Definitive Guide™ to *SASE Security*

A pragmatic approach to implementing a secure access service edge architecture

Crystal Bedell

FOREWORD BY:
Nick Edwards

Compliments of:
MENLO SECURITY

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security's isolation-powered Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions, and backed by Vista Equity Partners, Neuberger Berman, General Catalyst, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Mountain View, California. For more information, please visit www.menlosecurity.com.

Definitive Guide™ to *SASE Security*

A pragmatic approach to implementing a
secure access service edge architecture

Crystal Bedell

Foreword by Nick Edwards
Vice President, Product Management

CYBEREDGE
PRESS

Definitive Guide™ to SASE Security

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

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

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-1-948939-23-2 (Paperback)
ISBN: 978-1-948939-24-9 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Menlo Security Contributors: Mark Guntrip, Eric Schwake, Jonathan Lee

Table of Contents

Foreword

For decades we were accustomed to traveling to an office for work. Some of us enjoyed the commute, while others dreaded the idea of slogging through traffic. But in the blink of an eye, everything changed. Suddenly, we were all working from the same office: the home office.

The global pandemic caused businesses — from small and mid-sized companies to enterprises — to take a major detour that resulted in mandating work-from-home policies. The percentage of employees working remotely tripled from 19 to 61 percent as a result of the pandemic, according to research from analyst firm ESG. To ensure this remote workforce had every opportunity to remain productive, companies expedited digital transformation initiatives, and many looked to cloud technologies for the answer.

Employees spend most of their time working in the cloud. Why? Because critical tools like software-as-a-service (SaaS) applications and email are found there, too. With applications, data, and people serving as the key ingredients in this massive migration, it's become clear that the cloud is the backbone of remote work. Just about everything today happens in the cloud — except security.

Having people, data, and applications "everywhere" while confining security to an organization's perimeter has created a mismatch. The old ways of relaying traffic among multiple checkpoints, like firewalls and virtual private networks (VPNs), aren't sufficient to secure modern work. They interrupt traffic flow, increase the likelihood of vulnerabilities, and struggle to protect the new perimeter: users.

When security teams turned to VPNs to enable secure remote access, it quickly became clear that VPNs didn't scale, they hampered productivity, and they ultimately compromised security. Trying to shoehorn a security fix for a changed world into a legacy data center scheme simply doesn't work.

Securing this digital transformation is a race as the threat landscape becomes increasingly sophisticated. Today's hybrid

IT environments drastically expand attack surfaces that digital marauders have quickly exploited. And ransomware attacks...well, they've reached new heights with the help of ransomware-as-a-service providers.

The pandemic has forced security leaders not only to question some long-held security tenets, but also to revisit approaches and technologies that are not adequate to secure modern work in hybrid IT environments. That's why the secure access service edge (SASE) architecture is considered the gold-standard framework for enabling organizations to adapt to modern network architecture and securely enable digital transformation. Combining a SASE framework with a zero trust mindset ensures that all content a user comes across is suspect and should be subject to enterprise security controls. Together, SASE and zero trust solve the security problem of enabling secure access in a distributed environment.

The goal of SASE is to enable secure connectivity for any user, from any device, with a consistent experience while enforcing security policies on access. The converged security technologies featured in the framework aren't new. They're simply packaged together to dynamically create a policy-based secure access service edge that moves the security perimeter out of the confines of the data center.

Organizations looking to improve security for digital transformation will find the *Definitive Guide to SASE Security* provides valuable technology insights and a pragmatic path to securing modern work and protecting productivity.

Nick Edwards
Vice President of Product Management
Menlo Security

Introduction

Over the past several years, more and more IT assets have moved out of the on-premises data center and into the cloud, leaving behind a critical component of the IT infrastructure — security.

With applications, data, and endpoints potentially spread around the globe, cybersecurity teams face a formidable challenge: deliver secure access anywhere, anytime without impacting the user experience. This simply can't be done from the data center. Security must also move to the cloud. But it's not enough to lift and shift on-premises solutions to cloud instances. Security must be rearchitected to be as close to the user as possible while adhering to zero trust principles and eliminating web-borne risks.

That's where SASE (pronounced "sassy") comes in. Chances are good you've heard the acronym many times before. Secure access service edge (SASE) is touted by industry analysts, pundits, and vendors as the answer to securing remote access to today's highly distributed IT resources. But for all the talk, few experts have offered a pragmatic approach to deploying SASE – until now. This book provides an in-depth look at SASE: what it is, how it solves modern security challenges, and how to deploy it.

Chapters at a Glance

Chapter 1, "Coming to Terms with Today's Reality," discusses how recent changes to enterprise IT environments impact the traditional approach to security.

Chapter 2, "Introducing SASE, a Modern Security Framework," reviews what SASE is and the benefits of implementing the framework.

Chapter 3, "Understanding the SASE Framework," outlines the core capabilities and methodologies of a SASE architecture.

Chapter 4, "Deploying SASE," describes a pragmatic approach to implementing this framework, including how to overcome common roadblocks.

Chapter 5, "10 Considerations When Deploying a SASE Framework," explores the factors that go into deploying an effective, future-proof SASE architecture.

Helpful Icons

TIP

Tips provide practical advice that you can apply in your own organization.

DON'T FORGET

When you see this icon, take note as the related content contains key information that you won't want to forget.

CAUTION

Proceed with caution because if you don't it may prove costly to you and your organization.

TECH TALK

Content associated with this icon is more technical in nature and is intended for IT practitioners.

ON THE WEB

Want to learn more? Follow the corresponding URL to discover additional content available on the web.

