LEARNING MADE EASY

Palo Alto Networks 3rd Special Edition

Secure Access Service Edge (SASE)

for dummies®
A Wiley Brand

Simplify operations and enhance user experience

Ensure secure connectivity and app performance

Stop cyberattacks with consistent security

Brought to you by

paloalto® NETWORKS

Lawrence Miller

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security, and security operations. Powered by Precision AI, our technologies deliver precise threat detection and swift response, minimizing false positives and enhancing security effectiveness. Our platformization approach integrates diverse security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection. From defending network perimeters to safeguarding cloud environments and ensuring rapid incident response, Palo Alto Networks empowers businesses to achieve Zero Trust security and confidently embrace digital transformation in an ever-evolving threat landscape. This unwavering commitment to security and innovation makes us the cybersecurity partner of choice. For more information, visit www.paloaltonetworks.com.

Secure Access Service Edge (SASE)

Palo Alto Networks 3rd Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Secure Access Service Edge (SASE) For Dummies®, Palo Alto Networks 3rd Special Edition

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

ISBN 978-1-394-30199-7 (pbk); ISBN 978-1-394-30200-0 (ebk); ISBN 978-1-394-30201-7 (ebk)

Publisher's Acknowledgments

Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager: Cynthia Tweed

Production Editor: Umeshkumar Rajasekhar

Special Help: Amy Lupold Bair, Shannon Bonfiglio, Carmine Clementelli, Rajesh Kari, Ashraf Aziz, Charles Choe, Paul Kaspian, Andrew Huang

Table of Contents

Introduction

If you're like most people, the environment you work in today is very different than it was just a few years ago. The rapid shift to cloud, artificial intelligence (AI), and hybrid work, accelerated by the COVID-19 pandemic, represent two of the most dramatic changes the world has experienced in recent history. We've now entered an era in which work is no longer a place we go to but rather an activity we perform, and cloud applications are vital to performing that activity. However, although work habits and apps have completely transformed, network security solutions haven't fundamentally changed in more than 20 years.

The growing appetite for all things cloud and the distributed nature of modern applications have completely decentralized corporate networks. When you combine this trend with the increasing numbers of remote users, branch offices, data, and services located outside the traditional corporate network, organizations are struggling to ensure sufficient levels of security and connectivity.

Most network security solutions on the market today weren't designed to handle all the types of traffic and security threats that organizations must deal with now. This forces organizations to adopt multiple disparate products to handle different requirements, such as secure web gateways (SWGs), firewalls, virtual private network (VPN) remote access, Multiprotocol Label Switching (MPLS), and software-defined wide area networks (SD-WANs). For every product, there is an architecture to deploy, a set of policies to configure, an interface to manage, and a set of logs. This creates an administrative burden that introduces cost, complexity, and gaps in security posture.

To address these challenges, *secure access service edge* (SASE) has emerged. A SASE (pronounced "sassy") solution is designed to help organizations embrace cloud and hybrid work by providing network and network security services from a common cloud-delivered architecture.

However, not all SASE solutions are effective. To solve for the needs of today's rapidly evolving and dynamic businesses, a SASE solution must provide consistent and secure access to all types of applications — including public cloud, private cloud, software as

a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) — delivered through a common framework to users in business offices, home offices, and remote locations. By removing multiple point products and adopting a single cloud-delivered SASE solution, organizations can reduce complexity while saving significant technical, human, and financial resources.

In *Secure Access Service Edge (SASE) For Dummies,* I fill you in on this approach to networking and security, including its core capabilities and key benefits for organizations in the modern digital workplace.

About This Book

This book consists of seven chapters that explore the following:

- Modern trends and their impact on the evolution of networking architectures (Chapter 1)
- SASE use cases (Chapter 2)
- SASE networking capabilities (Chapter 3)
- SASE security capabilities (Chapter 4)
- The secure browser (Chapter 5)
- Digital experience monitoring (Chapter 6)
- Ten benefits of SASE (Chapter 7)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backward!).

Foolish Assumptions

It has been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless.

Mainly, I assume that you work in an organization that's looking for a better way to simplify your approach to networking and security. Perhaps you're an IT executive or manager such as a chief information officer (CIO), chief technology officer (CTO), or chief information security officer (CISO). Or perhaps you're a network or security architect or engineer.

As such, this book is written for technical readers with a general understanding of cloud, networking, and security concepts and technologies.

If any of these assumptions describes you, then this is the book for you. If none of these assumptions describes you, keep reading anyway — it's a great book, and you'll learn quite a bit about SASE.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:


REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!


TIP

Tips are appreciated, never expected, and I sure hope you'll appreciate these useful nuggets of information.


WARNING

These alerts point out the stuff your mother warned you about. Well, probably not, but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much I can cover in 80 short pages, so if you find yourself at the end of this book, thinking, "Gosh, this was an amazing book! Where can I learn more?" check out `www.paloaltonetworks.com/sase`.

IN THIS CHAPTER

- Considering the move to hybrid work
- Understanding the role of the cloud in digital transformation strategies
- Evolving the network architecture
- Discovering a new approach to enterprise networking and security

Chapter 1
The Evolution of Networking

In this chapter, you learn how cloud and hybrid work trends have changed enterprise networking and how a secure access service edge (SASE) can help your organization address its modern networking and security requirements.

Understanding the Transformation of Work

The way we work has changed dramatically over the last few years. In fact, according to the UK's FDA Working Hours Survey, 97 percent of employees want to continue remote work even though it's no longer the default as it was for many employees during the pandemic.

This increase in remote workers has also increased the number of devices being used for business. People are using smartphones to access the internet and software as a service (SaaS) apps for work.

Work is also constantly closer at hand than ever before. The prevalence of public Wi-Fi hotspots and 5G cellular connectivity means that the internet and work assets are always just a few clicks away. This ubiquitous connectivity enables users to work from anywhere.

The way work is done is also shifting to a heavy reliance on browsers. According to a report by Palo Alto Networks in partnership with Omdia, more than 85 percent of a worker's day is spent in the browser. The browser is now a primary hub of productivity; it's used to access critical corporate applications and data.

Business leaders are increasingly adopting policies for hybrid work and bring your own device (BYOD) that enable employees to take advantage of these new realities. However, this "new normal" introduces new networking and security concerns that traditional remote access connectivity is not designed to address.

THE TOP HYBRID WORK SECURITY THREATS

The hybrid workforce is here to stay, and with that comes security risks that organizations need to consider. Cybercriminals often target the weakest link in a network, so it's important to understand the risks when adapting a hybrid workforce for your organization.

Here are some of the top hybrid work security threats today:

- **Home networks:** Home networks can be insecure and often lack the security capabilities that corporate or branch offices use.
- **Increased attack surface:** The increase of remote users, SaaS apps, generative artificial intelligence (GenAI), and devices have made organizations more vulnerable, giving modern threat actors more entry points into the network. This has forced organizations to stitch together disjointed solutions that are complex to manage and create security gaps.
- **Sophistication of threat actors:** With hacker-friendly resources easily available to threat actors of all skill levels, including hacking as a service (HaaS) and adversarial artificial intelligence (AI), the barrier to entry to launch advanced and evasive threats has been significantly lowered. This has led to a significant increase in new

and never-before-seen threats that legacy security solutions struggle to prevent.

- **Shadow IT:** As more people work from home or remotely, the use of *shadow IT* (unsanctioned apps) can increase, causing gaps in security that IT departments are unaware of. Applications not managed by an organization's IT (like Google Drive, Slack, and WhatsApp) can open the door to threats.
- **Proliferation of connected devices:** As more people work remotely, their use of personal devices for work purposes increases as well, including mobile devices, tablets, and laptops. Those devices now have corporate data on them, so if the devices are lost, the organizations are at risk of losing corporate data. Unmanaged and Internet of Things (IoT) devices that also connect to the internet introduce additional vulnerabilities for organizations.
- **Data leaks:** Data leaks occur with any unauthorized or unintentional transfer of data from inside an organization to an external party or destination. These leaks are often unintentional, such as when someone inside a company accidentally transfers confidential or sensitive data to an unsanctioned/unapproved cloud application, or when they overshare confidential or sensitive data on cloud-sharing apps or public cloud storage. However, intentional leaks also happen, like when an attacker or a disgruntled employee deliberately steals the company's data.

Journeying to the Cloud

We live in an age of cloud and digital transformation. Users and applications have moved outside the traditional network perimeter, accessing an ever-increasing number of applications, including SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS) application workloads across multiple public clouds. Organizations face the challenge of proactively protecting their users, applications, and data from security threats, without compromising user experience.

Companies are fully embracing multi-cloud, with 90 percent of organizations deploying apps in two or more clouds and 98 percent of organizations claiming to be multi-cloud. In fact, by 2026, 75 percent of organizations will adopt a digital transformation model predicated on cloud as the fundamental underlying platform.

REMEMBER

As the cloud continues to play an integral role in digital transformation, the enterprise network must evolve to support new technologies, business initiatives, and the hybrid workforce.

Assessing the Impact on Branch Networking and WAN Architectures

In the early 2000s, Multiprotocol Label Switching (MPLS) networks began to replace traditional Asynchronous Transfer Mode (ATM) and private leased line hub-and-spoke wide area network (WAN) architectures. Over the next decade, MPLS became the prevalent enterprise WAN architecture.

MPLS networks provided a simple network connection between branch offices and central headquarters or data center sites. This design worked well because, at the time, most network traffic was between client desktop computers located in headquarters and branch offices and business applications hosted on servers in the on-premises data center. Internet traffic volume was relatively low and generally consisted of email and static web page browsing. Any internet-bound traffic — including traffic from the branch offices, which traversed the MPLS connection to the central headquarters or data center sites — was sent through the perimeter firewall for security protection. All network traffic could be inspected, and the perimeter firewall could enforce a centralized security policy.

As internet usage increased, many branch offices began to experience performance issues and latency. Backhauling their internet traffic across the MPLS connection for perimeter firewall inspection created significant bottlenecks, negatively impacting both internet traffic and data center traffic. The rapid adoption of cloud-based SaaS applications amplified this problem exponentially and put the final nail in the MPLS coffin. Organizations began to provision direct internet access (DIA) connections for their branch offices from local internet service providers (ISPs) to alleviate some of this congestion.

Adding DIA connections at branch offices alleviated some of the network congestion issues, but it introduced a whole new set of challenges. On the networking side, these challenges have included:

- **Routing complexity:** Routers must be configured to send traffic over the appropriate network link (for example, data center traffic over the MPLS link and internet traffic over the DIA link). The simplest solution in most cases is to configure static routes, which provide only limited resiliency.
- **Inefficient bandwidth usage:** It may be possible in certain cases to configure some basic round-robin load balancing between multiple internet connections, but more advanced algorithms that take distance, cost, load, or other weighted factors into account are generally not available. As a result, there may be times when the DIA link is congested while the MPLS link — which could otherwise be used to backhaul internet traffic through the headquarters or data center internet connection — is relatively idle.
- **Management complexity:** In many cases, the local ISP provides a commodity router for the DIA link and doesn't give the customer management access. Even if the customer has management access, the ISP routers likely won't be the same type as the MPLS routers. This means different management interfaces, different operating systems, and different remote administration tools — multiplied by the number of different remote locations, different ISPs, and different router models that you need to manage.

On the security side, challenges created by this evolved WAN architecture have included:

- **Loss of visibility and control:** With most network traffic traversing the DIA connection at remote offices destined for the cloud and the internet, enterprise security teams can't see the traffic and apply security policies from a centralized perimeter firewall in the data center.

- **Lack of integration and interoperability:** To address the loss of visibility and control, many organizations deploy firewalls, intrusion prevention systems (IPSs), web content filters, data loss prevention (DLP), and other point security solutions in their remote offices. These solutions often come from different vendors and have limited or no integration capabilities. This makes it more difficult for security teams to correlate events and implement a cohesive enterprise security strategy.
- **Management complexity:** Different security solutions from multiple vendors mean different management interfaces, different operating systems, and different remote administration tools — multiplied by the number of remote locations that you need to manage. This management complexity challenge is exponentially more difficult on the security side because of the volume and types of security information that must be analyzed daily from these different tools.

Introducing the SASE Vision

A new architecture was needed to address this shift in networking and security requirements.

REMEMBER

SASE converges networking and security services into one unified, cloud-delivered solution that includes the following, as summarized in Figure 1-1:

- **Networking:** Including software-defined wide area network (SD-WAN), virtual private networks (VPNs), quality of service (QoS), routing, and SaaS acceleration
- **Security:** Including Zero Trust network access (ZTNA), cloud secure web gateway (SWG), cloud access security broker (CASB), firewall as a service (FWaaS), secure browser, DLP, Domain Name System (DNS) security, IoT, sandbox, URL filtering, and IPS
- **Secure browser**
- **User experience**

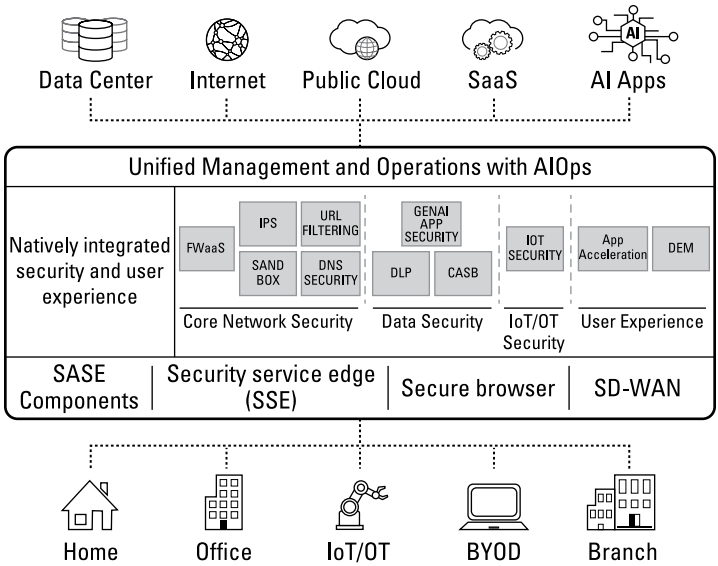


FIGURE 1-1: SASE delivers advanced network and security capabilities in a converged cloud-delivered solution.

