSE's capabilities and requirements
- Assessing the benefits of SSE

Chapter 3
Security Service Edge: A Plan for the Future of Cloud-Based Security

Secure Access Service Edge (SASE) changes our perspective of how security is delivered in a cloud-based world where data can be accessed from anywhere. When workers are remote, when applications become software as a service (SaaS), and when data moves throughout the cloud, an organization's cybersecurity efforts also must move throughout the cloud. Properly implemented, SASE shows us that security must be as close as possible to where data resides and is accessed. In SASE, security will protect an organization's interests and provide consistent controls no matter how distant those interests are, without degrading network connectivity and the user experience.

Part of achieving SASE is security consolidation and integration — the very essence of Security Service Edge (SSE).

SSE relocates critical control and inspection points to the cloud(s) where your business runs. That shift places security adjacent to where data, applications, and people operate — and where the danger is. With SSE, inspection and control services for SaaS,

web, and data — plus, sophisticated threat awareness and neutralization — work as a single, coherent, interoperable system.


TIP

You don't have a network problem. You have a cloud security problem. The only necessary network conversation is one about embracing an architecture that makes SSE the primary inspection point in the cloud.

SSE provides capabilities that transcend what traditional firewalls can do. Properly implemented, SSE also discerns context — the details of what, how, and why data is accessed — enabling it to make nuanced security decisions in real time. SSE connects all your security "senses" into a single brain that interprets the data, comprehends the breadth of risks presented, and negotiates the right level of access at any given moment, in any scenario.

In this chapter, we look at how SSE works.

Exploring Why We Need SSE

The old approach to security was based on establishing a perimeter and deploying a firewall to attempt to repel attackers targeting your corporate data center. But because no security is unbreakable, an attacker who successfully breached the perimeter was free to move laterally throughout your network, rendering your data and applications effectively defenseless.

SASE architectures still rely on identity and access management to authenticate the worker and on endpoint protection platforms to safeguard devices. But effective SASE also implements Zero Trust principles that grant access and monitor confidence based on a comprehensive set of conditions. In the cloud, the context surrounding the person becomes the perimeter.

Zero Trust is a philosophy based on three propositions that are fundamental to SSE and, therefore, to SASE:

- **The implicit trust present in legacy designs has outlived its usefulness.** Zero Trust inverts "trust, but verify" to "verify, *then* trust." Every person or action that requests access to data must have its identity and context verified every time to arrive at a certain confidence level. No exceptions.

- **Provide only minimum access (also known as *least privilege*) appropriate for the determined confidence level.** Access is limited to a specific resource and is nontransferable to other resources.
- **Context must be constantly reassessed based on signals such as worker identity, device identity, device security posture, time of day, geolocation, business role, and the sensitivity of the data.** Every signal change must trigger a fresh reevaluation. (Netskope calls this *continuous adaptive trust,* and we cover it more deeply in Chapter 4.)

SASE provides a framework for an effective Zero Trust program fully encompassing environments in which people, applications, and data are anywhere. But, as we discuss in Chapter 4, Zero Trust is a set of principles, not a technical architecture for how to implement different security functions in a unified way.

SSE provides that technical architecture. SSE unifies, integrates, and coordinates many security services, improves security's capabilities, and provides high performance for workers and business needs in an integrated, customized way based on context. To deliver the desired outcomes, SSE supplies the following:

- Detailed context, including worker history, device, requested data, application, network, and even the reason for the request
- Information about the resources the person is permitted to access to satisfy the request, which SSE can glean from authorization and entitlement details
- Granular detail that classifies the sensitivity of different data resources (to prevent data loss)
- Guidance and a detailed set of policies describing the desired security outcome based on various combinations of people, data, applications, and other contextual information

The difficulty is that many of the security outcomes, such as data loss prevention (DLP) and threat awareness and neutralization, require multiple security components to work together.

WARNING

Implementing each service independently requires repeating a fair amount of security work in the consoles of one tool after another. That's cumbersome and error-prone when a sale — or a life — is on the line.

SSE eliminates repetition. When properly implemented, it combines those services and enables them to share context, entitlements, security policies, risk intelligence, browser isolation, data encryption/decryption, and more. That cohesion empowers security services to process transactions in a single pass to deliver the proper access quickly.

Discovering How SSE Brings Security Services Together

SSE is predicated on integrating many security services supported by numerous related capabilities. There's a right way to build SSE . . . and there are plenty of wrong ways.

WARNING

As the term *SSE* gains popularity, deceptive marketing will soon follow. Improperly built SSE is easily recognized by its lack of integration. Approaches that just link discrete processes or update old appliance daisy chains are evidence of systems assembled from separate components, built in pre-cloud legacy styles, and possibly acquired from multiple vendors. These stitched-together systems introduce significant latency, won't deliver the broad benefits of SSE, and are not meaningful steps on your overall SASE journey.