Chapter 1

Coming to Terms with Today's Reality

In this chapter

- Learn how digital transformation initiatives have been impacted by the COVID-19 pandemic
- See how the browser became the new office
- Understand why the traditional approach to security is no longer operable in a modern IT environment

Ask an office worker to describe their work environment, and they're just as likely to describe a makeshift home office as an open floor plan with modern art and fluorescent lighting. Regardless of their surroundings, today's knowledge workers all "go" to the same place to accomplish work objectives: the Internet. In this chapter, we look at the drivers that helped transform the office from a physical location to a virtual connection, and their impact on the legacy castle-and-moat security model.

Full Speed Ahead!

How and where we work have changed dramatically and in a relatively short period of time. Practices and policies that organizations were cautiously implementing prior to 2020 were fast tracked when the global COVID-19 pandemic forced people to isolate and socially distance.

Digital transformation, accelerated

Most organizations began their digital transformations well before the pandemic. They were actively moving data and workloads to the cloud and adopting cloud-based services and applications. As quickly as resources moved outside the corporate perimeter, users followed — pushing the boundaries of remote work and bring your own device (BYOD) policies. However, few organizations were equipped to enable and support a fully remote workforce.

When isolation and social distancing mandates forced businesses to send workers home, digital transformation efforts accelerated. The use of both managed and unmanaged devices grew rapidly. The adoption of cloud-based applications expanded as IT organizations scrambled to enable employees to work from anywhere. The result: people, data, applications, and services all became highly distributed — and there's no going back.

DON'T FORGET

The pandemic highlighted the need for increased IT and business agility to improve resilience and accomplish more with limited resources. Cloud services and mobile device use allow organizations to deliver on these goals. Meanwhile, employees want the flexibility to continue to work from anywhere, at least part time, and security teams want to protect IT assets regardless of their location. The broad use of online collaboration tools as part of daily work patterns, the increased adoption of SaaS applications, and faster transition to public cloud infrastructure are all trends that show no sign of abating.

The browser is the new office

The office as a central location where employees go five days a week to conduct business is now the exception rather than the rule. Instead of physically traveling to the office, workers power on laptops from their kitchen tables, spare bedrooms, and local coffee shops. They share workspace with a beloved pet and fight family members or roommates for bandwidth on a network that's most likely less secure than the one in the corporate office.

DON'T FORGET

As we learned from the COVID-19 pandemic, conducting business no longer requires people to be in a space designated for that purpose. For most knowledge workers, conducting business simply requires an Internet browser — and they already have access to one anywhere and everywhere they go. For cloud-first companies and those born in the cloud, the

Internet is the corporate network and users are the new perimeter, as shown in Figure 1-1.

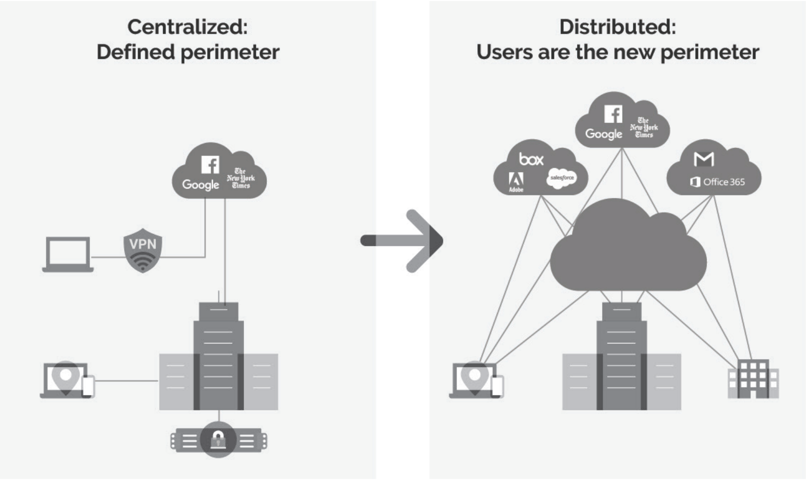

Figure 1-1: With people, data, applications, and services now highly distributed, users are the new perimeter.

Distributed… Everything

Thanks to the acceleration of digital transformation initiatives and widely embraced work-from-home practices, the IT environment and use cases look radically different from just a couple of short years ago. From our experience working with and talking to other companies, the following trends are emerging:

- Data is processed and stored in a variety of public and private cloud services.
- Users are accessing resources anytime, anywhere, from any device.
- More user work is performed off the enterprise network than on.
- More workloads run in infrastructure-as-a-service (IaaS) environments than in the enterprise data center.
- More applications are consumed as software-as-a-service (SaaS) solutions than as software running on enterprise infrastructure.
- More sensitive data resides outside the enterprise data center, in cloud services, than inside.
- More user traffic is destined for cloud services than the enterprise data center.
- More branch office traffic is heading to public clouds than to the data center.

Modern Security Challenges

While transformative changes like digitalization help businesses to modernize and respond to unforeseen challenges, they have also served to make security more difficult. Network security approaches have been slow to adapt, and traditional security models simply don't work.

Problems with the old way

Traditional network and network security infrastructure was built for the traditional castle-and-moat model with a defined network perimeter. In this legacy model, traffic is backhauled to a centralized, on-premises security stack where it is monitored and policies are applied. This approach worked when people, applications, and data were centralized in offices. However, it lacks the automation, scale, and intrinsic security needed to connect and protect applications, data, and users across a globally distributed business fabric.

CAUTION

The legacy data center-centric approach doesn't make sense anymore. Backhauling traffic through the data center is not cost-efficient if remote workers are accessing resources on the Internet. In addition to increasing operational costs, backhauling traffic impacts quality of service and the user experience. Latency and bandwidth issues cause slow performance and impact employee productivity — unacceptable conditions for the modern, competitive business environment. Users need fast, secure, and reliable access to applications whenever and wherever they happen to be.

These issues are exacerbated as enterprises expand their adoption of public cloud services and a growing, more-diverse workforce increases the complexity and scope of the cyberattack surface. For example, the number of third parties that need access to cloud-based resources has increased. Vendors and supply chain partners, contractors, affiliates, subsidiaries, and acquired entities commonly are granted access to some business systems, further increasing the need to provide secure access to cloud-based resources.