Revisiting Modern Networking and Security Challenges with SASE

With networking and security functions unified in a single, multifunction cloud-delivered solution, SASE solves the challenges of better user experience and consistent security in the following ways:

- **Lower capital costs:** SASE requires lower capital investments than other approaches. SASE delivers networking and security capabilities in the cloud, with minimal hardware or software required on-site or on users' devices.
- **Full visibility and control:** SASE provides full visibility and control with cloud-delivered capabilities including ZTNA, cloud SWG, CASB, FWaaS, IPS, sandboxing, URL filtering, DNS security, IoT security, and secure browser.

- **Less complexity:** All cloud service management functions can be centrally managed in the cloud from an intuitive single-pane-of-glass management interface. This means network and security teams no longer need to learn, configure, and manage multiple systems from different vendors.

WARNING

Converging networking and security in the cloud with SASE promises to remedy the shortcomings of legacy security and networking architectures. However, many solutions on the market today are incomplete, requiring organizations to make trade-offs between security and functionality or require other products to fill the gaps. Dubbed *multivendor SASE*, this approach retains the legacy challenges of stitching together a multivendor environment, and troubleshooting can be a nightmare. What's the solution? Keep reading to find out.

IN THIS CHAPTER

- Enabling hybrid workforces with SASE
- Connecting and securing branch and retail locations

Chapter 2
SASE Use Cases

In this chapter, you find out about some of the most common use cases today for a secure access service edge (SASE), including hybrid workforces and branch locations. Both use cases present different challenges that a SASE solution can solve.

Discovering How SASE Enables Hybrid Workforces

Connecting and securing the hybrid workforce with traditional solutions can be a challenge, especially when users work from home or in locations where you don't have IT staff. For years, the standard solution for connecting remote users into a corporate network was remote-access virtual private networks (VPNs). In fact, for many people, *remote access* and *VPN* are synonymous.

However, the requirements for remote access today are very different than when VPN was invented in the mid-1990s. Today, IT is asked to support the needs of a dynamic, mobile workforce accessing applications that may be hosted in public cloud, private cloud, software as a service (SaaS), or conventional data centers, while maintaining high levels of performance and robust, consistent security controls. This requires an entirely new approach to remote access.

Traditional remote-access VPN limitations

Remote-access VPNs are built to do one thing: allow users outside the perimeter firewall to access resources inside the corporate network, typically through the data center.

Remote-access VPNs use a hub-and-spoke architecture (see Figure 2-1), with users connected by encrypted tunnels of various lengths depending on their distance from the data center. Nearby users may enjoy high performance, but distance degrades performance, introducing issues with bandwidth and latency. Nevertheless, this architecture is optimal for data center applications because the goal is to reach the "hub" where your internal applications and data are located.

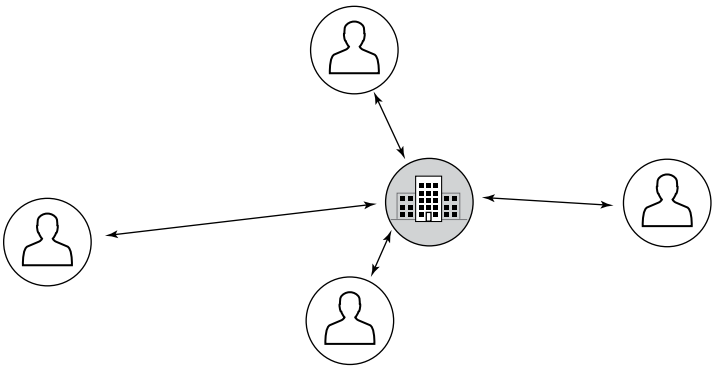


FIGURE 2-1: Traditional remote-access VPN architecture.

The model breaks down when a mixture of cloud applications is involved. During the pandemic, many corporate applications moved to a variety of web-based architectures including SaaS as well as one or multiple public cloud (infrastructure as a service, or IaaS) providers. With remote-access VPN, traffic always goes to the VPN concentrator or gateway first, even if the application is hosted in the cloud (as shown in Figure 2-2). As a result, the traffic goes to the VPN gateway at the corporate headquarters or data center and then egresses from the perimeter firewall to the internet, with the application response going back to headquarters or the data center before it returns to the user. With cloud applications, this traffic essentially follows a "trombone" path, making a lengthy (and slow!) round trip to reach an internet-accessible

location. This approach is sensible from a security perspective, but it doesn't make sense for network optimization.

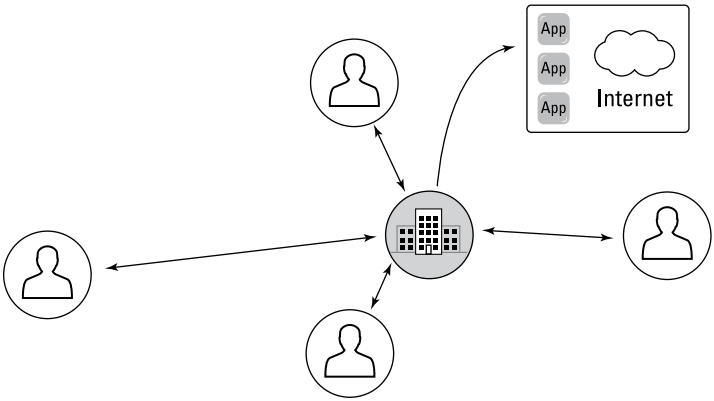


FIGURE 2-2: Traditional remote-access VPN backhauling traffic to reach the cloud.

Using cloud applications over remote-access VPN can hurt the user experience. As a result, end users tend to avoid using remote-access VPN whenever possible. They tend to connect when they need access to the internal data center and disconnect when they don't, and that leads to multiple issues.

WARNING

When users are disconnected, their organizations lose visibility into application usage, control over access to unsanctioned applications, and the ability to enforce security policies. In addition, the drastic increase in mobile workforce places significant demands on VPN gateways/concentrators to scale without the infrastructure to support it. The constant traffic overloads force the VPN gateways to deliver poor performance and negatively impact the end-user experience.

Unsatisfactory compromises

To compensate for the networking problems with remote-access VPN, IT teams typically introduce multiple compromises, each with its own security implications:

- **User-initiated tunnel:** A common remote-access VPN deployment model is to let users initiate the tunnel as needed. They typically connect for a short time, complete

their work with a given application, and disconnect. When disconnected, they have direct access to the internet with no traffic inspection.

- **Split-tunnel VPN:** A common yet insecure method of deploying remote-access VPN is to set up a policy that permits split tunneling. In this model, traffic bound for the corporate domain goes over the VPN tunnel, and everything else goes directly to the internet. The improvements in network performance come at a cost, though: Internet and cloud traffic are not inspected.
- **Web proxy/secure web gateway (SWG):** To compensate for scenarios in which users are not connected to the VPN, many organizations have tried alternative network security measures such as using a proxy for the web browser when users are off-network. However, by definition, a web proxy doesn't fully inspect network traffic. Even worse, the traffic inspection the proxy does perform will be fundamentally different from the inspection that's happening at headquarters, with inconsistent results depending on users' locations.

With the rapid growth of mobile workforces and cloud-based applications, organizations are finding that their remote-access VPN is neither secure nor optimized for the cloud. A new approach is necessary to account for today's application mix.

A modern architecture for the hybrid workforce

Today's hybrid workforce needs access to the data center and the internet, as well as to applications in the public cloud. A proper architecture should optimize access to all applications, wherever they (and the users) are located.

REMEMBER

A SASE solution provides a cloud-delivered networking and security infrastructure that enables an organization to connect users automatically to a nearby cloud services edge, provide secure access to all applications, and maintain full visibility and inspection of traffic across all ports and protocols (see Figure 2-3).

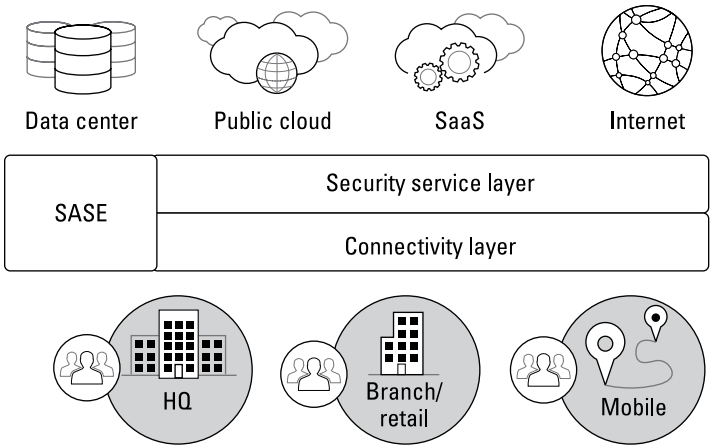


FIGURE 2-3: Easy access to the connectivity layer, wherever your users are.

The benefits are significant for both managed and unmanaged devices.

For managed devices:

- Users have a SASE client app installed on their laptops, mobile phones, or tablets. The app connects to the SASE platform automatically whenever internet access is available, without requiring any user interaction.
- Users can access all their applications, whether in the cloud or the data center. The connectivity layer connects applications in different locations, making it possible to establish secure access (based on application and user identification policies) to public cloud, SaaS, and data center applications.
- SASE delivers protection through the security service layer, such as protections against known and unknown malware, exploits, command-and-control (C2) traffic, and credential-based attacks.
- Organizations migrating from a legacy proxy-based web security solution to SASE should have the opportunity to do so without significant network architecture changes. Over time, customers can easily transition from a proxy-based architecture to a more secure connection method that protects all apps, ports, and protocols, not just web.

For unmanaged devices:

- Users taking advantage of bring your own device (BYOD) policies can securely access applications without an app installed by using a clientless VPN.
- Clientless VPN enables secure access to web-based and SaaS applications from unmanaged devices with inline protections by using Security Assertion Markup Language (SAML) proxy integration.

CASE STUDY: AN ENERGY SERVICES PROVIDER

Companies around the world have adapted to support a hybrid workforce, sometimes overnight. A SASE solution can help, as it did for an energy services provider with more than 100,000 employees in 120 countries looking to support its remote workforce during and after the pandemic.

It needed:

- A solution to scale with its remote workforce quickly
- To stay ahead of cybersecurity risks and threats
- A faster way to connect remote employees and cloud applications

A SASE solution helped the company to:

- Increase the number of employees working remotely from 25,000 to 80,000 users
- Reduce complexity
- Strengthen security and enable a single unified policy base across the enterprise
- Provide a seamless and consistent experience for all users

Enabling Efficient and Secure Branch and Retail Connectivity

Cloud adoption is doing more than changing user mobility strategies; it's affecting branch and retail networking strategies, too. With the growing number of applications in the cloud, it doesn't make sense to carry all of an enterprise network's traffic back to headquarters over expensive Multiprotocol Label Switching (MPLS) connections.

As a result, many organizations are redesigning their wide area networks (WANs) to enable branch offices and retail stores to go directly to the cloud. With the drive to reduce the IT footprint at the branch to cut operational costs and reduce complexity, organizations are also looking for ways to reduce the amount of hardware that needs to be physically deployed and managed at each location.

The challenges of traditional branch and retail networking

The traditional standard for branch and retail networking uses an MPLS circuit between each remote site and headquarters or the data center in a hub-and-spoke topology. This makes sense when the remote site largely uses applications hosted in an internal data center or when bandwidth requirements aren't very high.

For example, a company that sells machine parts may host an inventory application in its internal data center. Retail stores across the region may query the database to get real-time information on warehouse inventory. The application doesn't require significant bandwidth, but the connection must be reliable because any downtime or performance issues could lead to lost business.

WARNING

Many applications have now moved out of the internal data center and into the public cloud. As a result, hub-and-spoke networking creates serious performance issues because traffic must pass over the MPLS connection, egress the perimeter firewall, connect to the cloud-based host, and then follow the reverse path back to the user. The MPLS link is a bottleneck because the traffic makes an unnecessary trip to headquarters over a relatively slow connection. This adds cost and complexity due to the additional MPLS resources required to hairpin traffic.