SSE is never a daisy chain of appliances or a sequence of discrete processes where data might pass through a DLP engine, then an access control list evaluator, then a web gateway, and so on. Nevertheless, it's helpful to tear apart the characteristics that describe a fully integrated SSE.

Single-pass, staged analysis

REMEMBER

In an ideal SSE, integrated security services operate in parallel. All inspections occur simultaneously, in real time, regardless of whether the traffic is from the web, the cloud, or your data center.

A typical single pass provides increasingly fine-grained traffic filtering to secure data and applications. Start by picturing traffic flowing through a funnel.

Proper SSE differentiates between corporate applications (for example, Salesforce or Workday), personal applications (such as an individual's Gmail account), and third-party applications or services (such as company instances of Microsoft Office 365 or Dropbox). It uses that awareness to initiate the appropriate connections necessary to protect each application or service in accordance with policy.

Proper SSE assesses context, adjusting access based on, for example, whether a doctor (see Chapter 4) is using a hospital-owned tablet in a patient's room, their phone on the coffee shop's Wi-Fi, or the gaming computer in their kid's bedroom.

Proper SSE imposes policies to prevent data from being lost or leaked. Controls can prevent downloading documents, taking screenshots, entering data into web forms, or posting to social media.

Proper SSE offers continuous monitoring. As the worker conducts normal activities, SSE is watching for anomalies. When data objects are classified, SSE can differentiate between sensitive and nonsensitive content, dynamically altering access permissions and allowed activities. SSE might trigger an alert, issue advisories, or query the worker for more information to guide their activity safely.

Powered by shared services

All high-level security functions, including DLP, threat awareness and neutralization, digital experience management (DEM), and others, can tap any or all of the services and techniques that we describe here to achieve desired security outcomes:

- **Shared context:** All SSE elements share a massive collection of metadata that identifies the person, device, and location. The destination website, application, or service is identified and given a risk assessment, and its activities are assessed. Any data requested or created by the worker and the application is considered. Rich SSE context includes an evaluation of worker behavior, even referencing past interactions to analyze current activity. This constantly updated contextual landscape informs the actions taken and policies enforced by all SSE elements. (In Netskope's SSE, this service is called Cloud XD.)

- **Continuous adaptive trust:** Access to data and applications is not a simple, binary decision. Access must be flexible based on changing requirements and contexts. Proper SSE aligns the amount of trust with the value of the assets being accessed, guided by the vast wealth of contextual signals available and the organization's appetite for risk as dictated by policy.
- **Policy-based administration:** As part of single-pass security, proper SSE features a detailed, shared policy framework that enables the organization to establish the boundaries of its risk tolerance and clearly define expected security outcomes. This represents a significant departure from the thousands of rules that typically populate firewalls. The components of SSE consult the policy framework to control activities and data across all applications, application categories, and web services.

SSE: Main Attractions

Now that we've described the underlying components of SSE, we can examine the capabilities SSE delivers. Some will be familiar things that your organization has already deployed in another form, so it's likely that SSE will replace them over time.

REMEMBER

SSE aims to enable people and your business to work as quickly and securely as possible. By functioning everywhere, SSE ends futile efforts to stretch security in your data center to follow data, applications, and people that have moved to the cloud.

Table 3-1 shows the minimum requirements for capabilities for a product to be accurately described as SSE according to various analysts in 2021.

TABLE 3-1 Minimum Requirements for SSE Capabilities

Capability	What It Does	How SSE Makes It Better
Secure web gateway (SWG)	Controls access and defends against web threats only.	Addresses cloud-enabled threats and data risks for personal instances of managed applications, thousands of shadow IT applications, and cloud services.
Cloud access security broker (CASB)	Serves as a security policy enforcement point placed between cloud service consumers and cloud service providers to enforce enterprise security policies as cloud-based resources are accessed. Evaluates behavior and has awareness of SaaS application functionality to set appropriate access for a given person.	Eliminates policy duplication (between SWG and CASB), simplifies administration (single agent for SWG, CASB, and ZTNA), and provides visibility into all lanes of traffic.
Zero Trust network access (ZTNA)	Enforces the premise that no one is blindly trusted and allowed to access company assets until they've been validated as legitimate and authorized. Supports implementation of least privilege access, which selectively grants access only to resources that people or groups of people require, nothing more.	Boosts ZTNA by giving it adaptive access capability. Harmonizes policy administration and decision with other SSE components while still maintaining distributed policy enforcement.
Remote browser isolation (RBI)	Separates worker devices from the act of web browsing by hosting and running all browsing activity in a remote, cloud-based container. Such sandboxing protects data, devices, and networks from all kinds of threats originating from malicious websites.	Enables RBI to leverage data classification and roles context. Adds isolation to the array of policy actions in SWG and CASB.