What we need today

TIP

With the continued migration of people, data, and applications to the cloud, it’s become clear that the traditional ways of implementing security and policies are no longer effective. Everything perimeter-based security was built for – the environment, the way data is used, and the way people work – has changed. To fully realize the promise of digital transformation projects, security must also make the journey to the cloud, putting it in close proximity to the people, data, and applications it is designed to protect.

Requirements for a modern security architecture

A modern security architecture must reflect the current reality of how we work and deliver IT services. To that end, security must:

☑ **Deliver secure remote access for a distributed workforce.** A modern approach requires automation, cloud scale, and intrinsic security to connect and protect applications, data, and users across a globally distributed business fabric.

☑ **Be invisible to the user.** If users can see security or feel it, they’ll try to work around it, but if security is invisible, then it just happens. See the sidebar on page 6 for a more detailed explanation of what it means for security to be invisible.

☑ **Manage traffic flow for an improved user experience.** The legacy approach of backhauling data is a problem from the perspective of both user experience and cost. A modern approach to security must make Internet access safe, seamless, and reliable without forcing users to jump through extra hoops.

What Is Required for Security to Be Invisible?

Most security professionals are familiar with the adage that you can’t protect what you can’t see. You need visibility into the environment and connected assets to manage, monitor, and secure them.

It’s the same idea for end users: they can’t circumvent what they can’t see. Your goal, then, is to make security invisible. That means the security architecture you implement requires no change in . . .

- work processes
- application performance
- data access
- devices supported
- browser experience

Bottom line: invisible security means users work unhindered. They have no reason to come up with crafty workarounds – nor can they because there is nothing, as far as they can see, to work around.

Chapter 2

Introducing SASE, a Modern Security Framework

In this chapter

- Learn what SASE is
- Explore what comprises a SASE architecture
- Understand the benefits of implementing SASE

Despite their rapid acceleration, digital transformation initiatives are far from over. As remote and hybrid work models become the norm and mass migration of applications and data to the cloud continues, the need for a new security architecture is critical. Employees require fast, reliable, and secure access to the tools and information they need to do their jobs and keep the business running – wherever they log in and regardless of the network or device. In this chapter we introduce *secure access service edge (SASE)*, a security framework with the promise of securing work from anywhere, at any time.

What is SASE?

DON'T FORGET

SASE is an emerging cybersecurity framework that moves security and connectivity elements typically located on premises to the cloud, where they are closer to the data, applications, and people that use them. But it isn't just this relocation of technologies to the cloud that makes SASE, well, SASE. Also, cloud-based network connectivity and security functions are converged and integrated, as shown in Figure 2-1.

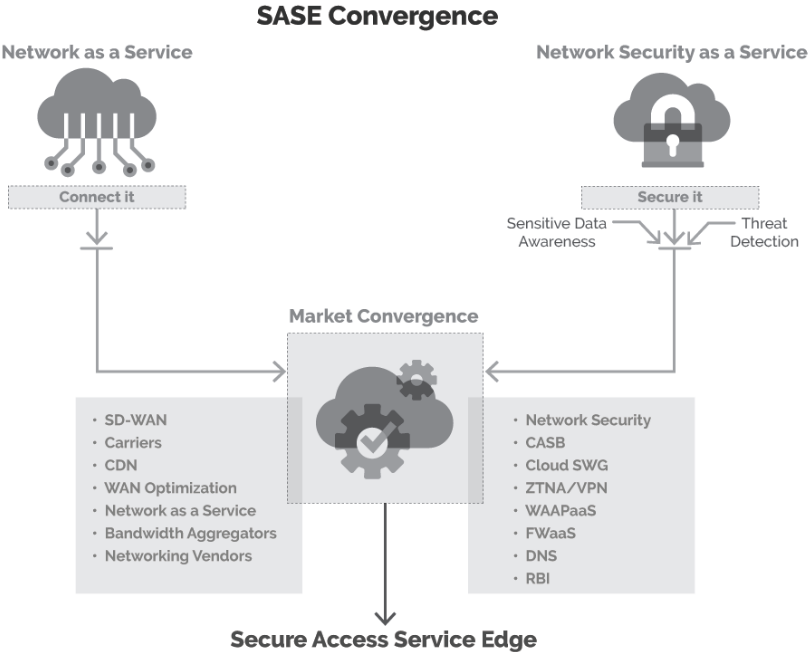

Figure 2-1: SASE is the convergence of cloud-based networking and security technologies.

DON'T FORGET

It's important to understand that SASE is not a single solution. It's not a plug-and-play product you can buy off the shelf. SASE is a dynamic and adaptable architectural framework for deploying application, cloud, data, endpoint, network, and infrastructure security technologies. This framework is highly extensible – there are no limits to what can be deployed in a SASE architecture. However, a SASE architecture is typically comprised of the following centrally managed network security functions:

> ☑ *Secure web gateway (SWG)*
>
> ☑ *Cloud access security broker (CASB)*
>
> ☑ *Firewall-as-a-service (FWaaS)*
>
> ☑ *Zero trust network access (ZTNA)*

☑ *Data loss prevention (DLP)*

☑ *Remote browser isolation (RBI)*

TECH TALK

It's important that capabilities deployed in a SASE architecture are controlled through centralized management and policies, as shown in Figure 2-2. Policies control traffic flows and enforce security controls for users — whether they're on premises or remote — and the resources they need to access, whether residing in the data center, at a branch office, or on the Internet.