Compounding this issue even further, employees at branch or remote locations need access to more bandwidth-intensive applications than ever before, driving up bandwidth requirements. It's common to see branch offices and retail stores adopt new applications, such as:

- Real-time collaboration tools such as videoconferencing, instant messaging, file sharing, and Voice over Internet Protocol (VoIP)
- Video streaming, cloud application access, and online data backup services
- In-store guest Wi-Fi

As a result, enabling direct internet access at the branch is necessary for businesses to compete today. However, the options for how it's done can be overwhelming when you consider the need for bandwidth capacity, reliability, operational efficiency, and security.

Augmenting MPLS with direct internet access

As organizations have embraced the cloud, traditional connectivity options of private links from branch to data center have begun to create problems. Many organizations have augmented their private links with internet connections to improve WAN availability and enable direct cloud access.

REMEMBER

Providing branch locations with direct internet connections requires IT teams to consider many factors. Plenty of options are available, with most major cities having a range of providers for low-cost, high-speed, business-class internet. However, the speed of the service is not the only concern. Organizations also need to consider the reliability and security of the service, and those issues aren't always easy to address.

As a result, many organizations look to software-defined wide area network (SD-WAN) as the answer to these challenges. SD-WAN provides the intelligence to:

- Optimize forwarding decisions based on applications, transports, bandwidth availability, and performance service-level agreements (SLAs)

- Automate complex networking tasks (such as policy-based routing)
- Deploy and configure at scale
- Provide a centralized interface to manage networking across branch locations

However, no SD-WAN solution is complete without a natively integrated, robust security service.

Replacing MPLS with broadband and 5G

WARNING

As organizations expand, their branch offices become distributed, with more remote locations added as part of their infrastructure. Providing WAN connectivity with MPLS to these branches comes with operational challenges and significant costs.

Similarly, organizations that grow due to mergers and acquisitions create a heterogeneous WAN network. Managing the differences in providers, SLAs, and bandwidth requirements monopolizes IT resources; the results are poor network connectivity and degraded application experience. These organizations require reliable, highly available WAN connectivity that can easily support the bandwidth demands of the cloud applications.

Many organizations are easily transforming complex networks with affordable and high-bandwidth internet connections like broadband and, most recently, 4G LTE and 5G. With the speed and reliability enhancements and cost savings they provide, metered links like 4G and 5G are proving just as effective as WAN links for remote and mobile locations. Organizations now are able to replace their MPLS WAN connectivity without any compromises in speed or performance.

REMEMBER

Many organizations have found a de facto solution in SD-WAN due to its ability to support carrier-independent multiple WAN links like broadband, direct internet, and 4G/5G. SD-WAN's automated VPN connectivity delivers encrypted WAN links on top of public internet connections that ensure security and conformance. In addition, the application intelligence-based steering ensures that the WAN links are best utilized as active–active or active–backup based on bandwidth, performance SLAs, and business policies to deliver the best user experience.

A modern architecture for branch transformation

Branch offices need access to all applications, including those in the data center, on the internet, in SaaS applications, and in public clouds. The proper architecture should optimize access to all applications, wherever the applications or the users are located.

This architecture is known as the *thin-branch approach.* Much of the branch services are done in the cloud, which keeps the branch lightweight. A thin-branch approach enables businesses to manage security and access through a centralized control via the cloud.

In contrast, legacy WAN solutions often take a *thick-branch approach,* in which much of the branch services such as security, segmentation, routing, and more are done specifically at the branch, requiring more overhead and effort.

WARNING

Using the thick-branch/legacy WAN approach can result in infrastructure sprawl, separate management interfaces, and tedious troubleshooting that can increase operational complexity significantly. In addition, managing WAN connectivity, VPN tunnels, quality of service (QoS), and security policies at the branch demands higher processing power and resources. Businesses are forced to upgrade their branch infrastructures, adding costs to improve application performance and user experience.

REMEMBER

The thin-branch approach aligns heavily with the SASE architecture, utilizing the cloud and providing a positive user experience. SASE provides cloud-delivered networking and security infrastructure that makes it possible to connect branch offices to a nearby cloud gateway, enabling secure access to all applications together with full visibility and inspection of traffic across all ports and protocols.

With this architecture, organizations don't have to manage separate on-premises networking and security appliances. Policies are applied to traffic destined for the cloud, to the internet, back to corporate headquarters, and even over a full-mesh VPN for branch-to-branch applications.

This change immediately eliminates operational expenses such as the shipping, installation, and ongoing maintenance of extra IT equipment at remote sites. Staffing can focus on operations and protecting the organization from a central location instead of handling the enforcement at the branch network edge.

CASE STUDY: A HIGH-TECH COMPANY

Organizations with branch and retail locations often struggle to provide adequate connectivity and security outside the corporate headquarters or data centers. A SASE solution with SD-WAN can help, as it did for a high-tech company with more than 60,000 employees that was looking to reduce costs and increase network speeds.

The challenges it was facing included:

- An inability to scale or meet employee needs with its legacy MPLS solution
- Unreliable internet connectivity that impacted branch operations
- Extensive manual operations that consumed IT staff's time and resources

Implementing a SASE solution with SD-WAN provided:

- Application awareness and insights into application traffic
- Centralized management for simplified network operations
- A zone-based firewall for branch segmentation and security
- Improved uptime and availability of branch locations
- Scalability up to 2 gigabits per second (Gbps) of WAN throughput at large office locations

IN THIS CHAPTER

- Defining the need for SD-WANs
- Getting real about VPNs
- Ensuring service quality with QoS
- Implementing intelligent routing
- Accelerating SaaS performance

Chapter 3
SASE Networking Capabilities

In this chapter, you find out about the core networking capabilities of a secure access service edge (SASE) solution and how security has become a critical component to software-defined wide area network (SD-WAN). In addition, you look at how to ensure the best quality for your SD-WAN.

Discovering How SD-WANs Provide Value

Wide area networks (WANs) use links such as Multiprotocol Label Switching (MPLS), wireless, broadband, virtual private networks (VPNs), and direct internet to give users in remote offices access to applications, services, and resources, enabling them to carry out daily functions regardless of location.

Traditional WANs rely on physical routers to connect remote or branch users to applications hosted in data centers. Access rules, traffic policies, and quality of service (QoS) prioritization need to be manually configured on each device. The data flows are typically determined by a network engineer or administrator

who creates rules and policies, often manually, for each router on the network. This process can be time-consuming and prone to errors.

SD-WAN enables enterprises to leverage a combination of WAN transport services including MPLS, Long-Term Evolution (LTE), 5G, and commodity broadband to securely connect branches and users to applications both in the cloud and in the data center.

SD-WAN abstracts the control and management processes from the underlying networking hardware, making them available as software that can be easily configured and deployed from the cloud or on-premises. A centralized control plane means network administrators can create new rules and policies and then configure and provision them across an entire network at once.

REMEMBER

As cloud applications become mainstream, the traditional approach of a private WAN link backhauling traffic to a data center doesn't work, because the traffic must be sent out to the cloud from the data center. Backhauling traffic to data centers was a suitable WAN architecture when all applications were hosted in data centers. However, now that most applications are cloud/software as a service (SaaS) based, it doesn't make sense to backhaul traffic to the data center on its way to the internet. It's better to go directly to the internet from the branch (known as direct internet access, or DIA) for cloud/SaaS and back to the data center only for apps hosted there. SD-WAN makes this possible.

Compared to traditional WANs, SD-WANs can intelligently manage multiple types of connections, including MPLS, broadband, LTE, and others, as well as support applications hosted in data centers, public and private clouds, and SaaS services. SD-WAN can route application traffic over the most optimal path based on performance (considering factors such as latency, jitter, packet loss, availability, and more), in real time, by intelligently load-balancing across multiple links. Prior to SD-WAN, organizations had to manually configure multiple links to behave a certain way using policy-based routes — for example, to determine which application should take which link.

REMEMBER

Companies are embracing SD-WAN to connect branch offices to the corporate network and provide local internet breakout for better performance and user experience.

SD-WAN Advantages

SD-WAN offers geographically distributed organizations and companies with multiple branches many benefits, including the following:

- **Operational resiliency and simplicity:** SD-WAN enables centralized management and simplified configuration rules. In addition, by combining SD-WAN with zero-touch provisioning — a feature that helps automate the deployment and configuration processes — organizations can further reduce the complexity, resources, and operating expenses required to turn up new sites.
- **Greater flexibility and agility:** With SD-WAN, organizations have more connectivity options, such as broadband internet, which is faster to provision than MPLS. Configuring, deploying, and managing MPLS is time-consuming for most organizations. It can sometimes take a service provider up to three months to install a new MPLS circuit, and MPLS isn't readily available in all areas. SD-WAN remediates this challenge because it separates control of the network services from transport, letting organizations securely use any available internet connection (such as broadband or LTE) without being limited to the coverage provided by the MPLS carrier.
- **Improved user experience:** Without SD-WAN, connecting branch offices to cloud applications is expensive. Traditional WANs must backhaul traffic to the headquarters or corporate data center, usually over MPLS (as shown in Figure 3-1), which can lead to inefficient resource usage and poor performance. By enabling efficient access to cloud-based resources without needing to backhaul traffic to centralized locations, organizations can provide a better overall user experience. That leads to less frustration, higher productivity, and better collaboration. SD-WAN delivers an application assurance framework that measures, enforces, and alerts IT administrators about application performance. The foundational SD-WAN capabilities, such as measuring service-level agreements (SLAs), traffic failover, and load balancing, should extend to security service edge (SSE) and leverage SSE's distributed and global hyperscale architecture to optimize application performance at the middle mile.

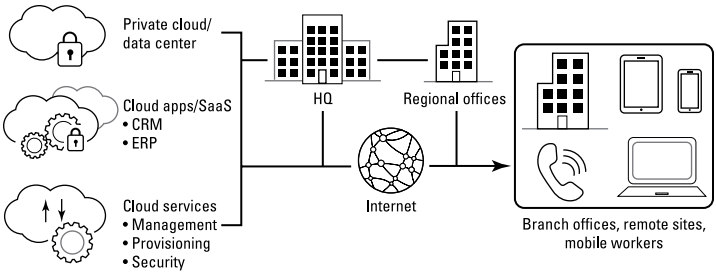


FIGURE 3-1: Efficient SD-WAN traffic routing.

- **Efficient use of resources:** Here are some ways that SD-WAN can lead to greater efficiency:
  - According to industry research, companies can save up to 40 percent over five years by cutting down on hardware, software, and support acquisition.
  - Fewer personnel are needed to manage, troubleshoot, and provision WAN equipment.
  - Because SD-WAN supplements or substitutes MPLS with broadband or other internet connectivity, traffic can be routed based on the best option for cost versus performance.
  - With AI, issues remediation can be done faster and more intelligently.
- **Integrated security:** SD-WAN must deliver Zero Trust security with accurate user, application, and device visibility, including Internet of Things (IoT) and precision artificial intelligence (AI). By connecting seamlessly with a globally distributed cloud-delivered SSE with low-latency connections, organizations have access to capabilities including firewall as a service (FWaaS), cloud access security broker (CASB), secure web gateway (SWG), and IoT security to ensure Zero Trust at all times. This provides visibility to all your assets, including the rapidly growing IoT devices, to ensure you can apply the proper controls and policies to the entire network.

Prioritizing Security

WARNING

When adopting SD-WAN, decision-makers often prioritize connectivity and cost benefits over security. This practice is a mistake that can put the network at risk.

Although SD-WAN offers many benefits, it can also bring challenges if it isn't architected correctly, including new security risks, unreliable performance, and increased complexity resulting from the need for multiple overlays. When security is an afterthought, it tends to be bolted on, introducing management complexity and subpar protection. Plus, network performance can become less reliable because organizations use the congested public internet as the WAN middle mile. Organizations sometimes try to address these challenges by building their own SD-WAN hubs and interconnect infrastructures, which results in more complexity.

In a SASE solution, SD-WAN edge devices can be connected to a cloud-based infrastructure rather than physical SD-WAN hubs located in data center or colocation facilities. This enables the interconnectivity between branch offices without the complexity of deploying and managing physical SD-WAN hubs. In addition, organizations can improve application performance when routing branch traffic to a distributed cloud edge versus a centralized hub. Leveraging the cloud for middle-mile connectivity can ensure greater end-user experience for the branch while also diminishing the need to build a global backbone that's complex and time-consuming.

TIP

You may have already adopted SD-WAN in your network infrastructure (or you may be considering it) as a way to securely connect and control access to branch offices and remote employees. SASE creates a unified approach for SD-WAN and security services to connect to, providing a single point of view and simplified management solution to protect your network.

Understanding the Role of VPNs

For many years, VPNs have enabled secure connectivity to corporate networks and resources over the internet. The two most common types of VPNs are remote access (for connecting remote users) and site-to-site (for connecting remote locations).

VPNs facilitate secure data transit over the internet through a tunneling protocol, where data is encrypted using Internet Protocol Security (IPSec) or Secure Sockets Layer (SSL). The tunneling protocol also *encapsulates* (wraps) the data with routing information for the receiving user.

VPNs are effective at enabling secure access to corporate data centers and other physical locations, but they aren't optimized for access to the cloud. As a result, there is no security or access control when users disconnect to reach cloud apps or services, as shown in Figure 3-2.