(continued)

TABLE 3-1 *(continued)*

Capability	What It Does	How SSE Makes It Better
Firewall as a service (FWaaS)	Provides network security for all outbound ports and protocols for safe, direct-to-Internet access via an agent on managed devices or via Generic Routing Encapsulation (GRE) and Internet Protocol Security (IPsec) for offices. One policy engine and one security platform, providing simplified management for workers and branch offices using one console.	Enables organizations to aggregate traffic from multiple sources — whether from on-site data centers, branch offices, mobile workers, or cloud infrastructure. Provides consistent application and security enforcement of policies across all locations and workers while giving complete network visibility and control without deploying physical appliances.

SSE Capabilities: Coming Soon to Your Security Team

SSE will evolve greater capabilities as products mature and cloud-first initiatives proliferate. Proper SSE architecture embraces much more than the original baseline definition, such as:

- Enhanced classification to support DLP
- Security posture management for cloud and SaaS
- Threat awareness and neutralization
- DEM

We cover each of these in the following sections.

Enhanced classification to support DLP

DLP is a catchall name for a feature meant to prevent intentional and accidental data exfiltration by intentional and unintentional misuse. DLP detects the movement of sensitive information, prevents it from spreading to unwanted locations, interrupts workers with educational pop-ups to stop unintentional exposure, and incorporates machine learning to assess worker risk scores.

TIP

SSE improves DLP by actively identifying and classifying data, making it possible to track and enforce rules regarding movement of sensitive data more accurately.

Security posture management for cloud and SaaS

Cloud security posture management (CSPM) and SaaS security posture management (SSPM) discover and remediate misconfigurations across clouds (the most common form of cloud security failure). Utilizing the context provided by SSE, application programming interface (API)–enabled controls, and real-time assessment of public cloud deployments, CSPM and SSPM mitigate risk by analyzing configuration, by suggesting changes that reduce or even eliminate the likelihood of potential attack, and by monitoring for regulatory compliance.

TIP

CSPM and SSPM in proper SSE implementations recognize threats and actively take steps to increase an organization's security posture.

For example, some CSPM and SSPM implementations can identify noncompliance when an organization's policy requires encrypting all data in the cloud by default. This is a very strong stance to take because it mandates access controls that must agree: A person's identity must be present on the access control list for an encrypted object and on the list for its associated encryption key. CSPM and SSPM recognize when a person has access to one but not the other and flags the inconsistency.

Threat awareness and neutralization

Threat awareness and neutralization discovers evidence of successful attacks and raises alarms so the danger can be contained. Typical evidence includes unusual network activity, changes in configuration, and deletion of log files. Forensic analysis determines whether an active threat is in the environment. Threat neutralization is a perfect example of a service that derives benefit from and contributes evidence to the shared capabilities of the SSE architecture.

Digital experience management

One emerging and powerful aspect of SSE is its ability to gauge worker experience and application performance, especially because the network boundary now extends to the cloud and beyond. By providing continous monitoring of all traffic, customers benefit from end-to-end visibility into their network and application behavior with real-time, actionable insights based on real human activity to ensure SSE delivers without performance trade-offs. When device, network, or application issues arise, DEM can help identify the root causes quickly, accelerate resolution of help-desk tickets, and provide proactive steps to prevent small issues from becoming major, business-impacting events.

Networking Must Evolve, Too

Up to this point, we've focused on the security features and capabilities SSE provides for a cloud-first world. But more transformation is required beyond what we think of as security.

REMEMBER

Network access must be distributed to enable workers and organizations to extract full value from the cloud-based systems SSE is protecting, as shown in Figure 3-1.

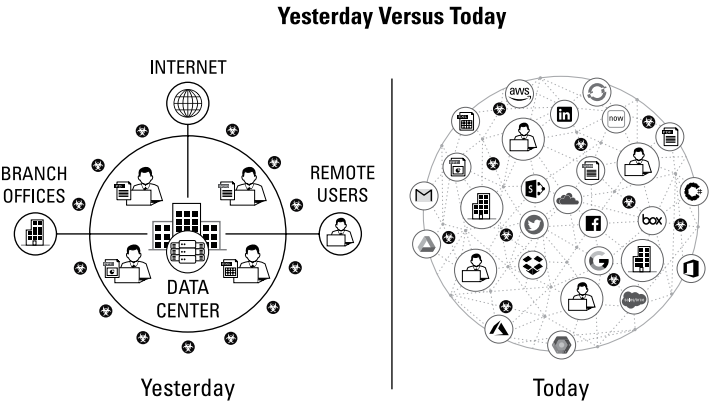

FIGURE 3-1: The old access model was inefficient and ineffective compared to the new model, which enables access from anywhere.

