LEARNING MADE EASY

Fortinet Special Edition

Single-Vendor SASE

for dummies®
A Wiley Brand

Consistent security for the hybrid workforce

Networking and security convergence

Superior user experience

Brought to you by

FORTINET

Lawrence Miller

About Fortinet

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.

Single-Vendor SASE

Fortinet Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Single-Vendor SASE For Dummies®, Fortinet Special Edition

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

ISBN 978-1-394-22516-3 (pbk); ISBN 978-1-394-22517-0 (ebk)

Publisher's Acknowledgments

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

Project Manager: Jennifer Bingham
Acquisitions Editor: Traci Martin
Editorial Manager: Rev Mengle
Client Account Rep: Cynthia Tweed
Content Refinement Specialist: Saikarthick Kumarasamy

Table of Contents

Introduction

Digital innovation, cloud adoption, and the shift to a hybrid workforce have fundamentally transformed the network. As organizations increasingly rely on cloud-based resources, such as software-as-a-service (SaaS) applications, the need for a new approach to secure network access — especially the challenges of implicit trust inherent in legacy network architectures — has become clear.

Modern enterprise users require immediate, uninterrupted access to network- and cloud-based resources and data, including business-critical applications, from any location, on any device, at any time. The challenge is that many of the issues resulting from digital innovation efforts, such as dynamically changing network configurations and the rapid expansion of the attack surface, mean that many traditional security solutions no longer provide the level of security and access control that organizations and users require.

Secure Access Service Edge (SASE) is an enterprise strategy that combines network security functions with wide-area network (WAN) capabilities. SASE's goal is to support the dynamic, secure access needs of today's organizations. SASE plays a critical role in ensuring that security can be delivered anywhere, including at the WAN edge, cloud edge, data center (DC) edge, core edge, and endpoint devices used by today's hybrid workforce.

About This Book

This book consists of six chapters that explore the following:

- The challenges of securing the modern hybrid workforce (Chapter 1)
- Why you need a single-vendor SASE solution (Chapter 2)
- Which key components are integral to a single-vendor SASE solution (Chapter 3)
- How to use single-vendor SASE to address common use cases (Chapter 4)

- The Fortinet Universal SASE solution (Chapter 5)
- Ten important criteria and business benefits to look for in a single-vendor SASE solution (Chapter 6)

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.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you're an IT or security decision maker looking for a better way to secure your hybrid workforce. Whether you're a chief information officer (CIO), chief information security officer (CISO), chief financial officer (CFO), vice president of IT or infrastructure, or a network, cloud, or security architect, this book will help you understand how a single-vendor SASE solution can help you simplify operations, lower costs, and improve the user experience for your organization.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway. It's a great book and after reading it, you'll be singled out as the "go-to" source for information about single-vendor SASE.

Icons Used in This Book

Throughout this book, you will find 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.

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected — hopefully, 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.

CASE STUDY

Case studies about single-vendor SASE.

Beyond the Book

There's only so much that can fit in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" go to `https://fortinet.com`.

IN THIS CHAPTER

- Looking at security gaps created by a hybrid workforce model
- Addressing virtual private network (VPN) issues
- Shining a light on shadow IT
- Recognizing the value of a single-vendor networking and security solution

Chapter 1
Recognizing the Challenges of Securing a Hybrid Workforce

Providing secure, reliable, and consistent access to corporate assets and applications for the hybrid workforce is one of the biggest challenges facing IT teams today. Secure, authenticated access to critical applications and resources combined with consistent enterprise-grade protection, whether users are on-premises, working from home, or somewhere in between, is crucial.

In this chapter, you learn how the modern threat landscape has evolved in the wake of the global pandemic and the advent of the hybrid workforce. You'll discover how this new work model has opened new security gaps, why virtual private networks (VPNs) are no longer adequate to secure remote connectivity, how shadow IT both confers benefits to organizations and puts them at risk, and why you need a comprehensive single-vendor solution to address the challenges of a modern hybrid workforce.

Identifying Security Gaps

The modern hybrid workforce has introduced new networking and security challenges that organizations must address to ensure a robust security posture and a performant network infrastructure that meets the dynamic needs of the enterprise and its users.

Often, network and security teams address different business needs with "one-off" point solutions, such as a standalone router to provide Internet connectivity at a branch location and a small firewall appliance to provide secure connectivity to the Internet, the public cloud, and the corporate data center.