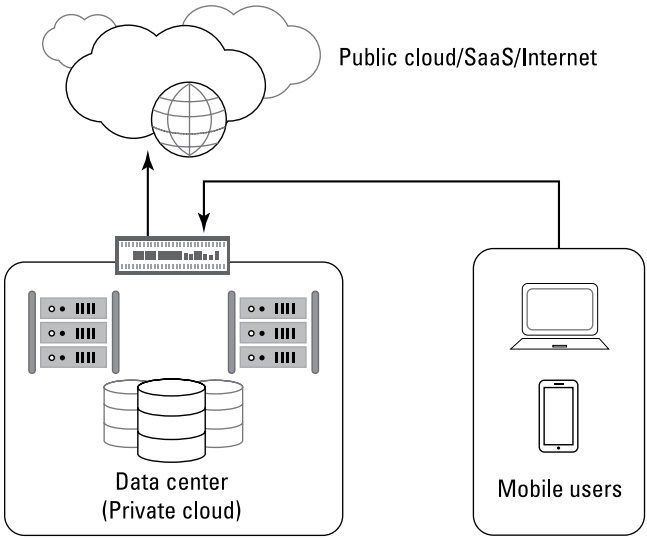


FIGURE 3-2: Remote-access VPN is not designed to support cloud applications.

A SASE solution encompasses VPN services and enhances those capabilities. Operating in a cloud-based infrastructure, it securely routes traffic to physical locations, as well as to public cloud

services such as SaaS, platform as a service (PaaS), infrastructure as a service (IaaS), and private cloud apps and services.

In an IPSec VPN, you can create a site-to-site connection to a cloud-based infrastructure from any IPSec-compatible device located at a branch or retail location via a branch router, wireless access point (WAP), SD-WAN edge device, or firewall, all without the need to back-haul traffic to a physical location for security scrubbing (see Figure 3-3). Remote users can employ an always-on IPSec or SSL VPN connection between their endpoint or mobile devices and their applications, with the SASE solution ensuring consistent traffic encryption and threat prevention.

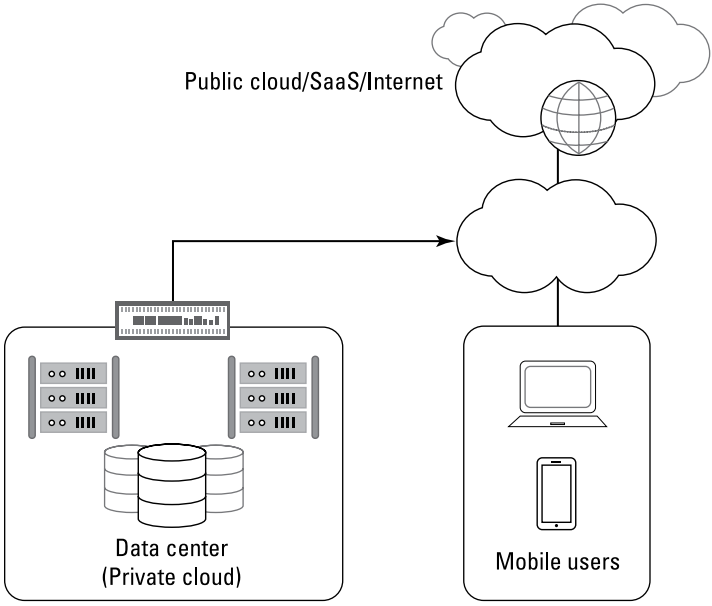


FIGURE 3-3: SASE uses cloud infrastructure to connect users to both cloud apps and the data center.

REMEMBER

No matter which type of VPN service you use in your organization, a SASE solution provides a unified cloud infrastructure to connect to instead of backhauling traffic to physical corporate locations. This dramatically simplifies the management and policy control needed to enforce least-privilege access rules.

Ensuring Quality of Service

As organizations transition from MPLS to SD-WAN using DIA links, they often find that the service quality varies. Quality of service (QoS) controls establish bandwidth allocations assigned to particular apps and services and prioritize them when there is a contention for bandwidth. Businesses rely on QoS to ensure that their critical apps and services (for example, medical equipment or credit card processing services) perform adequately. QoS also helps businesses avoid and overcome bandwidth congestions caused by nonbusiness-related traffic, like streaming video, which can severely impact business operations and sales (see Figure 3-4).

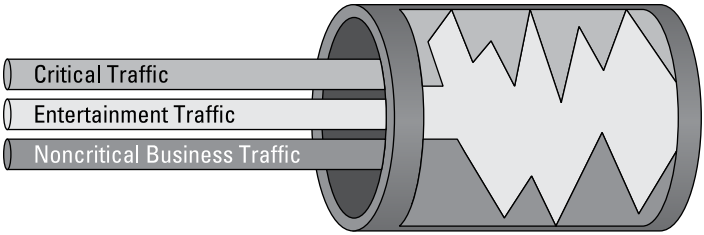


FIGURE 3-4: Bandwidth without QoS control.

WARNING

QoS is an important step when an organization begins migrating from MPLS to SD-WAN. As businesses start augmenting or replacing their MPLS links with broadband internet, they realize it's a "best effort" that doesn't provide an SLA guaranteeing performance for application traffic. If you have QoS configured for your network, your broadband internet service provider (ISP) will ignore QoS tagging on its routers. As a result, organizations typically procure enough bandwidth to meet their expected peak utilization, which can add to costs significantly.

Administrators can use QoS to designate which apps and services should take precedence over others, as shown in Figure 3-5. A SASE solution incorporates QoS services in the cloud, enabling IT administrators to easily mark sensitive applications, such as Voice over Internet Protocol (VoIP), as high priority over general internet and entertainment sites and apps.

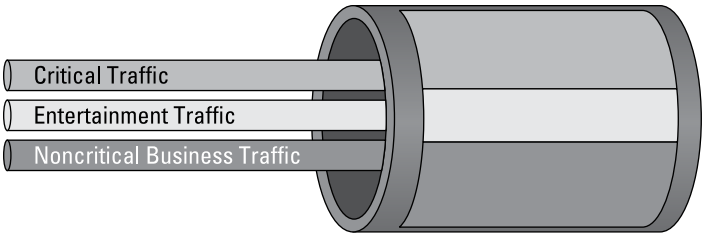


FIGURE 3-5: Bandwidth with QoS control.

REMEMBER

Managing the QoS traffic and allocation to guarantee performance SLAs doesn't need to be difficult. An effective SASE solution enables organizations to accurately identify applications and dynamically shape and prioritize traffic based on the business policies to better manage bandwidth and improve user experience.

Routing

Traditional architectures connected to WANs use routers to allow users to access applications, the cloud, and the internet from local area networks (LANs). Routers connect networks, steer application traffic, and control user access on the network. As a result, these branch routers lack the ability to provide brownout controls and application remediation when WAN connections degrade or bandwidth saturation occurs. Businesses leveraging unified communications as a service (UCaaS) and SaaS applications with higher-bandwidth demands suffer from poor user experience due to such limitations and are forced to add more bandwidth to accommodate. Doing so can become costly.

Highly trained IT experts are required to configure branch routers. Using a command-line interface (CLI), they construct and configure core functionalities such as traffic forwarding, QoS, and access controls. When an organization has just a few routers, this may be workable, but it becomes a problem when an organization has hundreds or even thousands of routers, dispersed across many branches worldwide. When organizations have service updates or need to upgrade their network, the idea of reconfiguring many routers manually just isn't practical.

Effective SASE solutions use intelligence and automation to avoid the inefficiencies of traditional routers. They simplify routing based on application intelligence, performance SLAs, and bandwidth requirements to accurately steer traffic. This results in effective bandwidth utilization on any WAN links (MPLS, broadband, direct internet, and 4G/5G), which can decrease costs and improve application performance. Additionally, automating complex routing configurations and remediation tasks enables large-scale deployments while reducing troubleshooting and resolution efforts.

Accelerating SaaS Performance

It's a no-brainer that organizations are moving to the cloud by adopting SaaS applications to simplify their branch infrastructures. As more and more branches require access to applications, it has become pivotal for businesses to address growing bandwidth demands and ensure exceptional user experience for employees at the branch. As a result, high jitter, latency, and packet loss can be detrimental to the application performance at the branch.

WARNING

Legacy networks, with their data center backhauling and packet-based routing, fail to intelligently steer traffic on the best-performing and highest available WAN links while also adding significant latency to SaaS application access. Legacy approaches to SD-WAN have relied on taking the traditional model of packet routing and forcing it to fit the cloud-ready enterprise. Some solutions can appear to simplify the creation of VPNs over broadband connections but have fallen short in delivering on the transformative promise of SD-WAN.

Legacy SD-WAN solutions are built using Layer 3 packet-based policies, with limited app-based networking policies and app visibility. This makes it difficult for network teams to deliver application SLAs. As a result, businesses now need deep application visibility, with Layer 7 intelligence for network policy creation and traffic engineering. Only then can network teams provide exceptional user experiences by delivering SLAs for all apps, including cloud, SaaS, and UCaaS.

Organizations are struggling to deliver the best user experience for these SaaS applications, which are increasingly used for productivity and collaboration. SaaS applications have more dynamic content with application protocols, ports, and server IPs constantly evolving, making it challenging to optimize application brownouts and degradation with traditional techniques. They're distributed and increasingly hosted across multiple cloud platforms, making it difficult to provide connectivity based on availability, performance, and geographic locations.

REMEMBER

To combat these performance issues, a SASE solution can provide accurate application identification combined with advanced performance SLAs like mean opinion score (MOS), server response time, and transaction failures to steer SaaS traffic. In addition, they can automate application remediation to ensure consistent performance during network degradation. This results in critical improvements to user experience without added bandwidth requirements.

Some advanced SASE solutions provide application acceleration capabilities such as the ability to optimize network protocols like Transmission Control Protocol (TCP), resulting in better performance for throughput-intensive tasks, such as large file transfers. In some cases, advanced SASE solutions can deliver application acceleration for complex SaaS applications by intelligently predicting the content users will request and requesting that content in advance to reduce the latency that the user experiences.

IN THIS CHAPTER

- Implementing ZTNA
- Ensuring internet security with a cloud SWG
- Identifying and securing access to SaaS applications
- Deploying a next-generation FWaaS
- Preventing sensitive data loss and ensuring regulatory compliance
- Securing DNS resolution
- Leveraging threat prevention tools

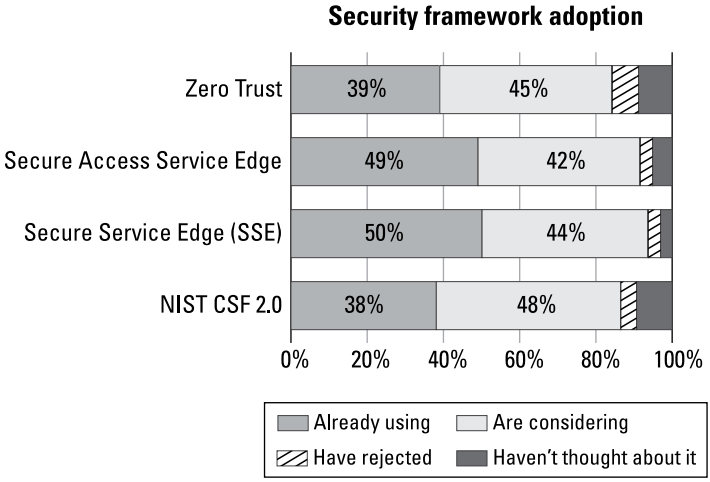
Chapter 4
SASE Security Capabilities

Security is fundamental for organizations as users access data and applications from anywhere, like their home, headquarters, branch offices, and the cloud. In this chapter, you find the critical tools needed to provide security across all different aspects of the network and the core security capabilities in a secure access service edge (SASE) solution.

Modernizing the Access Infrastructure with ZTNA

Many companies still lack the appropriate protection and policies needed to adequately secure their users, applications, devices, and data, as shown in Figure 4-1. This is especially true with the transformation of work and users demanding secure and reliable

access to apps and data, regardless of their location or device. Legacy remote access VPN solutions were never designed to facilitate or accommodate the rapid rise of hybrid work and direct-to-app connections. Having to work with systems ill-equipped for the current reality stresses IT security teams who are struggling to adapt their policies and techniques to this new way of work. As a result, more and more organizations are looking to modernize their access infrastructure around Zero Trust Network Access (ZTNA). In fact, 83 percent of global organizations are planning to implement a converged security solution extending comprehensive security measures across services, networks, and platforms.



Source: Verizon Mobile Security Index 2024 report

FIGURE 4-1: Security framework adoption.

ZTNA is a key part of the Zero Trust philosophy of "never trust, always verify," developed by Forrester Research. Under ZTNA, users who want to directly access applications must authenticate through an access broker. This enables an IT admin to apply more granular controls leveraging user identities to restrict access and minimize their exposure.

ZTNA solutions are based on a micro-perimeter architecture, providing granular access only to authorized applications and data. However, legacy ZTNA approaches provide too much access,

incorporate an "allow once and ignore" model that lacks continuous trust verification as well as ongoing content inspection, and provide inconsistent and incomplete security. To achieve true least-privilege access with consistent protection, organizations must deploy additional controls on top of the traditional ZTNA model to deliver dynamic and adaptive access controls while inspecting and securing all traffic and data across all use cases. That ultimately leads to increased deployment and management complexity and, thus, increases the risk of a breach.