In the old access model, workers connected to a network protected by a well-defined perimeter. Branch offices maintained expensive private network connections to the data center. This became a hurdle as business operations flourished, first on the web and later in the cloud. The only safe option was to detour worker traffic through the data center's security stack before interacting with cloud and web resources.

The approach is inefficient and ineffective. Allowing workers to directly interact with cloud resources greatly improves performance and productivity but subverts the data center's visibility and control. Persisting the old model by building, maintaining, and monitoring private networks to reach all that the cloud can offer is complicated and expensive and simply doesn't scale in an era where security must be a top priority at every business level, including the boardroom.

The new network model envisions an architecture built for remote work, where people connect from anywhere and interact with other people and information mostly in the cloud. For best performance and application experience, an SSE provider's network must

- Peer with numerous connections to the destinations that matter most
- Consist of a sufficient number of points of presence equipped with full compute resources and strategically distributed such that workers are never far away

TIP

The way to achieve quick, effortless connections is to work with a provider whose network is highly peered with numerous direct connections to the destinations that matter most. The more connections your provider offers, the better the performance, the stronger its resilience, and the happier users will be.

REMEMBER

A well-connected provider offers better performance, stronger resilience, and delightful experiences. Worker experience matters! Digital transformation succeeds when security and networking merge into a cohesive partnership from day one. Security that degrades network performance — or that forces a dangerous trade-off between safety and productivity — won't do.

Like all aspects of SASE and SSE, network transformation is optimized over time. Your cloud security vendor must straddle the divide between the security you have now and where you want to be in the future. It must provide SSE, deliver new on-ramps for your distributed workforce, and integrate gracefully with existing network infrastructure and processes.

The SSE Security Payoff

By adopting a SASE architecture with Zero Trust principles at its core and partnering with an SSE vendor capable of delivering critical, distributed security services, an organization can anticipate significant benefits:

- Increased confidence when granting access to data and applications outside the data center
- Flexible security based on risk insights with adaptive policies and control over specific activities tailored to each application
- The ability to extend Zero Trust principles beyond private applications to cover web and SaaS applications
- Access to additional security services such as RBI and advanced DLP based on the assessed level of risk or trust
- Continuous monitoring for changes in context that automatically trigger a reassessment of trust and access
- A reduction of the attack surface by eliminating exposure of protocols and services to the public Internet
- Correctly configured clouds that eliminate the most common form of cloud security failure

All these benefits represent aspects of the security nirvana we mention in Chapter 1. Chapter 4 looks at the business payoff of proper SSE and the steps for bringing it to life.

IN THIS CHAPTER

- Achieving a state of continuous adaptive trust using Zero Trust principles
- Looking at the four steps to adopt SSE
- Discovering the business benefits of SSE

Chapter 4
Using Zero Trust to Bring SASE to Life

As we discuss in Chapter 2, moving security to the cloud matters now because the cloud fundamentally matters to business. Cloud adoption is brisk — faster than even forward-thinking organizations predicted just five years ago. Businesses are moving to the cloud to achieve rapid development, access to on-demand resources, elastic scaling, and a much lower administrative burden so they can innovate and build new products and services in record time.

Attackers are moving to the cloud because, well, businesses are. So, we all must care about how to ensure that our data, our applications, and our people are safe in the cloud.

WARNING

If the cloud isn't protected, then its benefits remain elusive.

Those leading the charge must make the case, first, that protecting the cloud is important and, second, that Secure Access Service Edge (SASE), Security Service Edge (SSE), and retooling the network will yield better risk management and reduce security friction. Plans for adoption should explain why this change is worth the trouble, predict the specific business benefits, and outline how to measure those benefits along the way.

Building on our discussions of security transformation, SASE, and SSE, this chapter describes the path to the security nirvana we all want, one in which our data, applications, and people are safe in the cloud and creating substantial and unmistakable business value. That path now inexorably includes the application of Zero Trust principles to how we architect our security.

From Zero Trust to Continuous Adaptive Trust

A successful implementation of SASE and SSE is more than swapping out technology. As we explain in Chapter 3, Zero Trust revamps some basic assumptions about how security works. In the on-premises, network-based model, the assumption is that the network is secure and you must verify a person's identity before granting access. The typical paradigm granted the user access to everything or nothing — "allow" or "block" were the only choices. Zero Trust changes this model as follows:

- **When a person requests access, that request is evaluated in the context of several conditions.** Identity is one of them, but the system also considers where the person is, the time of day, the device, the type of network connection, and many other variables.
- **The application to which the person is being connected is part of that context.**
- **The desired service level is an important factor.** Is this a life-or-death use of an application or a video game played for fun?
- **How the network path is protected may change based on the application being used.** If someone is accessing their personal email account, an ordinary Internet connection is used, with Transport Layer Security (TLS) protection negotiated between their email server and email client. If a doctor is accessing patient records, a secure, encrypted, and authenticated path is established, regardless of the capabilities of the underlying network or application.