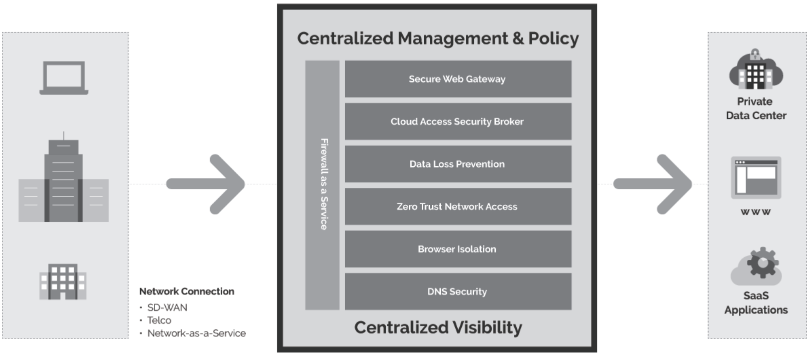

Figure 2-2: A SASE architecture provides central management of network security capabilities and their policies.

Why SASE?

There are several benefits to adopting SASE as your security architecture.

☑ Without full visibility, you don't know if threats are hiding in blind spots in the IT environment. A SASE architecture provides a holistic view of your IT environment for continual visibility across all users, devices, and IT assets.

☑ SASE helps satisfy both modern, adaptive network requirements and complex, layered security demands by applying zero trust network access, as we'll explain further in Chapter 3.

☑ The perimeter-based approach to security has resulted in myriad vendors, policies, and consoles, increasing operational overhead and complexity. Solution integration simplifies network and security administration and management, thereby reducing the risk of human error, inconsistent policies, and operational overhead.

☑ The cloud-native design improves the scalability of network traffic and security capabilities. Organizations can reduce their capital expenses, deployment time, and overhead associated with deploying security and networking capabilities at scale.

☑ SASE eliminates the need to backhaul traffic to the data center for security purposes. Instead, users are connected directly to the assets they need, improving network performance for an enhanced experience and higher productivity.

☑ Organizations can confidently roll out bring your own device programs because the SASE architecture implements appropriate controls and policies to reduce the risk that an infected device will connect to corporate assets.

☑ Hiring managers can hire the right person no matter where they are located because they can do their job securely from any location.

☑ Organizations can give partners and contractors secure access.

Chapter 3

Understanding the SASE Framework

In this chapter

- Take a deeper look at the core SASE capabilities
- Understand the role of zero trust in a SASE architecture
- Learn about the importance of isolation as the foundation of a SASE architecture

There's more to implementing a secure access service edge (SASE) architecture than adopting cloud-based network and security capabilities from various vendors. In this chapter, we take a closer look at the framework as a whole.

Core SASE Capabilities

As we mentioned in Chapter 2, a SASE architecture is not limited to specific network and security technologies and is, in fact, highly extensible. That being said, there are a number of core capabilities that are commonly included in a SASE architecture, as illustrated in Figure 3-1.

Network services

SASE simplifies network complexity and management by combining a *software-defined WAN (SD-WAN)* and other networking infrastructure components. The network services typically included in a SASE architecture include:

☑ SD-WAN

☑ WAN optimization

- ☑ Quality of service
- ☑ Routing
- ☑ Software-as-a-service (SaaS) acceleration
- ☑ Content delivery/caching

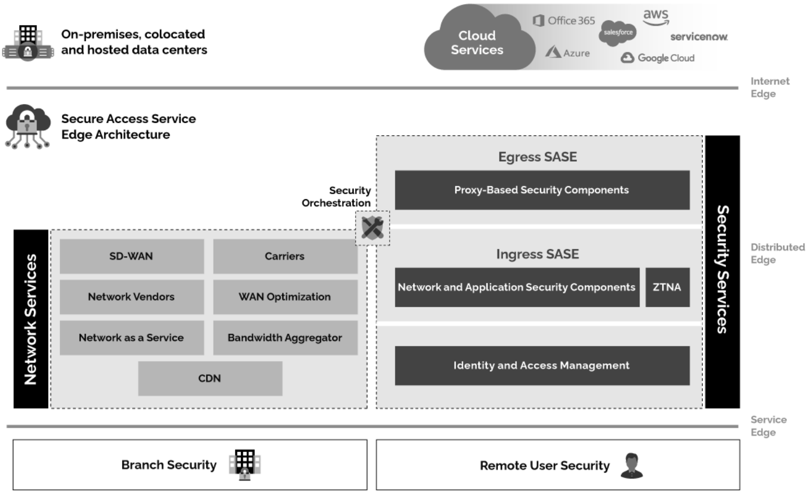

Figure 3-1: A SASE architecture includes network and security services.

Security services

Security services included in a SASE architecture are collectively referred to as the security service edge. According to Gartner®, “The combination of CASB, SWG and ZTNA is called Security Service Edge (SSE). SSE secures access to the web, usage of cloud services and access to private applications. Capabilities include access control, threat protection, data security, security monitoring, and acceptable use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service, and may include on-premises or agent-based components.”[1]

[1] Gartner, “Guide to Cloud Security Concepts”, Patrick Hevesi, Richard Bartley, and Dennis Xu, September 21, 2021.

Gartner Disclaimer: *GARTNER is registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.*

Security services can be divided into two categories: outbound and inbound, referring to the direction of user traffic. Note: zero trust network access (ZTNA), as we explain in chapter 5, is both an inbound and outbound control.

Outbound controls

Outbound, or egress, controls are proxy services that help users gain secure access to off-premises resources from anywhere. Outbound controls include:

- ☑ Cloud access security broker (CASB)
- ☑ Secure web gateway (SWG)
- ☑ Remote browser isolation (RBI)
- ☑ Encryption/decryption
- ☑ ZTNA

Inbound controls

Inbound, or ingress, controls provide secure access to on-premises applications from anywhere. Inbound controls tend to be application-layer controls and network services, including the following:

- ☑ *Web application firewall (WAF)*
- ☑ Firewall-as-a-service (FWaaS)
- ☑ *Web application and API protection (WAAP)*
- ☑ *Identity and access management (IAM)*
- ☑ ZTNA

SASE Security Methodologies

So far, we've explained how SASE security capabilities differ from traditional approaches in terms of where they're located — that is, in the cloud. But SASE security capabilities also differ from traditional solutions in terms of *how* they apply security.