The modernization of ZTNA was introduced to overcome the shortcomings of legacy approaches. ZTNA is designed to secure all apps, including public, private, software as a service (SaaS), and generative artificial intelligence (GenAI) applications, with real-time, artificial intelligence (AI)–powered inspection to ensure all user-to-app traffic is secure. With a common policy framework and single-pane-of-glass management, ZTNA secures today's way of work without compromising performance to ensure exceptional user experiences.

REMEMBER

Layer 7 inspection and control, as well as advanced threat protection (ATP) security, are imperative to Zero Trust.

SASE builds upon the key principles of ZTNA and extends them across all the other services within a SASE solution. Identifying users, devices, and applications, no matter where they're connecting from, simplifies policy creation and management. SASE removes the complexity of connecting to a gateway, by incorporating the networking services into a single unified cloud infrastructure.

REMEMBER

A SASE solution should also secure all applications, as well as incorporate advanced security services for the consistent enforcement of DLP and threat prevention policies. This is necessary because, although access controls are useful for establishing who the person is, other security controls are also needed to make sure their behaviors and actions are not harmful to the organization and its data. It's also necessary to apply the same controls across access to all applications.

WHAT IS ZERO TRUST?

Zero Trust is a cybersecurity strategy that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by leveraging network segmentation to prevent lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

Zero Trust was created by John Kindervag at Forrester Research, based on the realization that traditional security models were designed to operate on the outdated assumption that everything inside an organization's network should be trusted. Under this broken trust model, it's assumed that a user's identity and device are not compromised and that all users act responsibly and, thus, can be trusted implicitly. The Zero Trust model recognizes that trust is a vulnerability. When they're on the network, users — including threat actors and malicious insiders — are free to move laterally and access or exfiltrate whatever data they aren't limited to. ***Remember:*** The point of infiltration of an attack is often not the target location.

Protecting Web Traffic with a Cloud SWG

Secure web gateways (SWGs) provide one solution to the problem of securing web traffic (mentioned in Chapters 2 and 3).

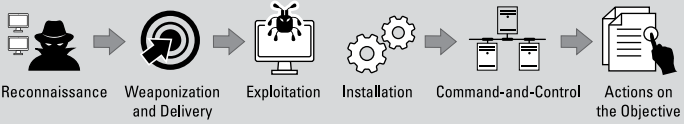
Instead of fully inspecting all network traffic, a web gateway examines traffic from a web browser and blocks websites and known malware. Organizations looking for a better solution may use this approach without having to deploy a hardware appliance at the branch.

Many organizations rely on an SWG to protect employees and devices from accessing malicious websites. Palo Alto Networks has detected more than 126 million new malicious pages each year.

SWG can be used to block inappropriate content or websites that businesses simply don't want users accessing while at work, such as streaming services like Netflix. Additionally, SWG can be used to enforce an acceptable use policy (AUP) before granting internet access.

KNOW YOUR ENEMY: MODERN CYBERATTACK STRATEGY

Modern cyberattack strategy employs a patient, multistep, covert process that blends exploits, malware, and evasion in a coordinated attack. The cyberattack life cycle shown here is a sequence of events that an attacker goes through to successfully infiltrate an organization's network and steal data.



Here are the steps of the cyberattack life cycle:

1. **Reconnaissance.** Like common criminals, cybercriminals carefully study their victims and plan their attacks, often using social engineering, phishing, email address harvesting, and other tactics to research, identify, and select targets. They also use various tools to scan networks and SaaS applications for vulnerabilities, services, and applications that can be exploited.
2. **Weaponization and delivery.** Next, the attacker determines the malware payload and the method that will be used to deliver it. For example, data files or web pages can be weaponized with exploits that are used to target the victim's vulnerable software and delivered via an email attachment or drive-by download.
3. **Exploitation.** The attacker generally has two options for exploitation: social engineering or software exploits. *Social engineering* is a relatively simple technique used to lure someone into clicking on a bad link or opening a malicious executable file, for example. *Software exploits* are more sophisticated because they essentially trick the operating system (OS), browser, or other third-party software into running an attacker's code. This means the attacker must craft an exploit to target specific vulnerable software on the endpoint. When exploitation has succeeded, an advanced malware payload can be installed.

(continued)

(continued)

4. **Installation.** When a target endpoint has been infiltrated, the attacker needs to ensure *persistence* (resilience or survivability). Various types of advanced malware are used for this purpose, including antivirus software, backdoors, bootkits, and rootkits.
5. **C2.** Communication is the lifeblood of a successful attack. Attackers must be able to communicate with infected systems to enable C2 and to extract stolen data from a target system or network. The attacker can also use this communication to move laterally, targeting other systems on the victim's network. C2 communications must be stealthy and can't raise any suspicion on the network.
6. **Actions on the objective.** Attackers have many different motives for an attack, including data theft, destruction of critical infrastructure, hacktivism, or cyberterrorism. This final phase of the attack often lasts months or even years, particularly when the objective is data theft, because the attacker uses a low-and-slow attack strategy to avoid detection.

WARNING

Web gateways are not a substitute for firewalls. Partially inspecting traffic with a SWG means the remaining traffic passes through uninspected or else the application breaks. The organization remains blind to applications that legitimately use alternative ports, as well as those intentionally evading inspection. Security is compromised because there is no inspection of non-browser traffic and no protection against other stages of the attack life cycle, such as secondary malware payloads or ongoing command-and-control (C2) traffic with a compromised endpoint.

As organizations grow, coverage and protection become more difficult. A SASE solution moves SWG into the cloud, providing protection in the cloud through a unified platform for complete visibility and control over the entire network.

REMEMBER

A SASE solution should include SWG, enabling organizations to control web access and enforce security policies that protect users from hostile websites. But remember that a SWG is just one service of the overall SASE solution. Other security services like ZTNA, cloud access security broker (CASB), firewall as a service (FWaaS), Domain Name System (DNS) security, DLP, and ATP are also necessary to ensure all application traffic is secured.

Securing Access to SaaS Applications

SaaS applications (like Box, Microsoft 365, Microsoft Teams, Salesforce, and Slack) offer companies, employees, and customers many business and operational benefits. However, for each benefit, there are also potential drawbacks when it comes to information security, as shown in Table 4-1.

TABLE 4-1 The Pros and Cons of SaaS Adoption

Pros	Cons
SaaS apps can be deployed quickly. As a cloud-delivered service, SaaS apps can be onboarded rapidly within enterprise environments. When they're stood up, they can be made readily accessible to all users via the cloud from anywhere with internet connectivity.	As a cloud-delivered service, accessible over the public internet, malicious actors can more readily try to gain unauthorized access. SaaS apps increase the attack surface, largely driven by factors such as additional third-party connections and increased use of public cloud infrastructure.
Most enterprise data today originates within SaaS apps, which then store this data at a relatively low cost to the organization. Having this data in the cloud allows employees to more easily collaborate with multiple users across various locations.	With enterprise data widely dispersed and stored across SaaS apps, sensitive and proprietary company data can become overexposed. Losing visibility and control of enterprise data to third-party SaaS vendors increases the risk of intentional and unintentional data loss and noncompliance.
SaaS apps are easier to update. Instead of having your IT department manually upgrade an application and/or a physical server in a datacenter, that function can be done from any location virtually, without the need to maintain hardware, and it's often done automatically.	SaaS vendors do an amazing job of releasing new features and functionality, but the frequent pace of change also makes it difficult for IT and information security teams to keep tabs on potential misconfigurations, vulnerabilities, and security risks.

The volume of data being created, transferred, stored, and shared in SaaS cloud environments continues to increase. At the same time, employees are using more SaaS apps than ever, accessing them from a range of devices, and not prioritizing security during use.

As a result, some undesirable trade-offs have emerged:

- **Lack of centralized visibility** into sanctioned and unsanctioned SaaS applications (shadow IT), including app misconfigurations and risks, user activities, and data. Fragmented and siloed views across SaaS platforms increase the likelihood of vulnerabilities as security controls are not applied uniformly across all SaaS apps. Moreover, the lack of clarity into which SaaS apps are used and how they impact productivity can hinder an organization's business and operational efficiency.
- **Oversharing and exposure of sensitive data** results from an increasing business and operational need to share data more widely with partners, contractors, and vendors. Sensitive data is growing exponentially and sprawling across SaaS apps, users, and locations across on-premises and cloud environments, resulting in overexposure.
- **Risk from advanced threats** and difficulty with end-user management poses a substantial challenge in SaaS security management. The inability to detect zero-day threats and track user access and activity across SaaS prevents IT security teams from identifying potential misuse or unauthorized access.

REMEMBER

Shadow IT refers to IT applications and services that are acquired and operated by end users without explicit organizational approval and often without organizational IT knowledge or support. Unsanctioned SaaS applications are literally exploding in number, and it's nearly impossible to keep up with this growth in terms of visibility and control.

Many organizations depend on CASBs to gain visibility into SaaS application usage (both sanctioned and shadow IT), understand where their sensitive data resides, enforce company policies for user access, and protect their data from unintentional loss and threat actors. CASBs are cloud-based security policy enforcement points that provide a gateway for your SaaS provider and your employees.

The problem with legacy CASBs

Legacy CASB approaches to securing SaaS applications only partially address modern problems, leaving organizations exposed and vulnerable due to several critical limitations:

- **They're unable to keep pace with the growth of SaaS and GenAI apps.** Legacy CASBs are focused on scanning web traffic, missing more than half of all SaaS traffic. They also rely on static signature-based databases and support requests for app discovery hindering their ability to identify and control new SaaS applications. Limited visibility into shadow IT leads to security gaps.
- **They provide inaccurate data loss protection.** These solutions typically protect only data that goes through a proxy. They use separate tools and policies for SaaS and other control points and often deliver inaccurate pattern-based detection that requires significant manual tuning. Outdated detection and classification methods produce excessive false positives, which can result in incident triage fatigue and poor user experience. This is only exacerbated by the increasing use of unstructured sensitive data exchanges within SaaS collaboration apps and AI platforms.
- **They have inadequate threat detection and management capabilities**. Security, unfortunately, has always been a checkbox in legacy CASB, with the majority of vendors using third-party or ineffective sandboxing as the only threat detection method. With new malware strains, phishing kits, man-in-the-middle techniques, as-a-service offerings, and AI-generated threats, traditional security methods are insufficient.

In addition, legacy CASB products were designed with complex architectural constraints that introduce potential chokepoints. They use a stand-alone proxy designed to perform a limited amount of inline inspection capabilities, in addition to application programming interface (API)–based controls for introspective SaaS application security. Threat protection and DLP capabilities are siloed and not tightly integrated with the overall existing network implementation, requiring additional labor and expense to manage disjointed policies and multiple consoles to perform incident triage.

SaaS security


TIP

A modern SaaS security solution (or next-generation CASB) should be natively integrated into SASE as a core capability for comprehensive SaaS application security and DLP. An integrated SASE solution helps you understand which SaaS apps are being

used and where enterprise data is going or stored, no matter where users are located, delivering the following outcomes:

- **Ability to keep up with SaaS application growth and its risks:** Organizations require a solution that automatically detects all SaaS apps in use. Visibility should extend to GenAI apps with the ability to identify risks, such as excessive user permissions, app misconfigurations, and compliance violations. A modern SaaS security solution should also provide centralized, robust, and easy-to-use policy management to define and enforce access controls based on user roles and responsibilities. This includes the ability to detect deviations from established policies in real time and enable swift corrective actions.
- **Accurate sensitive data detection and protection:** Organizations need the ability to continuously monitor for sensitive data loss across all SaaS apps. In addition to properly identifying and classifying sensitive data, the ability to automatically generate end-user alerts, produce detailed reporting, and take action in real time is also important. Organizations seek the ability to not only process vast volumes of structured and unstructured sensitive data, but do it accurately to reduce false positives and minimize the impact to employees.
- **Advanced protection from internal and external threats:** Organizations want the ability to enforce Zero Trust security with access controls and usage strictly based on user roles and context to prevent insider threats and possible adversaries already inside SaaS environments. Automated threat detection and response capabilities that leverage AI and machine learning (ML) will uncover modern threats.

Here's a checklist of solution capabilities that organizations should consider:

- Visibility into sanctioned and tolerated SaaS applications
- Continuous discovery and control of new and unsanctioned SaaS apps (shadow IT/AI)
- The ability to monitor and assess application usage and risk
- User access control, permissions monitoring, and protection from app misconfigurations

- Compliance-related application attributes, reporting, and remediation
- ML- and AI-powered data discovery and classification for high detection accuracy
- Advanced data discovery models using techniques such as natural language processing (NLP), exact data matching, indexed document matching, and optical character recognition
- Access control for managed and unmanaged devices
- End-user notifications to coach users and provide exemption workflows
- Integrated threat protection to stop known, unknown, and zero-day attacks
- DLP to block sensitive data transfers to SaaS and GenAI apps
- Centralized command center for holistic visibility and streamlined data and security operations to accelerate incident response and remediation

A comprehensive SASE solution includes SaaS security and DLP from a single integrated service. Organizations can improve their SaaS security posture, protect data in the cloud, encourage safe employee behavior, and defend against sophisticated threats as part of an integration platform. What's more, an integrated SASE solution avoids multiple gateways for consistent security enforcement, improves the user experience, and simplifies operations through a unified management console.