Based on this context, the confidence level of a person's session is determined, and the person may be trusted a little or a lot. A person requesting access at an unusual time from an unusual location to a highly sensitive application (an instance of a low confidence level) likely will encounter a multistep authentication process. The access granted may be limited to a small set of data and functions and then in a read-only mode. A worker who is accessing at their customary time from a secure location (an instance of a high confidence level) may get full access to all data and application capabilities.

Consider this example of a doctor accessing electronic health records that illustrates Zero Trust principles at work in SSE:

> A doctor is carrying a hospital-owned tablet as they treat a patient in the hospital. Based on the doctor's identity, location, device, and other factors, the SSE determines it is safe to give the doctor full access to the patient's records.
>
> The doctor heads across the street for a cup of coffee. They pop open a personal laptop, connect to the shop's network, and try to access patient records. The SSE recognizes the doctor but identifies that the hospital does not own the laptop and that the laptop is on an unknown network. The doctor is allowed to view and comment on the records but can't alter the data.
>
> The doctor is eating dinner at home; alerted to a crisis, they log their child out of Minecraft to use the family PC to access the patient's records. The SSE recognizes that this computer is less secure than the hospital's tablet. Instead of denying access, the SSE provides a series of prompts that enable the doctor to verify their identity further and frame the nature of the reason they need access. The SSE then provides the doctor with a secure set of resources to respond to the emergency — for example, inside an isolated browser session under control of the SSE.

You might be familiar with the term *Zero Trust network access* (ZTNA). ZTNA is an excellent choice for augmenting your virtual private network (VPN) to accommodate more remote access scenarios. With ZTNA, workers don't receive access to an entire portion of a network that could allow connections to many services. Instead, ZTNA grants the worker a connection only to the application they're seeking to use and — as shown in our doctor story — only the minimum access needed to perform the task at hand.

If we take a closer look at this model and how it functions in the most advanced form, some important ideas emerge that can guide our efforts:

- **Context:** In pre-SASE security, the network defined the perimeter, a barrier you had to cross to gain access. A certain line of thinking suggests identity is the new perimeter in Zero Trust because your identity must be validated to allow access, but that concept is insufficient. A better approach is to evaluate the whole context, including identity but also many other variables, to determine what kind of access is permissible.
- **Least privilege:** Zero Trust always tries to grant only the minimum access needed to allow the person to get the job done. The most advanced form of Zero Trust also tries to constantly discover if too much privilege has been granted and strives to squeeze that excess trust out of the system.
- **Risk scoring:** SSE constructs a history of activities when workers interact with applications. It's possible to analyze that history to construct a representation of normal activity and to detect suspicious activity in real time. This analysis generates risk scores for a worker, for an application, and for a website. These scores provide additional context to determine what type of access to grant.
- **Resource concealment:** ZTNA-based access doesn't expose public IP addresses that anyone can connect to. Connectivity is possible only after the context has been evaluated. By default, everything is hidden. (Yes, there's a role for obscurity in security, contrary to what's often taught in infosec classes.)
- **Continuous adaptive trust (probably the biggest idea on this list):** Continuous adaptive trust is the practice of monitoring a connection and constantly adjusting the permissions based on changes in context. Is a person who normally used Salesforce trying to access the CFO's treasury system? Red flag: Reduce access and authorization, boost the risk score, and alert someone to take action. Is another person trying to access a dangerous website? Display a window with a warning before granting access. The goal is to constantly react to changes in context to properly protect the data, the applications, and the people.

REMEMBER

Implementing SSE with Zero Trust principles shrinks the attack surface and is far more data-driven, thus greatly improving the overall security posture. As the level of risk presented by a person, an application, or a website is constantly being reevaluated, security is adapting in real time based on changes in context.

Now, with our continuous adaptive trust mindset firmly in place, we can move to a discussion of how to implement SSE the right way.

Four Simple Steps to SSE

Bringing SSE to life for most organizations entails moving from on-premises-based security with the network as the perimeter to cloud-based security with context as the perimeter. We're going to assume a starting point that reflects where most companies are right now — an on-premises firewall that includes VPNs for remote access, an on-premises secure web gateway (SWG) appliance that controls web access, and perhaps a subscription to a stand-alone cloud access security broker (CASB) that protects use of software-as-a-service (SaaS) applications.