Zero trust in action

Like SASE, zero trust is a security concept that has gained significant traction over the past couple of years. In his May 12, 2021, Executive Order on Improving the Nation's Cybersecurity, U.S. President Joe Biden even mandated that U.S. Federal government agencies adopt zero trust security concepts with a tight deadline for doing so. With zero trust's rising popularity, you may be wondering how zero trust intersects with SASE.

ON THE WEB

First, let's establish what we mean by zero trust. According to NIST, "Zero Trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated."

In other words, you don't trust the user, identity, resource, or device. Zero trust assumes that there's been a compromise and gives least-privilege access to resources in isolation of network access. At every request, the entity is subject to continuous authentication, authorization, and risk evaluation. Like SASE, zero trust is a framework or strategy. You can't buy a zero trust product necessarily, but you can implement tools that support zero trust strategies, and that's where SASE comes in.

DON'T FORGET

Zero trust and SASE work hand-in-hand. SASE is necessary to apply zero trust principles in the cloud, and zero trust is necessary to make SASE well, SASE. Without zero trust, SASE is simply network security delivered in the cloud. With zero trust, SASE is a transformative initiative. Zero trust is applied in the cloud through security services such as zero trust network access, remote browser isolation, and data loss prevention.

Isolation at the core

Isolation is the foundation of security within a SASE architecture. Isolation provides a foundational security capability that's needed across web, email, and applications. The goal is to stop threats from infecting the endpoint, and isolation does just that by implementing a zero trust mindset.

Zero trust enabled by isolation prevents 100 percent of all malware threats from email and web attacks. All incoming traffic is considered malicious and routed through isolation where threats are stopped before they can get to the end user.

An isolation-powered platform achieves zero trust by taking the browsing process off the endpoint and moving it to the cloud, effectively creating an *air gap* between the Internet and enterprise assets. The content is cleaned and safely rendered from the cloud browser to the end user's browser, providing an experience identical to browsing the site outside of isolation. Any breaches or attacks are completely isolated away from the endpoint and user.

Isolation separates the enterprise's resources from the Internet, preventing attackers from gaining a foothold in the working environment. Malware is literally barred from user endpoints. All email and web traffic moves through the isolation layer, where the content is visible but never downloaded to the endpoint. As a result, the isolation-powered platform allows companies to maintain control of security and apply a consistent, global policy to all users.

Modern isolation technologies provide a seamless browsing experience. In fact, the user experience is no different from native browsing on a desktop. However, unlike native browsing on a desktop, the user engages with a website without running any active content on their endpoint. That means malicious content on a website can't infect a laptop, smartphone, or other device. In the case of phishing sites, warnings are displayed on the endpoint and isolation technology can prevent the user from being able to enter their credentials or upload any files.

As a result, users can safely open emails and use cloud-based applications without the risk of a cyberattack. Isolation enables zero trust and eliminates all malware threats from email and web attacks while fully protecting productivity.

Protecting the Endpoint and the User Experience

The largest corporation in Japan is an enticing target for cyberattacks, not only due to its size but also to its importance to the country's economy, its role in the lives of the Japanese people, and the diversity of its customer-facing services. It's no wonder, then, that the organization was the target of an attack that led to the theft of data belonging to 1.25 million people.

In response to the attack, Japan's Ministry of Internal Affairs and Communication created the Internet Isolation Guideline for businesses. The guideline requires the separation of an enterprise network from the public web while providing employees with Internet access to do their work.

When it adopted the guideline, the corporation focused on three key areas: email attachments and external devices, data theft and loss, and web-based attacks on the Internet. The company had solutions for email attachments and data loss prevention, but it didn't have a good solution for web-based attacks. At the time, the company relied on URL filtering and blocking to limit access to bad sites, while allowing access to good sites by using whitelists and blacklists.

Unfortunately, the company's approach to preventing web-based attacks was problematic. Many legitimate sites were categorized as risky or worse, and known good sites could be compromised with malware. Through no fault of their own, users could still have their devices infected.

After rigorous testing and evaluation, the company decided to adopt the Menlo Security Cloud Platform, the only solution in the industry with an Isolation Core™. The Menlo Security Cloud Platform is delivered as SaaS and provides complete protection against web-based malware attacks.

Internet isolation with the Menlo Security Cloud Platform has resulted in 100 percent malware-free web browsing for users across the entire organization. Most importantly, isolation does not impact the user experience and requires no additional browsers or plug-ins to be installed on devices – and users don't have to worry about whether they should click on links in an email or on the web.

"We improved security and usability at the same time," said an executive officer in the company's IT Systems division. "Menlo Security is an outstanding product, and we believe other Japanese corporations should also implement it."

Bringing It All Together

TECH TALK

Simply moving disparate security and networking capabilities to the cloud doesn’t result in SASE. The components must work together and be delivered as close to the user as possible. This is accomplished via *points of presence (PoPs)*, or local access points, which are located around the world, near connecting endpoints. Together, the PoPs make up a globally distributed network fabric through which security policies are applied and traffic is intelligently routed to minimize latency.

Chapter 4

Deploying SASE

In this chapter

- Learn the best starting point for your SASE journey
- Understand how to plan your SASE transformation
- Explore potential roadblocks on the SASE journey and how to overcome them

A secure access service edge (SASE) deployment doesn't happen overnight. As with any IT transformation, planning and resources are required to rearchitect your security infrastructure. Furthermore, you likely have significant investments in the hardware and software that underpin the traditional data center-oriented security model. Most businesses can't afford to abandon those technologies, and we assume you can't either. In this chapter we help you plan a SASE deployment strategy that takes into account your existing security risks and investments.