Deploying Firewall as a Service

Firewalls were originally designed to protect on-site company networks, but as more companies moved their applications and data to the cloud, firewalls had to evolve. Now, FWaaS enables firewall capabilities to be delivered as a cloud service.

In the past, organizations ran all their applications and data in on-site data centers and used a perimeter-based defense to secure their networks, with on-premises firewalls serving as the main security checkpoints. As companies moved to the cloud, adding more company- and employee-owned devices to their networks,

and began using more SaaS applications and data hosted on third-party infrastructure, they quickly discovered they no longer had clearly defined perimeters.

They also found that because many of their applications and data were now being run and managed on third-party infrastructure, they no longer had full visibility into, or control over, their entire networks. This problem was further exacerbated by the proliferation of third-party point products that had to be separately managed, forcing many organizations to completely rethink their approach to network security.

FWaaS is a deployment method for delivering a firewall as a cloud-based service. FWaaS has the same features of next-generation firewalls, but it's implemented in the cloud. Moving the firewall to the cloud provides cost savings by eliminating the need to install or maintain security hardware or software firewalls across their entire organization and more important, scale with their rapidly evolving environment.

The FWaaS approach enables organizations to:

- Aggregate all traffic from multiple sources (for example, on-site data centers, branch offices, remote users, and private or public cloud infrastructure) into the cloud
- Consistently apply and enforce security policies across all locations and users
- Gain total visibility into and control over their networks without having to deploy costly physical appliances

TIP

A company with 500 employees can expect to save 37 percent, on average, by using FWaaS solutions versus traditional hardware, according to Secure Data.

A SASE solution incorporates FWaaS into its unified platform, providing the same services as a next-generation firewall but as a cloud-delivered service. By encompassing the FWaaS service model within a SASE framework, organizations can easily manage their deployments from a single platform.

REMEMBER

A SASE solution should harness FWaaS capabilities to provide the protection of a next-generation firewall in the cloud. It's important to ensure your SASE solution doesn't just provide basic port blocking or minimal firewall protections. You need the capabilities of a next-generation firewall, as well as cloud-based security services, such as threat prevention services and DNS security.

Implementing Data Loss Prevention

Companies are processing massive amounts of data in more places than ever — in offices, multiple SaaS applications, email services, endpoints, enterprise browsers, and cloud storage environments. Thanks to cloud and mobile computing technologies, employees can directly access applications and data anytime, anywhere, from any device.

Accessing data from anywhere introduces some data protection challenges, including an increase in data breaches by insider threats, lack of visibility into where sensitive or regulated data is located and shared, and ineffective and inconsistent security. Companies need a solid data protection strategy to overcome these challenges. DLP protects sensitive data from loss, unwanted exposure, and theft, and it directly supports compliance and data privacy initiatives.

REMEMBER

DLP allows a company to discover and classify all its sensitive data consistently across all repositories and communication vectors, such as Box, Microsoft 365, Slack, corporate devices, and network traffic. DLP allows the usage of sensitive data to be monitored, detecting potential abuse or overexposure. It also protects sensitive data and proactively prevents data leakage.

TIP

For DLP to be effective, companies must:

- Protect their data across their networks, clouds, and users, including SaaS applications, cloud storage, email, endpoints, and network traffic
- Optimize their DLP deployment and management efforts

- Discover, classify, monitor, and protect all their sensitive data, such as personally identifiable information (PII) and intellectual property
- Clearly define and enforce protection and compliance policies in order to detect data exposure and violations
- Ensure that their data is being stored, accessed, and used in a way that complies with regulations and privacy laws, such as the European Union General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), U.S. Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS)

REMEMBER

DLP is a necessary tool to protect sensitive data and ensure compliance throughout the organization. Traditionally a composite solution monitoring data within the environments where it's deployed, DLP becomes a single cloud-delivered solution centered around the data itself with SASE. It consistently applies policies to sensitive data at rest, in motion, and in use, regardless of its location. With SASE, organizations can finally enable a comprehensive data protection solution, relying on a scalable and simple architecture and enabling effective ML by leveraging access to all the organization's traffic and data.

Securing DNS

Each device connected to the internet has an Internet Protocol (IP) address. The DNS is a protocol that translates a user-friendly domain name, such as `www.paloaltonetworks.com`, to an IP address — in this case, 199.167.52.137. DNS is ubiquitous across the internet. Without it, we'd have to memorize random strings of numbers, which our brains aren't equipped to do very well.

DNS carries a tremendous amount of bidirectional traffic, making it difficult to inspect and detect malicious activity. As a result, threat actors abuse DNS, using it to exfiltrate sensitive data, malware delivery, phishing, and more (see Figure 4-2). Palo Alto Networks offers two times more DNS-layer threat coverage than its competitors.

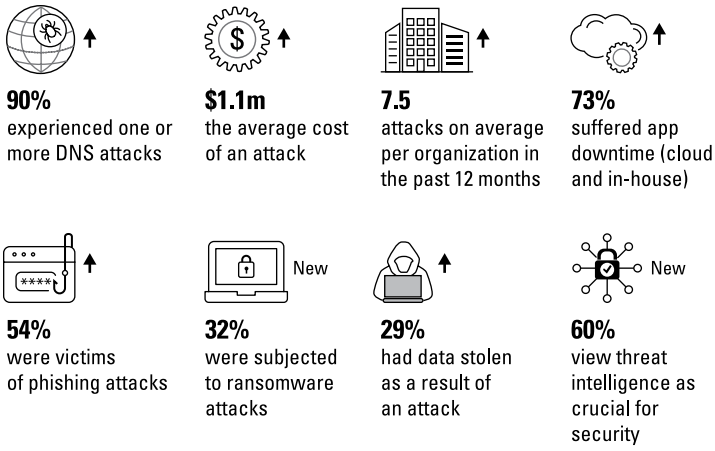


FIGURE 4-2: DNS is a key component of any comprehensive cybersecurity strategy.

DNS is a massive and often overlooked attack surface present in every organization. According to the Palo Alto Networks Unit 42 threat research team, up to 85 percent of malware uses DNS to initiate C2 communications. Unfortunately, security teams often lack basic visibility into how threats use DNS to maintain control of infected devices. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack, including reliable C2.

Security teams struggle to keep up with new malicious domains and enforce consistent protections for millions of emerging domains at once. It's impossible for enterprise network and security teams to keep up with the high volume of malicious domains, let alone advanced tactics like DNS tunneling for stealthy data theft.

DNS security protects users by detecting and blocking malicious domains used for phishing, malware, ransomware, and much more. A SASE solution that embraces DNS security capabilities and allows organizations to deliver safe access to the web for their users. Key capabilities include:

- **Automatically protecting against millions of malicious domains everyday with real-time analysis and continuously growing, global threat intelligence:** Rich and diverse

threat insights provide predictive analytics to help prevent new and emerging DNS-layer threats. Threat coverage continues to grow with a network effect of shared threat intelligence that allows organizations to:

- Prevent malicious domains used for establishing C2 channels, phishing, ransomware, malware, and data theft
- Obtain passive DNS and device telemetry to understand domain resolution history
- Benefit from threat research that provides human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots

» **Stopping threat actors that leverage domain generation algorithms (DGAs) to generate malware-hosting domains with rapid scale and speed:** The use of DGAs continues to grow, limiting the effectiveness of signature databases, which can only blocking known threats. DGAs create a list of randomly generated domains that can be used for C2, malware, phishing, and so on, which can overwhelm the signature capability of traditional security approaches. Modern DNS security solutions must combat this technique by using:

- Real-time inspection powered by ML and deep learning to detect new and never-before-seen malicious domains
- Seamless policy configuration for dynamic action to block malicious domains or sinkhole DNS queries
- Historical context of a domain to identify attributes that can be deemed malicious (that is, short-lived domains)

REMEMBER

Your SASE solution should provide DNS security delivered from the cloud and should be natively integrated rather than bolted on to your existing security architecture. The DNS security provided in your SASE solution should leverage a combination of predictive analytics, AI, rich threat insights, and automation to combat the latest and most sophisticated DNS-layer threats.

DNS-BASED ATTACKS

The SolarWinds supply chain attack became one of the most significant cybersecurity events at the end of 2020, impacting both commercial and government organizations worldwide. The DNS attack targeted SolarWinds Orion software with dormant malicious code that SolarWinds unknowingly sent out with a software update. The code resulted in hackers gaining access to IT systems, where more malware was then installed.

The attack used the SUNBURST Trojan, which uses DNS tunneling to receive commands from the adversary and exfiltrate data. The malware periodically contacted its C2 domain to report statuses and receive commands. When the C2 domain woke up from the incubation period, the majority of burst DNS requests were for new subdomains. The Trojan dynamically constructed these hostnames with *domain generation algorithms* (DGAs) to exfiltrate data. The DGA strings were encoded victims' identities, containing the infected organizations' domain names and security product statuses. When the attacker's DNS resolver received requests for these hostnames, it returned CNAME responses pointing to different C2 servers based on the exfiltrated information.

The SolarWinds supply chain attack leveraged DGA subdomains to exfiltrate data and provided a proxy layer for the attacking infrastructure.

Protecting Networks from Threats

The dynamic nature of public cloud usage and user mobility requires security teams to adapt and embrace a new approach to threat prevention. According to Palo Alto Networks research, threat detection and response is more difficult today than ever before because:

- There is a 73 percent year-over-year increase in red team tools to establish C2 channels.
- More than half a million (560,000) new malware variants are seen every day.

- There is an 1,100 percent increase in SaaS-hosted phishing attacks.
- More than 150 million malicious domains are seen per day.
- There is a 470 percent year-over-year increase in SaaS-based attacks.
- Fifty-five percent of employees use unapproved AI tools at work.

In today's world of small- and large-scale breaches, threat prevention is key to protecting your organization's data and employees. A variety of threat prevention tools exist, from anti-malware and intrusion prevention to Secure Sockets Layer (SSL) decryption and file blocking, providing organizations ways to block threats. However, these point products require separate solutions, making management and integration difficult.

A SASE solution integrates all these point products and services into a single cloud platform. This provides simplified management and oversight of all threats and vulnerabilities across your network and cloud environments.

Stopping exploits and malware by using the rich and diverse threat intelligence is crucial to protecting your network. Your SASE solution should incorporate threat prevention capabilities into its service so you can stop new and emerging threats and prevent patient zero. Be sure to check the quality of threat intelligence that's being provided by the vendor. The vendor should gather and share data from various sources, including customers, vendors, and other relevant thought leaders, to provide continuous protection from unknown threats.

REMEMBER

Continuous and effective threat prevention, detection, and automated response across your environment requires the following:

- Granular visibility into your users, apps, and data
- ATP over the network
- Threat detection and analysis by correlating risky configurations, anomalous user and network activity, host vulnerabilities, and threat intelligence gathered from multiple data sources
- Automated response to simplify security event triage
- Cloud context to expedite security investigations

IN THIS CHAPTER

- Understanding the role and security risks of the browser in the workspace
- Securing the workspace and access to corporate resources with the browser
- Introducing the secure browser and how it secures the browser-based workspace
- Knowing what to look for in a secure browser

Chapter 5
The Secure Browser

The secure browser is the latest feature that's an integral part of any comprehensive secure access service edge (SASE) solution. It's key in safeguarding the browser-based workspace on any device.

In this chapter, you discover the role the browser plays in the workspace, why secure browsers secure the workspace better than standard enterprise browsers, common use cases for a secure browser, and a checklist of key features that a secure browser needs to have.

Understanding the Browser's Role in the Modern Workspace

The browser is where work happens. It's the primary hub of productivity. In fact, more than 85 percent of a worker's day is spent in the browser, according to a study conducted by Palo Alto Networks in collaboration with the market research firm Omdia. The browser plays a central role in giving workers access to business-critical applications, such as Microsoft 365, Google Workspace, and Salesforce. These applications, as well as sensitive

information, are being accessed by users through the browser. The browser is also the gateway to corporate resources for independent workers, like contractors and third parties, as well as employees who perform work on their personal devices.

Recognizing the Risks the Browser Poses to Your Workspace

The reliance on the browser for day-to-day work introduces security risks and vulnerabilities. Browsers are a focal point for cyber threats. The study mentioned in the preceding section found that 95 percent of organizations reported a security incident originating in the browser, which highlights how the browser is a primary target for cyber threats.

Here are the largest risks that browsers face:

- **Phishing attacks generated by artificial intelligence (AI) and hosted on software as a service (SaaS) applications:** AI and SaaS applications are now being used to power phishing attacks on victims working on the browser. Generative AI (GenAI) can create unknown variants of malicious web attack code at a massive scale, generate convincing content for emails and web pages, and generate deepfake media to deceive victims. SaaS applications can be exploited to host malicious websites and manipulate URLs behind trusted SaaS sites to evade detection.
- **Advanced malware:** Encryption and AI-based code generation can obfuscate malware, improving the ability to evade detection. Advanced in-memory loading and execution techniques further make modern malware invisible, potentially bypassing detection on browsers.
- **Information loss:** Users may accidentally or intentionally share confidential information through entering information into insecure websites, falling victim to phishing attacks. Users may also download and upload files to unapproved locations and accounts, and screenshot or copy and paste confidential data.
- **Unmanaged devices:** An unmanaged device, such as a personal laptop or contractor device, is a device that is not

actively managed or secured by your organization's IT and security departments. This means the device may not be accounted for in an asset inventory and setup to the same security standards as a managed device. Unmanaged devices may lack the proper security controls and monitoring capabilities, increasing the attack surface and leaving the workspace vulnerable.