Step 1: Migrate mobile workers to regain visibility

The first thing to do is assess what your workers are doing and measure your current level of risk. The easiest way to accomplish this is to begin with your mobile user population, because these workers present potentially more risk. Direct their web and SaaS traffic through the SWG and CASB capabilities of SSE, configured as closely as possible to existing policies. Then watch.

This exercise generates a more complete picture of what workers are doing. Companies not already using CASB or SWG will discover an enormous (and potentially alarming) amount of activity. Companies that are already using CASB and SWG will learn more as well.

You'll most certainly find that mobile workers are accessing applications and services you weren't aware of. You'll learn where they're working and what sort of networks they tend to use.

The remaining part of Step 1 is to migrate access to internal systems in the data center from VPNs to the ZTNA in the SSE. This improves the worker experience and increases security at the same time. Imagine a plumber comes to your house to fix a leak while you're at work. They have access to your entire property on their way back and forth between their truck and your bathroom. Maybe they leave the front door open. All the while, you have no idea what's going on. ZTNA is like arming yourself with a magic teleportation button. The plumber shows up, you beam them from their truck to the leak and back with no stops in between. It's access control, perfected for the era of cloud.

Step 2: Migrate remaining workers and apply company-wide data classification

The second step is to move all your on-premises workers under the protection of SSE to control access to cloud-based applications and services. Taking this step so that all workers, both on-premises and mobile, are protected by SSE transforms your network architecture. All workers now traverse the SSE provider's closest point of presence, which then routes traffic to the destination in an optimal fashion — often with fewer hops than the public Internet. Now you can simplify the network and retire expensive private networks that may no longer be needed. As part of this network transition, software-defined wide-area networking (SD-WAN) may be introduced to selectively steer traffic from branch offices.

The goal is to gain a complete understanding of the data, applications, websites, and other services of interest to our workers. In this stage, the power of SSE to capture and analyze activity dramatically increases the scope and depth of the context. The security posture expressed by your SSE policies in this step should probably be similar to those already present in whatever legacy products the SSE is replacing. It's important to match a known state before you add new capabilities that may require education and training.

With this new context in hand, you can lay the foundation for better security by classifying data, applications, and people based on risk and behavior. With such classification completed, the SSE system can use internal and external data to compute real-time risk scores for workers, applications, and websites. It's now

possible to retire much of the legacy security infrastructure and move to the next stage where SSE moves to a new level of security.

Step 3: Implement continuous adaptive trust and expanded services

Up to this point, the experience workers encounter hasn't much changed. In Step 3, the experience changes significantly because security adapts based on context.

REMEMBER

Continuous adaptive trust evaluates context to balance risk against trust, providing the correct type of access at any given moment in time. It allows you to define far more detailed security policies. In addition, it more frequently raises warnings or suggestions when people are about to do something dangerous, helping to guide workers toward approved actions.

With SSE, security professionals know which data is sensitive and which applications and websites are risky. Combining this sense with capabilities like data loss prevention (DLP) allows security staff to control what people do with sensitive data in a fine-grained fashion — at a level unprecedented in security. Instead of a simple block-or-allow decision, access falls somewhere on a continuum.

Continuous adaptive trust also enables you to add more services. For example, let's say a doctor wants to visit a website that's considered risky. After a warning, the doctor still wants to go there. The SSE could then shunt the doctor into a remote browser isolation (RBI) session, a browser that runs on a virtual machine at the SSE provider, which further reduces the risk. Other advanced services can be added as needed.

Step 4: Proactively manage risk with dynamic analysis and scoring

In Step 4, the team operating the SSE can start the process of proactively finding risk and squeezing it out of the environment. One method to measure progress is by tracking the risk scores of workers, applications, and websites. The goal is to show a reduction in the amount of traffic to risky sites and in the frequency of risky actions. Another method is to reduce entitlements by tracking usage patterns and eliminating excess privilege.

At this point, some of the higher-level security controls such as DLP and threat neutralization can become the focus, augmenting the capabilities of CASB, SWG, ZTNA, and firewall as a service (FWaaS). In SSE, these controls work better than they did in their separate on-premises incarnations and much more can be done with them. For example, machine learning–based recognizers enable DLP to identify and react to sensitive documents in real time.


TIP

Digital experience management (DEM), cloud security posture management (CSPM), and SaaS security posture management (SSPM) further improve risk management. They add advanced methods to ensure consistent availability and performance and to find and fix configuration errors. SSE will allow even more such advanced services in the future.


REMEMBER

Your unique situation dictates the particulars as you work through the steps. But from a high level, the steps explain the process that most companies will go through to fully implement SSE.