Where to Start

CAUTION

Organizations learned early in their cloud migrations that a "lift-and-shift" approach does not optimize the benefits of the cloud. Similarly, simply lifting on-premises network and security technologies and shifting them to the cloud will not give you the full benefits of a SASE architecture. To effectively implement SASE, you need to start with an assessment of your existing network and security needs.

Focus on risk

TIP

Deploying SASE requires a phased approach that's implemented in alignment with your organization's specific business objectives. We suggest starting with the area that represents the greatest risk.

As we explained in Chapter 1, the web browser is the new office. Because it's where users spend most of their working day, the web browser is also the primary attack vector and is, therefore, an ideal starting point for a SASE deployment. A secure web gateway (SWG) is the most ubiquitous access point, touching every user within the organization and securing work (and personal web browsing) wherever users do business.

A SWG protects users from web-based threats on the Internet by stopping malicious content before it gets to the endpoint. SWG solutions typically work by blocking inappropriate or malicious websites based on policies set by the enterprise cybersecurity team. Those security policies follow the user wherever work takes them, regardless of the underlying infrastructure or connectivity method. This ability to deliver a secure Internet breakout at scale allows any user to access any application directly and securely without creating performance issues. However, to ensure scalability and the best user experience, it is important that the SWG is cloud based.

CAUTION

Most SWG solutions continue to rely on a detect-and-remediate approach to stopping threats. Unfortunately, threats are constantly evolving and are increasingly hard to identify before they infect the endpoint. By then it's too late. The threat has likely delivered its payload and could be moving throughout the network.

Instead of relying on the SWG to determine what content to trust and what to block, consider a solution that leverages isolation to enable zero trust. As we explained in Chapter 3, isolation takes the browsing process off the endpoint and moves it to the cloud, effectively creating an air gap between the Internet and enterprise assets. All browsing takes place away from the endpoint, eliminating the risk of infecting the endpoint with malware and having to know what content to trust and what to block. Isolation should be at the core of a SASE architecture, as shown in Figure 4-1.

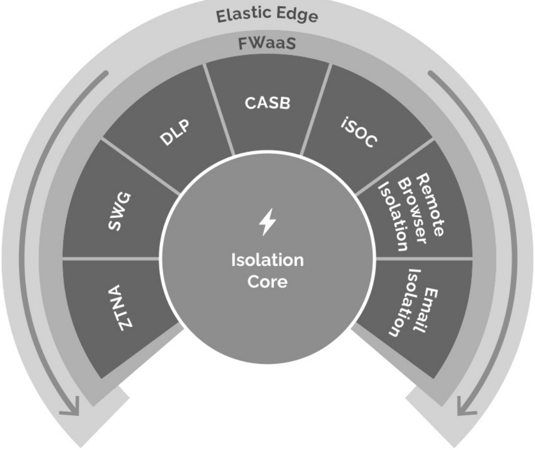

Figure 4-1: Isolation underlies all other SASE components.

Recovering Productivity and Preventing Web-based Threats with Isolation

For one U.S. bank, the detect-and-respond approach to stopping web threats was proving too costly. The bank's traditional cybersecurity solutions were stopping threats from infecting critical systems, but it was a painstaking and laborious process that impacted IT and end-user productivity.

Any potentially vulnerable web page triggered multiple alerts from the bank's cybersecurity solutions. It became so overwhelming that the CISO directed his team to reimage any machine suspected of infection. Every week the team tracked down, wiped, and restored an average of five machines spread across 70 branch offices. In addition to taking employees' devices offline during restoration, the team shut down access to websites that posed a risk, regardless of whether employees needed those sites for their jobs.

The bank's CISO was determined to find a new way to protect users from web-based threats. At the Gartner Risk and Security Summit he watched a team from Menlo Security demonstrate the technology for isolating Internet traffic away from the endpoint — without impacting performance or the user experience.

The Menlo Security Internet Isolation Cloud works by moving the fetch and execute commands to a remote browser in the cloud, where potentially malicious content is scrubbed out. Only safely rendered content is sent to the user's device. Because all access to the endpoint is closed off, malware can't reach it. And with no clients or special browsers to install, users can work the way they always do, with the same level of performance and access to resources.

Since deploying Menlo, the bank has experienced zero web-based malware infections. False positives have disappeared, and machines don't have to be reimaged on a regular schedule, freeing up IT resources for higher-value tasks.

"The Internet can be a very useful research tool, but you're really taking your chances providing access without isolation," said the bank's CISO. "Menlo allows you to provide the value of the Internet to users in a safe manner. And it's the only technology, as far as I'm concerned, that does that."

Or start with connectivity

TIP

Another option for starting your SASE journey is to begin with connectivity. If your primary concern is the ability to connect a distributed workforce to enterprise assets, then kick off your SASE deployment with an SD-WAN that will integrate with other solutions in a SASE architecture. An SD-WAN gives branch office and remote users the ability to:

- ☑ Prioritize business-critical traffic
- ☑ Mitigate network issues for the best application performance
- ☑ Deliver traffic to the closest point of presence (PoP), where additional services from other SASE components can be applied to that traffic

Continuing the Journey

Plan the rest of your SASE transformation around your hardware refresh cycles. As legacy solutions reach end of life, you can acquire additional capabilities focused on the following technologies (and shown in Figure 4-2):

- ☑ **A secure web gateway** protects users from web-based threats on the Internet by preventing malicious content from accessing the endpoint. A cloud-based SWG typically replaces the proxy in a traditional hub-and-spoke model where all traffic is backhauled to the physical appliance in the data center.

☑ **A cloud access security broker (CASB)** provides granular policy control for SaaS applications and deep visibility into application traffic to ensure compliance.

☑ **Zero trust network access (ZTNA)** provides secure access to applications and resources to users with granular access policies regardless of the device or network they are using all without impacting user productivity. ZTNA eliminates the need for legacy virtual private network (VPN) services by providing fast, seamless access to internal applications.