Securing the Browser-Based Workspace with a Secure Browser

Secure browsers address the security risks that browsers bring to your user's workspace and your corporate resources. Secure browsers are purpose-built to protect the browser-based workspace. They offer a variety of features that help organizations reduce the risk of cyberattacks, data leakage, and insider threats. Let's take a look at some of those security features.

Anti-phishing and anti-malware protection

The rise of AI-generated phishing attacks and advanced anti-malware necessitates the need for advanced and modern anti-phishing and anti-malware technology. These modern anti-phishing and anti-malware capabilities should be delivered to the browser to help protect the user's workspace from threats.

Necessary capabilities should include the ability to block new and unknown malware variants, inline real-time analysis that inspects user web traffic, and the ability to find phishing attacks that hide from signature-based approaches. Inline machine learning and AI should be leveraged to further improve the ability to detect new malware variants and modern phishing attacks that try to hide from signature-based anti-phishing approaches.

Data loss prevention

A secure browser needs to protect against information loss by implementing data loss prevention (DLP) capabilities. These DLP capabilities should be built into the browser.

Capabilities to protect against information loss ensure that sensitive information is passed only between approved channels and is not leaked through user actions, either intentionally or accidentally. They include the following:

- Masking sensitive data dynamically based on content and context
- Preventing user actions like screenshotting, copy/pasting, screensharing via collaboration tools, and printing
- Managing file transfers for downloads and uploads between corporate applications and personal drives with restrictions based on content and source

Protecting against compromised endpoints

Organizations that enable a bring your own device (BYOD) policy for employees or have outside collaborators like contractors, independent workers, and third parties need to secure the workspace on unmanaged devices. Personal and unmanaged devices may not be up to the same security standard that your organization has set and may be compromised with malware that target work on the browser, including keyloggers and screen scrapers. Secure browsers protect the workspace on unmanaged devices using the following capabilities:

- **Protecting the browser assets stored within the device:** This includes stored information like cookies, browsing history, and saved passwords. A secure browser adds an additional encryption layer to protect these assets. These assets are encrypted with a key that is independent of the device's operating system, protecting the assets from attackers. A secure browser also implements security measures to counteract spoofing attempts.
- **Defending the browser-based workspace against endpoint malware:** Built-in keylogger and screen scraper protection protects the browser against malware in the compromised endpoint.

- **Preventing insider tampering with the browser memory:** Controls protect the browser memory from tampering during runtime. This ensures the integrity of runtime operations.
- **Disabling or controlling certain browser components on websites that are deemed untrusted:** A secure browser also has full control over installed extensions and their permissions to ensure that extension access to sensitive information is strictly managed and controlled.

All of these capabilities are tied together with continuous device posture checks, continuous security inspections of the device, and continuous trust verification to consistently check if the device is secure.

Boosting visibility and control

A secure browser with the right features is able to boost visibility and control. Secure browsers offer deep visibility into browser activities for security, forensics, and compliance. IT teams can leverage secure browser capabilities to monitor user activities, centralize browser management in a single platform, give security teams a comprehensive view of web activities with incident monitoring, and allow for easy logging and control of all events for threat hunting and forensics.

Secure browsers offer greater control than consumer browsers by giving administrators the ability to set granular data policies and apply last-mile data, identity, and access controls on selected applications. Administrators can implement Zero Trust policies across selected actions and applications based on application and user context.

Extending SASE to any device

With the right SASE vendor, a secure browser can be natively integrated into a SASE solution. This means SASE's protective reach can be extended to any device anywhere in minutes and bring consistent visibility, control, and security to web applications on any device. A SASE-native secure browser increases IT and business agility and unifies visibility across any device for comprehensive oversight.

ENTERPRISE BROWSERS VERSUS SECURE BROWSERS

Enterprise browsers provide a secure, managed browser environment designed for businesses. They offer enhanced security, control, and features for workplace use. They typically enforce IT policies, control access to business-critical applications and resources, and provide monitoring capabilities for enhanced security.

Although standard enterprise browsers are better for improving business productivity and securing the workspace than consumer browsers, some enterprise browsers may not be adequate enough to fully secure the workspace against advanced cyber threats.

Secure browsers leverage advanced security features, powered by AI, to better secure the workspace on the browser against cyber threats, namely phishing attacks and malware. They implement more advanced security features compared to standard enterprise browsers and are designed to better defend the browser against modern, advanced cyber threats.

Boosting Employee Productivity with a Secure Browser

A secure browser can not only protect your organization from phishing attacks, malware, and data loss, but also boost employee productivity by:

- **Ensuring a familiar browser experience:** A major roadblock when it comes to implementing new security measures or adopting new security technology is impact on the user experience. Impact on the user experience can lead to disgruntled employees and motivation to try bypassing the new measures or technology. The right secure browser provides a familiar browser experience, similar to the experience found on standard consumer browsers.
- **Being easy to set up:** One of the major benefits of leveraging a secure browser is the ease of setup and user provisioning. A secure browser is easy to set up — it's a simple

download with no admin privileges required. After the secure browser is open, users simply have to log in and authenticate and they're ready to start browsing. Onboarding and offboarding users takes only minutes, and granular policies can be applied across defined user groups.

Identifying Key Use Cases for a Secure Browser

Still not convinced of the importance of a secure browser? Let's take a look at a few key use cases.

VDI and DaaS reduction

Virtual desktop infrastructure (VDI) and desktop as a service (DaaS) are used to provide remote access to corporate resources by hosting virtual desktops on servers. They provide organizations a greater amount of security and control with access to consistent desktop environments from various devices.

However, these solutions suffer from a number of drawbacks:

- **High cost:** VDI and DaaS require substantial investments in hardware and software and ongoing maintenance.
- **Complexity:** Setting up and managing VDI and DaaS environments is complex, with specialized IT skills and substantial resources required.
- **Performance issues:** Latency and performance issues are a major problem. This problem is exacerbated when accessing resource-intensive applications remotely.
- **Scalability:** Scalability is challenging. Increasing the number of remote users is costly and difficult for VDI and DaaS solutions.
- **Security gaps:** VDI and DaaS often don't properly secure web applications. Cyber threats like phishing attacks and ransomware are delivered through web applications like email, which VDI and DaaS solutions may not address.

A secure browser solves the challenges that VDI and DaaS solutions present. Secure browsers with the right features are cost-effective solutions that are easy to set up. They provide great performance and the ability to easily scale to a growing number of users. They also implement security measures to protect the workspace within the browser, defending against the potential security gaps like phishing attacks and ransomware delivered through web applications that VDI and DaaS may miss.

Reduction in shipping laptops

Shipping laptops improves security in an organization that employs outside collaborators and allows for remote and hybrid work. This solves the issue of unmanaged devices. Shipping laptops, however, is very expensive, time-consuming, and unscalable. The process for shipping laptops includes procuring new devices, provisioning all of them with the appropriate security features, distributing them to the right employees, and requiring employees to perform final onboarding and setup with IT assistance. This process can take weeks, with productivity heavily diminished.

A secure browser, able to be set up and provisioned in a matter of minutes, solves challenges that shipping laptops have, as shown in Figure 5-1. Secure browsers are very scalable, simply requiring a download and sign-in with a single sign-on (SSO) provider. They're also cost-effective, requiring minimal hardware costs and overall maintenance.

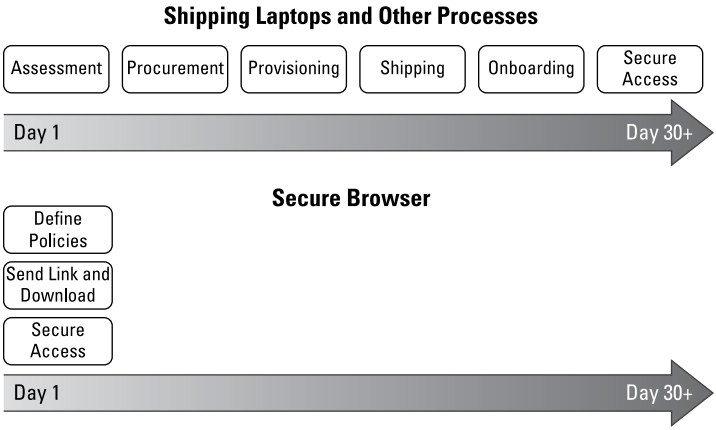


FIGURE 5-1: Secure browsers reduce the cost of shipping laptops.

Securing BYOD policies

BYOD policies are becoming more prevalent with the rise of hybrid and remote work. BYOD policies can boost flexibility and improve employee satisfaction. They can also, however, introduce security risk to the corporate IT ecosystem, increase attack surface, and increase the number of unmanaged devices being used to access critical business applications and sensitive information.

CASE STUDY: ACCELERATING SECURE ACCESS DURING AN ACQUISITION

A secure browser delivers secure user access to corporate resources while providing a great user experience and accelerating the onboarding process. A telecommunications company was able to onboard 650 global employees from an acquisition in minutes per employee with no loss in productivity with a secure browser.

It needed:

- A solution to quickly connect more than 650 new employees in 30 countries to critical business applications
- To allow new employees to work securely and productively from day one
- To secure the browser-based workspace against advanced cyber threats

A SASE-native secure browser helped the company to:

- Onboard and provision each of the 650 new employees in minutes per user
- Save $1.9 million on manual configuration and maintenance
- Extend strong security capabilities and Zero Trust to all employees
- Deliver an intuitive user experience with zero learning curve

Secure browsers enhance BYOD policies, enabling the rapid onboarding and offboarding of personal devices used by employees and extending advanced security capabilities to unmanaged devices. On unmanaged devices, work on the browser is secured against cyber threats that originate from the web, the endpoint, or insider risk. Secure browsers allow IT administrators to deploy granular policies that are tailored to specific job functions and roles, meaning employees can use their own devices to work securely while getting access to the resources they need to be fully productive.

Secure browsers fully secure work for BYOD while ensuring that employees are able to get access to all the business-critical applications and sensitive information to be fully productive.

IN THIS CHAPTER

- Understanding the user experience challenges that organizations face
- Identifying the key requirements for user experience monitoring
- Realizing the value of SASE native DEM

Chapter 6
Digital Experience Monitoring

In this chapter, you find out about the user experience monitoring capabilities of a secure access service edge (SASE) solution. Security and connectivity are important, but having exceptional user experience is key because it impacts productivity and operations.

User Experience Challenges

The concept of the "corporate network" has greatly expanded, providing more work for IT teams and increased opportunity for employees to get frustrated when they can't access the tools they need to do their jobs. Employees need consistency in both security and user experience across branch offices, home setups, and remote locations. IT teams need complete visibility into their workplace's end-user experience in order to support employees when performance problems arise.

Many businesses face the following user experience challenges:

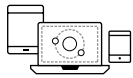
- **Security and user experience are seen as a trade-off.** Legacy networking and security architectures rely on backhauling all traffic to corporate data centers. This forces network administrators to choose between security and performance for their users.
- **There's a gap between what users experience and what IT sees.** With corporate resources distributed across public clouds, software as a service (SaaS), and corporate data centers, IT teams struggle to identify and diagnose application performance degradation. The hybrid workplace presents additional challenges as the plethora of home routers, Wi-Fi networks, and internet service providers (ISPs) introduce additional points of impact where IT has no visibility and control.
- **Existing monitoring approaches aren't SASE native and leave you in the dark.** Legacy monitoring solutions weren't designed for a hybrid workplace. They provide only a fraction of the visibility needed into true end-user experience and often require additional software or hardware.

Together, these factors have contributed to costly troubleshooting processes, loss of productivity, and poor user experiences in today's hybrid workplace. Digital experience monitoring (DEM) solutions used for network, endpoint, and application monitoring provide siloed visibility into their respective domains but lack the context of the overall SASE environment, making it difficult to troubleshoot effectively.

According to research by Palo Alto Networks (see Figure 6-1), cybersecurity is a priority for leadership teams, but there is still room for improvement, which can be seen by the following:

- Eighty-nine percent say cybersecurity is on their board's agenda at least once a quarter.
- Sixty-two percent believe their board's recognition of cyber risk has increased only marginally alongside the acceleration of digital transformation initiatives.
- Thirty-seven percent of respondents say lack of executive alignment on prioritizing cybersecurity is one of the top three challenges across their organization.

89% say cybersecurity is on their boards' agenda at least once a quarter



62% believe their boards' recognition of cyber risk has only marginally increased alongside the acceleration of digital transformation initiatives

37% of respondents say lack of executive alignment on prioritizing cybersecurity is one of the top three challenges across their organization

FIGURE 6-1: Cybersecurity is a priority for leadership teams.

Managing the digital experience

DEM is an established IT category that addresses user experience — human or machine — across every dependency, whether network or service, inside or outside your company.

DEM technologies monitor the availability, performance, and quality of experience an end user or digital agent receives as they interact with an application and the supporting infrastructure. Users can be external consumers of a service (such as patrons of a retail website), internal employees accessing corporate tools (such as a benefits management system), or a combination of both. DEM technologies seek to observe and model the behavior of users as a continuous flow of interactions in the form of user journeys.