Transforming the Network and the Rest of Security


TIP

Implementing SSE is an important step forward, and it's nonnegotiable for SASE. But to reach the security nirvana we're shooting for, the rest of the security landscape beyond SASE must also evolve so that all the important parts work together. Most businesses are shifting to a work-from-anywhere model in which the benefits of anywhere, anytime security are clear. This naturally shifts away from VPN and private networking-based connectivity and delivers the simplicity and cost advantages of SSE.

The larger point to keep in mind is how, by adopting SSE (and SASE), the overall technology infrastructure becomes simpler. In the old model, security controls to guard against unauthorized access were put into the corporate network because that network was the only path to the data. In the new model, the SSE provider's various points of presence become the paths to the data, offering not only access control but also full traffic inspection. The underlying network can then focus its overall mission to quickly and efficiently move bits around.

Identity and access management (IAM) systems perform the important job of authenticating workers. Many of these systems already are highly configurable through application programming interfaces (APIs). They're also designed to integrate with other systems, a necessary feature for any SSE implementation. IAM technology improvements provide even more context, monitoring, and advanced authentication capabilities that SASE and SSE can benefit from. SSE derives yet more benefit from endpoint protection platforms (EPPs). They collect important signals (thus, generating more context), perform detailed monitoring, and include mechanisms to control behavior and security configuration. Synchronize your SSE implementation plan with a corresponding EPP evolution so you get maximum value out of your security investments.

SASE and SSE will accelerate the change in the role of the data center. After the cloud rose to prominence, the data center lost its position as the focus of security-related activity. SSE moves security out of the data center and into the cloud.

REMEMBER

Data centers will still play an important role in most companies for a variety of good reasons such as cost pressures, regulatory requirements, risk management, and utility of special types of computing infrastructure. The data center will now be one of many locations where important applications are housed and protected by SSE.

SSE Business Benefits

Cyber risk is a priority for most boards of directors, but as we make clear in Chapter 2, security is not an end in itself. It has a mission to protect the business value being created by the systems that support the business. Companies moved to the cloud because it makes business sense. The job of a SASE architecture, including SSE, is to protect applications, data, and people. Here's how this translates to business value:

- **Security no longer gets in the way of business productivity.** Business agility can be supported and security teams no longer have to play the role of Dr. No, because the moves the business wants to make can now be properly secured. Security-induced friction is reduced dramatically. Product

development and maintenance processes become streamlined as security is more easily incorporated. A cloud-based SSE is perfectly suited to securing a multi-cloud environment.

- **The board of directors has much more confidence now that the types of control required to safely use cloud resources are being properly scrutinized and managed.** The process for managing risk related to people, data, and applications becomes vastly more sophisticated, as do the mechanisms used to mitigate risk. With SSE, risk can be proactively identified and systematically squeezed out of a company. In a real sense, security follows the data, which provides a sense of peace to the board about how well the most important assets are protected.
- **The security team becomes far more unified and business focused.** Instead of having a SWG person, a CASB person, and a firewall person, you have a team focused on the bigger picture with more insights to be proactive.

REMEMBER

Bringing SSE to life means bringing a much better world of security to life, and everyone involved in the business will find a benefit.

Chapter 5
Ten (or So) Do's and Don'ts for Your Journey to SSE

A big part of completing the journey to a secure and agile cloud is recognizing that your current IT organization wasn't designed for such a destination. It's natural that the IT organization reflects the technology architecture. So, if distinct individuals or teams tend your cloud access security brokers (CASBs), your secure web gateways (SWGs), your virtual private networks (VPNs), and your firewalls, along with or as part of a security operations center (SOC) team and a network operations center (NOC) team, you'll face pushback when you say, "Hey, let's now implement a new Secure Access Service Edge (SASE) and Security Service Edge (SSE) integrated architecture that also converges security and networking into one mighty brigade." People naturally resist change, partly for fear of losing control of a domain they've worked hard to master.

SASE and SSE offer tactical benefits that improve the quality of security and expand the reach of security services and strategic benefits that can accelerate business. The following sections provide a guide to succeeding with SASE and SSE adoption. First, we present four principles to accelerate your journey. Then we suggest four mistakes to avoid.

Make Data the Focus

Under SSE, security follows the data wherever it goes. So, it doesn't matter if you're creating data in Google Workspace and Microsoft 365, in a software-as-a-service (SaaS) application or on cloud object storage. SSE is always there to protect that data.

Because SSE becomes a primary inspection point that can also facilitate data classification, it's important to determine the purpose and location of all your data. Use this knowledge to prioritize the protection and proper use of sensitive data wherever it is, so you can be confident that you've done the most important job first.

Embrace Integration

At every step of the incident response cycle, building automation and integration skills is important so you can converge your security components into a finely tuned machine. The process involves extracting information from multiple systems, integrating that information to analyze what's going on, assembling the right team, and taking automated actions when possible.