☑ **Remote browser isolation (RBI)** safely renders all web content and documents in the cloud, away from endpoints. Granular policy controls allow administrators to configure policies for situations where content is blocked, read-only, or safe as original content based on user, group, file type, or website category.

☑ **Email isolation** protects endpoints from email threats. It stops malware from reaching the endpoint by sending links in email to isolated browser sessions and rendering any attachments in isolation.

☑ **Firewall-as-a-service (FWaaS)** provides firewall controls and security to all users in all locations for all ports and protocols. FWaaS eliminates the need to backhaul cloud application and SaaS traffic to data centers.

☑ **Data loss prevention (DLP)** identifies and prevents sensitive data from leaving your company. DLP inspects file uploads and user input for all browser sessions and cloud applications.

☑ **An isolation security operations center (iSOC)** examines global Internet traffic that flows through the provider's cloud to protect your organization from known and unknown threats. iSOC also provides your SOC team with actionable threat intelligence.

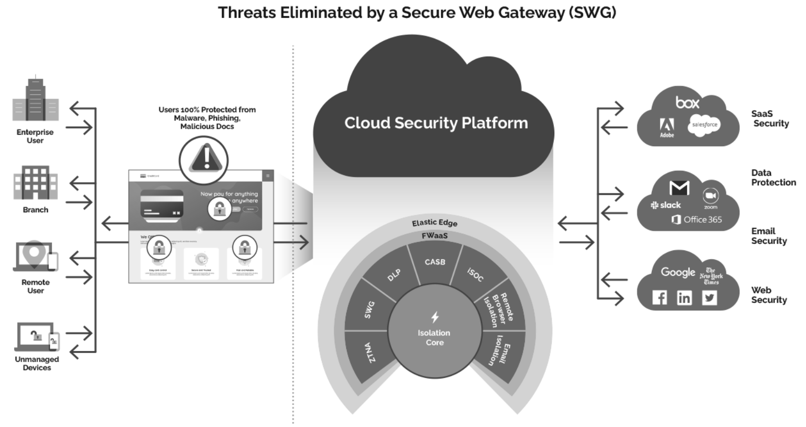

Figure 4-2: As on-premises solutions reach end of life, deploy the capabilities shown above as part of your SASE architecture.

Overcoming Potential Roadblocks

Nothing new — especially a transformative project like SASE — comes without challenges. However, they are not insurmountable. Nor will they hinder your progress if you're adequately prepared to overcome them. Let's look at some of the challenges you're likely to encounter when deploying SASE and how to surmount them.

Operational and cultural changes

The convergence of networking and security technologies requires cooperation between enterprise network and security operations teams. These teams often operate separately. To ensure a smooth move to a converged architecture, bring together members of both teams early in the migration process. If you can't get together physically, then do so virtually to assess potential benefits, challenges, and impacts.

People power

TIP

People are key to a successful SASE strategy. Take inventory of your human capital and understand the existing skill sets of employees — particularly those who deal with operational and security issues. This information will allow you to build on existing strengths as well as proactively identify and fill any gaps that could slow down your SASE deployment. Work towards creating a dedicated team of security and networking experts who share responsibility for enabling secure access from anywhere.

Lift-and-shift

Because everything in IT has changed — the data, the endpoints, and the applications — the SASE framework requires you to think about security in a different way. If you continue to think about security in the old way and attempt to migrate security capabilities to the cloud via a lift-and-shift approach, you'll be trying to force a square peg into a round hole.

You must therefore deploy security components that are built for the cloud and cloud first, because that is the world we work in today. Applications, data, and people are in the cloud. Security must be there, as well.

Similarly, SASE security components must be built to integrate with each other. Moving legacy solutions to the cloud doesn't give you that integration. You will still have separate policies for siloed security solutions. Integration provides centralized visibility and shared policies so you have a complete view of what's going on across all your users.

Buying more than you can consume

CAUTION ⚠

Another possible setback on your journey to SASE is biting off more than you can chew. Be smart about your investments. Figure out what you need, the order to put them in, and enable the solutions in a thoughtful manner to cause the least disruption to the business as possible. Because SASE capabilities are delivered as a service, turning them on is as easy as the press of a button, and consumption will fall under operational expenses. There's no need to plan years in advance to procure hardware with the hope that you've properly planned for future growth.

Chapter 5

10 Considerations When Deploying a SASE Framework

In this chapter

- Understand the need for both horizontal and vertical scalability in a SASE architecture
- See why zero trust must be bi-directional
- Learn how to future-proof your SASE deployment

Deploying a secure access service edge (SASE) is a significant undertaking that takes planning, time, and effort. To ensure that the investments you make today will continue to be of value several years from now, keep the following considerations in mind throughout your SASE deployment.

Horizontal Scalability

By horizontal scalability we mean the ability to increase throughput and user support at the press of a button. Business growth can happen rapidly and unexpectedly. You can't afford to wait for days or even weeks to build out your security services to accommodate an influx of new users or traffic. If your user base grows by an extra 5,000 people due to an acquisition or if business suddenly skyrockets over Thanksgiving weekend, you need to be able to support that growth immediately.

Vertical Scalability

By vertical scalability, we mean the ability to turn on additional security services as you're ready to expand your SASE deployment. It's crucial to find a vendor or vendors with platforms that can integrate all the elements critical to a successful SASE strategy, and that can scale up as business horizons and workforces shift and expand. Integration ensures that the services work well together and reduces the operational overhead associated with procuring additional capabilities. The services are ready right when you need them.

Points of Presence: Quality over Quantity

Vendors that offer SASE capabilities may own their own points of presence (PoPs), use a third party's PoPs, or leave it up to you to provide your own connectivity. Avoid the temptation to compare only the number of PoPs between providers. Consider PoP ownership, compute power, and geographic distribution to ensure you can meet compliance and privacy requirements for the inspection of data, storage of logs, and routing of traffic.