But digital experience increasingly depends on a host of external services (like cloud, SaaS, and the internet) that you don't own or directly control. You may not own all the underlying infrastructure, but you still own user experience. A comprehensive DEM solution includes the following monitoring approaches:

- **Endpoint monitoring:** Includes the collection of information about things like central processing unit (CPU) utilization, memory usage, and Wi-Fi signal strength to determine the negative impact those things may be having on a user's digital experience.
- **Real-user monitoring (RUM):** Tracks performance based on data coming from actual users. RUM is a reliable technique for monitoring how the application is being used and how real-world parameters such as network latency, device variation, and so on affect the end-user experience.

- **Synthetic monitoring:** Includes running regular tests from a source to a destination, or from a user to an application, that allow IT to monitor network and application service performance even when they aren't being used. Synthetic monitoring enables IT to understand the performance of assets they don't own and can't instrument, like SaaS applications and user ISPs. With synthetic monitoring, IT can easily diagnose a problem, because they have a baseline of app performance that enables them to pinpoint when and where the performance bottleneck is, like a network outage. Synthetic monitoring is one of the most critical technical components of DEM.

Automating DEM

As organizations continue their digital transformation, leaders in infrastructure and operations (I&O) are finding it more and more important to share business metrics based on digital experience. Consequently, digital experience monitoring has become indispensable for reaching key business outcomes.

When AI-driven *autonomous digital experience management* (ADEM) capabilities are integrated into a SASE solution, organizations benefit from proactive issue detection and intelligent remediation, enhancing their overall operational efficiency.

REMEMBER

ADEM enhances your IT team's tasks with easy-to-use, single-pane visibility that leverages endpoint, simulated, and real-time user traffic data to provide the most complete picture of user traffic flows possible.

Modern ADEM should provide businesses with the following:

- **SASE-native DEM:** DEM capabilities are natively integrated into a SASE solution to optimize experiences for every user, working from anywhere, without the complexity of installing additional software or hardware. Native integration offers effortless management and supports scalability as organizational needs evolve.
- **Segment-wise insights:** Analysts can view every segment in the application delivery path for all users — in a branch office or at home — to help find root causes fast and expedite troubleshooting.

- **Comprehensive visibility:** A unified view into the entire user experience journey requires performance end-to-end insights from endpoint devices, networks, and applications — all from one dashboard. Only with these insights will you have a true end-to-end view of everything that affects digital employee experience and productivity.

With ADEM, IT and security teams have the advantage of centrally implementing and monitoring remote access security policies and user experience for their hybrid workforces through a single pane of glass. And when capabilities are natively integrated with a SASE solution, no additional agents are required and no additional burden is placed on the user.

WARNING

Don't be fooled by complex monitoring solutions that require additional agents to be installed on end-user devices.

Identifying the key benefits of ADEM

The best business decisions are made when an organization views and understands its service from the end user's point of view. ADEM helps quickly pinpoint issues and deliver great digital experiences for every user, so IT can stop guessing what the problems are and start optimizing.

TIP

Stop guessing and start optimizing. Use a unified platform, with a single pane of glass, to give teams the precise, automated insights and context they need to proactively deliver better user experiences and drive better business outcomes.

SASE native digital experience monitoring offers companies the following benefits:

- **An integrated solution:** Organizations can have a fully integrated SASE solution with unified management of both mobile users and remote/branch networks without adding additional software or hardware.
- **Reduced ticket volume:** Proactive, synthetic monitoring approaches, in addition to real user visibility and remediation driven by artificial intelligence (AI), help address tickets before they're reported, and often, before users are even impacted.

- **Reduced time to isolate problems:** A single dashboard for network, application, and desktop support lets analysts quickly see and resolve user problems with precision, regardless of their location.
- **Increased efficiency:** With visibility and the right insights to quickly determine root causes, teams can stop finger-pointing and wasting hours on issue validation.
- **Predictive capacity planning:** ADEM leverages predictive analytics to forecast capacity requirements, enabling organizations to proactively scale resources and prevent performance bottlenecks as they grow.
- **Empowered users and IT teams:** The best ADEM solutions enable end users to resolve common issues independently through self-service capabilities, while IT teams benefit from AI-assisted tools that streamline operations and reduce the burden of routine tasks.

Seeing How SASE Native Monitoring Adds Value

Monitoring provides value across the organization, assisting both IT teams and end users — from outages outside an organization to common user device problems. With user experience monitoring, there is no longer any need for IT to rely on manual processes to identify and mitigate potential issues or use monitoring methods that provide only a fraction of the required visibility needed to troubleshoot effectively. Here are a few examples of how SASE native digital experience monitoring can add value.

Quickly identifying and resolving end-user device issues

With a single pane of glass into the SASE environment, IT can quickly identify and locate an issue, narrowing it down to an individual user device. For example, a user working at home using their home Wi-Fi may end up moving around in their house. In some areas of the house, the user may encounter low signal strength, which in turn negatively impacts their application experience. Another scenario may find a user performing an

operating system upgrade, or an upgrade starting without the user's knowledge. In either case, this event may result in high CPU usage. Monitoring capabilities would be able to observe that a user's new operating system (OS) software install/update resulted in high CPU usage, which in turn would negatively impact performance on user applications.

This level of visibility ensures that operations teams can significantly reduce the amount of time needed to locate and fix an issue that's impacting user experience. IT can determine if internet connections or endpoint devices are causing issues and proactively notify users of the potential problem.

Optimizing the hybrid workplace experience

Now that hybrid workplace is the norm, companies will need to continuously monitor every user's experience to make sure their user experience is always consistent as they shift between working from home, connecting over nontrusted networks, and working from the office over a trusted corporate campus network.

Monitoring capabilities offer deep insights and visibility into every part of the service delivery chain impacting user experience, including critical collaboration tools like videoconferencing and business instant messaging apps. That monitoring can include watching for device issues, home Wi-Fi and network issues, internet path issues, and issues with the applications itself. All that information can enable IT to quickly isolate problems and resolve issues for any user, working from anywhere.

Some advanced SASE solutions also have the ability to significantly improve user experience issues through the acceleration of key protocols, such as Transmission Control Protocol (TCP) and the intelligent acceleration of complex SaaS applications.

Monitoring the branch experience

Analysts need not only a unified view into user experience, but also visibility into remote offices located across the world. When monitoring capabilities are natively integrated into a software-defined wide area network (SD-WAN), organizations can monitor end-to-end user experiences for critical branch endpoints,

including Internet of Things (IoT) devices. This enables an administrator to view an application experience score on a per-path basis, whether that path is active or backup. When they're able to run proactive synthetics on every path, an administrator can recognize the best path, per application, for all users in a branch office. Without native integration into an SD-WAN, IT wouldn't be able to attain such comprehensive visibility.

Optimizing and gaining visibility into the browser experience

IT teams can gain real-time visibility into the user experience for every browser-based application with browser-based RUM. A unique combination of ADEM synthetics and browser-based RUM enables IT teams to perform precise root cause analysis from the user's environment to the application, leading to enhanced troubleshooting, faster remediation, and a better user experience. Insights that IT teams get access to through browser-based RUM include browser performance metrics like loading performance, interactivity, and visual stability.

IN THIS CHAPTER

- Getting full visibility and control of users, data, and apps
- Protecting the hybrid workforce and enabling consistent security
- Improving performance and aligning networking and security

Chapter 7
Ten Benefits of SASE

Thinking that secure access service edge (SASE) may be the right choice for your business? Here are ten important business and technical benefits of deploying SASE in your organization.

Complete Visibility across Hybrid Environments

SASE enables complete visibility of hybrid enterprise network environments that connect data centers, headquarters, branch and retail locations, public and private cloud, and users — no matter their location.

The combination of Zero Trust network access (ZTNA), secure web gateway (SWG), cloud access security broker (CASB), and firewall as a service (FWaaS) capabilities in SASE empower enterprise security teams with full visibility into all network activity in the environment, including users, data, and apps.

Greater Control

Users are increasingly leveraging a variety of applications — including SaaS applications from multiple devices and locations — for both work-related and personal purposes. Many applications, such as instant messaging (IM), peer-to-peer (P2P) file sharing, and Voice over Internet Protocol (VoIP), can operate on nonstandard ports or hopping ports. Users are increasingly savvy enough to force applications to run over nonstandard ports through protocols such as Remote Desktop Protocol (RDP) and Secure Shell (SSH), regardless of the organization's policy regarding various applications (sanctioned, tolerated, and unsanctioned).

SASE can classify traffic by application on all ports by default — and it doesn't create an administrative burden by requiring you to research which applications use which ports to configure appropriate policies and rules. SASE provides complete visibility into application usage along with capabilities to understand and control their use.

Better Monitoring and Reporting

SASE eliminates the need to monitor multiple consoles across different networking and security products and creates separate reports for key metrics. Monitoring and reporting can be done from a single pane of glass in SASE, which also helps networking and security teams correlate events and alerts to simplify troubleshooting and accelerate incident response.

Less Complexity

SASE enables your business to simplify networking and security by eliminating unnecessary limited use of siloed point security solutions and operating from the cloud to cut operational complexity and cost. SASE also enables your business to avoid logistical issues with shipping, installing, and upgrading multiple networking and security hardware devices to remote branch (or retail) locations.

Consistent Data Protection Everywhere

In a traditional Multiprotocol Label Switching (MPLS) wide area network (WAN), all traffic from branch and retail locations is backhauled to a headquarters or data center location. This basic design architecture eliminates the need for firewalls at branch and retail locations because all traffic can be inspected and a centralized security policy can be enforced by the perimeter firewall at the headquarters or data center location.

Consistent data protection is about consolidating data protection policies across every environment and data communication vector, eliminating disjointed data protection policies and configurations, which too often cause security blind spots, complex manageability, policy inconsistency, shadow IT, and shadow data. Instead, SASE enables a consistent data loss prevention (DLP) policy across every environment where data lives and flows. You can rapidly and easily deploy new security services and applications with specific security policies everywhere instead of having to individually manage them at each location.

Reduced Costs

Organizations may choose to invest in commodity point networking and security products. Although this may initially seem to be a less expensive solution, administrative costs will quickly grow out of control because limited networking and security staff resources must learn different management consoles and operating systems — many of which will potentially have very limited remote management capabilities.

SASE enables organizations to extend the networking and security stack to all their locations in a cost-effective manner via a converged, cloud-delivered solution that fully integrates networking and security capabilities and functions.

Lower Administrative Time and Effort

Managing multiple point networking and security products from different vendors in many locations is an administrative burden that few organizations can afford. The cost to train and retain

networking and security staff on a multitude of point networking and security products can quickly exceed the organization's capital investments for these products.

SASE enables single-pane-of-glass management of networking and security functions for all your locations in a consistent manner, which reduces the administrative burden and helps to lower training and retention costs.

Reducing the Need for Integration

SASE combines multiple networking and security capabilities and functions in a unified cloud-delivered solution, thereby eliminating the need for complex integrations between multiple point networking and security products from different vendors.

Better Network Performance and Reliability

SASE helps organizations improve network performance and reliability for all users and locations by delivering SD-WAN capabilities that enable multiple links from different sources to be load-balanced, aggregated, and configured for failover. This helps reduce congestion and latency associated with backhauling internet traffic across MPLS connections or routing traffic across a connection experiencing high utilization or performance issues.

Enhanced User Experience

User experience is key for productivity and employee satisfaction. Digital experience monitoring (DEM) helps identify and remediate user-experience problems before they impact employees, IT, and the business. With SASE, DEM improves operations and optimizes experiences for every user, working from home or from branch offices, without the complexity of installing additional software and hardware. Some advanced SASE solutions also have the ability to significantly accelerate applications, further improving overall user experience.

paloalto NETWORKS | PRISMA® SASE

Raise the bar on security with Prisma SASE.

Get to know the industry's most complete AI-powered SASE solution.

There's simply no better way to protect your growing hybrid workforce, accelerate digital transformation initiatives, and secure generative AI. In fact, Prisma® SASE is the only single-vendor SASE solution that can keep you ahead of the latest threats and deliver a superior user experience while fueling the innovation and productivity a modern business demands.

Prisma SASE provides Zero Trust security, exceptional network and user experience, and AI-powered operations. Learn more about Prisma SASE and how it can secure your business.

CONTACT US TODAY

Build your digital transformation on a SASE framework

A secure access service edge (SASE) solution offers comprehensive protection for all users, applications, data, and devices by integrating best-in-class security capabilities with a seamless user experience. It enables organizations to deliver consistent, secure access regardless of user location — whether supporting a remote, hybrid workforce or securing connectivity at a Zero Trust branch. By combining networking and security into a single, cloud-native service, SASE simplifies operations, enhances resilience, and ensures policy enforcement across distributed environments. Discover how implementing a SASE solution can enhance security, reduce complexity, and support your organization's long-term growth and agility.

Inside...

- Learn what a SASE solution is
- Discover ways to protect against emerging threats and secure GenAI apps
- Understand how to gain full visibility and control over users, apps, and data
- See how a SASE solution can simplify monitoring and reporting
- Learn why secure browsers are an integral part of SASE

paloalto NETWORKS

Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 150 *For Dummies* books on numerous technology and security topics.

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

ISBN: 978-1-394-30199-7
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.