SSE integrates the crucial security services for protecting the cloud, but it lives as part of a larger ecosystem of important security services. Identity and access management (IAM) systems, endpoint protection platforms (EPPs), and security information and event management (SIEM) tools are some of the key components that work together with SSE-specific functions to provide comprehensive security and to support the rapid diagnosis of and response to problems.

Remember Bad Guys Are in the Cloud, Too

SSE and SASE represent a large leap forward in the scope and quality of security. It's reasonable to feel satisfied after you get the fundamentals working. But remember, attackers have used the cloud to raise their game as well. The percentage of malware delivered via cloud applications rose from 50 percent in Q2 of 2020 to an all-time high of 68 percent in Q2 of 2021, according to Netskope's Cloud and Threat Report (`www.netskope.com/blog/`

july-2021-netskope-cloud-and-threat-report). SSE propels you ahead of the bad guys, but you must constantly learn and adapt to remain ahead.

Acknowledge That Security Is a Key Part of Business Strategy

Security must be part of a discussion of business strategy from the beginning. Getting excited about applications and the cloud makes no sense if those applications and the people working with them can't be secured. The good news is that SSE will help security teams more easily become a business enabler. If the security team understands the business goals and their security ramifications, the team can say "yes" more often because they have more power to protect anything the business wants to do.


TIP

For a SASE and SSE adoption to be successful, the program's promoters must explain that the benefits of securing the cloud are important at the grand strategy level. The message: We've invested in the cloud to transform our business and create better outcomes. Now, we must protect that investment. The excitement about achieving and protecting these outcomes will be the best motivation to enthusiastically adopt SASE and SSE.

Don't Think in Silos

SASE and SSE solve the thorny problems that tend to accompany cloud projects. Avoid attempts to implement CASB, SWG, and Zero Trust network access (ZTNA) as independent projects, which adds more niche vendors promising more distracting bells and whistles. The goal is to protect the cloud with a context-aware integrated platform. There will be resistance to the change that SASE and SSE entail.


WARNING

One huge mistake is to slow down the process by approaching the problem from conventional IT silos. These "cylinders of excellence" perpetuate old ways of thinking in the new world. Security should no longer be categorized as merely a network issue. Don't have a network conversation about a security problem. SSE has become the critical security visibility and control point as part of a fully functional SASE architecture.

Don’t Port Over Old Rules

People are often scared of their firewalls because they’ve accreted layers of rules created by people who departed long ago. The same can be true of other security technologies that require complex rules and configuration settings to achieve desired outcomes. SSE is different. Although rules and configuration still exist, much of the work is accomplished by defining policies that describe outcomes. When implemented effectively, SSE manages the details of rule interactions on its own. So, don’t worry about the configuration of your old technology. Instead focus on your desired security outcomes and use SSE to achieve them.

REMEMBER

Most SSE products also offer cloud security posture management and SaaS security posture management to help you get it right and keep it going well.

Don’t Hate the Data Center

Now that you’re embracing SASE and SSE, it’s easy to think the traditional data center is not important. We’ll always have data centers in some form; after all, the cloud is nothing but a collection of data centers with access through application programming interfaces (APIs). The data center’s new purpose is a place for important computing workloads and applications. The data center is no longer the leading role in the security infrastructure, but it still plays an important supporting part.

Don’t Be Afraid of Change

Don’t let fear of SASE and SSE slow you down. Yes, there is a change in architecture and new products to master, a tough task because the products interact with everyone in the company. An SSE implementation will teach you more about your people, your data, your applications, and your third-party sites and applications. This knowledge, then, will open the door to more automation to find errors and implement effective responses. Compared to your current security posture, living in the new world will feel like nirvana.

SSE is the security stack that will determine a successful SASE architecture. This book shows you how to achieve SSE today.

The SASE journey requires reliable partners with truly integrated platform capabilities, not vendors wielding smoke-and-mirrors-style marketing proclaiming "SASE" or "SSE" in giant headlines. This book is your practical guide to SSE and SASE, including why both concepts are so fundamental to building cloud-centric security and networking architectures of the future, and how to invest and design for Security Service Edge (SSE) today.

Inside...

- Define SASE and SSE
- Learn the critical role of Zero Trust
- Protect critical business data in the cloud
- Supercharge your work-from-anywhere workforce
- Avoid design pitfalls for SSE and SASE

Netskope leaders **Jason Clark** (CSO and CMO) and **Steve Riley** (Field CTO) are widely acknowledged authorities in cloud computing technology, cybersecurity, and networking, with decades of experience from global organizations including Gartner, Optiv, Riverbed, and Websense.

ISBN: 978-1-119-87700-4
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.