Centralized Policy and Reporting

Inconsistent security policy management across different tools results in operational inefficiencies and misconfigurations that can increase your organization's risk exposure. The integration and convergence of network and security capabilities in a SASE architecture should result in centralized policy management and reporting.

Bi-directional Zero Trust

TIP

Most vendors consider zero trust to be an inbound control in which endpoints are assumed to be compromised and users are given restricted access to IT assets. But that's only half the picture. To effectively eliminate threats, zero trust must be bi-directional. In other words, zero trust should be applied to protect applications from users (such as through the use of a zero trust network access solution) and to protect users from applications, business documents, and web content (as provided via isolation).

Isolation as the Foundation

Cloud-based security capabilities that leverage isolation at their core enable a zero trust approach to cybersecurity. This is the only way to eliminate malware. Isolation assumes that all web-based content is malicious. Thus, isolation creates a protective layer around users as they navigate the web, blocking not only known and existing threats, but unknown and future threats as well. Rather than responding to attacks after the fact, you can prevent them from reaching users in the first place with isolation.

Support for Unmanaged Devices

To meet the demands of today's workforce and ensure operational agility, a SASE deployment must be endpoint agnostic. The security capabilities should support all types of users and devices, eliminating the complexity of implementing and enforcing bring your own device (BYOD) policies.

Nothing Left Uncovered

CAUTION

Similarly, a SASE deployment should protect all types of data, applications, and cloud environments to ensure complete coverage and visibility, both today and in the future. Any IT assets that are not covered by SASE will essentially become blind spots — areas where you lack visibility and, possibly, protection. Even if you choose to implement separate security controls for the outliers, you'll be exposed to increased risk due to the potential for inconsistent security policy management.

Unified Platform

Look for a provider that offers a unified platform for network security capabilities. Ideally, the platform consolidates multiple security services and protects users regardless of their location or endpoint device. The platform should span security control and visibility across all the applications users require to work, including web, email, and software-as-a-service (SaaS) applications while enabling data loss prevention (DLP) policy.

Extensibility/APIs

TECH TALK

Cybersecurity must move at the speed of business. To ensure that your SASE deployment can go wherever the business goes, look for a platform that easily integrates with other solutions. Extensibility through APIs will enable you to continue your SASE journey regardless of what tomorrow brings.

Your Next Steps

Digital transformation initiatives took on a life of their own when a pandemic forced organizations to support remote work for their entire workforce in a short period of time. Going forward, security teams need to change the way they think about and apply security. Using this book as your guide, we hope you can move deliberately and confidently along the journey to a SASE architecture. Moving security services to the cloud, where they are closer to your users, and applying isolation with zero trust methodologies will give users the anytime, anywhere secure access they need to do their jobs while making your job easier.

Glossary

air gap: created by removing any physical or digital connections between two or more IT assets or networks.

cloud access security broker (CASB): a technology solution that provides users with safe, secure access to software as a service (SaaS) applications. A CASB also detects sanctioned and unsanctioned SaaS applications, and discovers and monitors sensitive data.

data loss prevention (DLP): a technology solution used to monitor traffic for sensitive information leaving the network. A cloud based DLP solution can monitor traffic outside the traditional network perimeter, where users access information on the Internet.

firewall as a service (FWaaS): a cloud-based firewall that, like a standard firewall, filters, monitors, and blocks ingoing and outgoing traffic and enforces an organization's security policies.

points of presence (PoPs): network access points through which user endpoints access the secure access service edge.

remote browser isolation (RBI): a technology service that protects users' devices from web- and email-based cyberattacks by executing dynamic content away from the endpoint, in the cloud.

secure access service edge (SASE): a framework for delivering security and networking services through the cloud. SASE enables a zero trust approach to connecting distributed users, devices, branch offices, applications, and software as a service applications.

secure web gateway (SWG): a technology solution that protects users from web-based threats on the Internet by preventing malicious content from accessing the endpoint.

security service edge (SSE): a term, coined by Gartner, to refer to the integrated, cloud-based security capabilities of a SASE architecture.

software as a service (SaaS): applications hosted and managed in the cloud by a service provider.

software-defined wide area network (SD-WAN): as a critical component of a secure access service edge architecture, SD-WAN automatically optimizes traffic routes between two locations across any network architecture.

web application and API protection (WAAP): a cloud-based security service designed to protect web applications and APIs by analyzing incoming traffic.

web application firewall (WAF): a type of application firewall specifically designed to filter, monitor, and block HTTP traffic to and from a web service.

zero trust: a default-deny approach to security that assumes everything on the Internet is a potential threat and that no device, data, location, or network is to be trusted.

zero trust network access (ZTNA): a technology solution that grants access only to applications required for a particular role or person to do their job.

Discover how to implement a secure access service edge architecture to deliver secure anytime, anywhere access to data and applications on premises or in the cloud.

Accelerated by the global pandemic, digital transformation initiatives took on a life of their own. Seemingly overnight, end users (and their devices), data, and applications moved to the cloud — leaving security behind in the on-premises data center. Now it's up to cybersecurity teams to transform security for a highly distributed IT environment. This guide will show you how.

- Exploring how we got here — review how the IT infrastructure has transformed and the challenges it poses for security
- Introducing SASE — explore the secure access service edge architecture and the benefits it delivers to both IT and the business
- Understanding the SASE framework — learn about the capabilities and methodologies that make a SASE architecture effective
- Deploying SASE — understand how to implement a SASE architecture, including overcoming potential roadblocks
- Reviewing SASE requirements — know what to look for when deploying a SASE framework

About the Author

A former editor of SearchSecurity.com, Crystal Bedell is a senior marketing consultant specializing in cybersecurity. She's been helping technology providers create engaging content since 2000.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-24-9

9 781948 939249