Unfortunately, these approaches often create gaps in the organization's security posture and introduce other challenges, such as:

- **Inconsistent security policies and controls:** Lack of a centralized management console for siloed security tools often leads to inconsistent — and potentially insufficient — enforcement of security policies and application of security controls. Applying and enforcing consistent policies, whether a user is on-network or off-network, is challenging. This negatively impacts user experience and productivity.
- **Inefficient use of network resources:** Multiple direct Internet access (DIA) links are often provisioned for branch locations to ensure connectivity if a link fails. Depending on the networking equipment used, these configurations may not support load balancing, traffic prioritization (that is, quality of service or QoS), automated failover/failback, and other advanced networking capabilities. Different firewalls and other security tooling on the various DIA links also create many security challenges.
- **Lack of onsite expertise:** Branch locations don't always have local IT resources to troubleshoot networking and security issues when they inevitably arise. Practically every organization today must work with limited budget resources and workforce shortages, especially within the security profession. Remote access options may be limited for many point solutions, requiring IT staff to get creative with third-party remote access tools which may introduce new risks to the enterprise IT environment.

- **Increased complexity:** Managing disparate solutions from different vendors is challenging. It requires limited IT and security staff to learn specialized skills and new interfaces to operate each of the various tools. Complexity leads to a greater risk of security misconfigurations and requires more time to troubleshoot when issues arise.

Understanding VPN Performance Issues

Virtual private networks (VPNs) have traditionally been used to provide secure connectivity between remote user endpoints (including branch, mobile, and other locations) and corporate networks. Unfortunately, VPNs have notoriously been plagued with many performance and usability issues. Additionally, VPNs have traditionally been configured for all-or-nothing access: If a device is trusted (that is, connected to the VPN), then it has access to the entire network, which means a compromised device may compromise the entire network.


TECHNICAL STUFF

VPNs encrypt traffic, typically using either Internet Protocol security (IPSec) or secure sockets layer (SSL), to secure traffic sent and received over the Internet.

Although VPNs enable secure access to corporate data centers and other physical locations, they aren't optimized for access to public cloud resources. Thus, many users either connect to these cloud resources without a VPN, or they use features such as split tunneling to send certain traffic bound for the corporate network over the VPN, while other traffic — such as cloud applications — routes directly over the Internet, thereby bypassing the VPN tunnel altogether. As a result, no security or access controls are provided for these users when they connect to cloud applications and services.


WARNING

Although split tunneling can improve the performance of a VPN by offloading certain traffic from a corporate VPN concentrator, it introduces many potential security risks including compromised data security, exposure to malware and other threats, and loss of monitoring and control capabilities. Also, current VPN options don't provide continuous verification of a user's identity and they lack the granular controls to limit access to only those resources that are authorized for a particular user.

Addressing Lack of Visibility and Shadow IT

Providing IT and security teams with end-to-end visibility of network traffic has always been a challenge. With the hybrid workforce now connecting to corporate and cloud resources from practically anywhere, this challenge has grown exponentially.

The challenge is further exacerbated by shadow IT. Shadow IT refers to IT activities undertaken outside of the typical IT infrastructure and typically without the IT or security department's knowledge or explicit authorization.

REMEMBER

Shadow IT is the result of end users finding technology and applications that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use, than corporate IT solutions. Shadow IT solutions are acquired and operated by end users without explicit approval and often without IT knowledge or support. For example, end users may download and install personal versions of Box and Gdrive, rather than using the corporate or enterprise versions of those apps. Although these personal versions may be free or relatively inexpensive for end users, they ultimately cost more if large numbers of users purchase individual plans, they often don't have important security and privacy features enabled, and IT has no visibility or control.

Shadow IT can introduce new risks if not properly managed, including:

- **Data loss and inconsistent data:** With shadow IT, individual employees may be responsible for reporting data around important concerns like IT security or productivity. This can lead to inconsistencies, which could make it difficult to track and properly react to data that would otherwise be readily available and consistently reported if an IT team were in control.
- **Compliance issues:** The compliance landscape often undergoes unexpected, even drastic, changes. Because shadow IT relinquishes control to individual employees, who are often busy or preoccupied with other important things, compliance issues may go unaddressed.

- **Downtime and fewer required security measures:** With shadow IT, if something goes wrong, the amount of downtime can be exacerbated by the inexperience of the user. Sometimes, when an employee has an issue, it may take several hours for them to fix it. But it would take mere minutes for a trained IT professional who has experience handling that type of problem.

Comparing Point Products Versus Consolidation

To ensure consistent connectivity and security for users everywhere, networking and security solutions must converge at the edges and in the cloud. Secure Access Service Edge (SASE) consolidates networking and security capabilities and functions in a single, cloud-delivered solution. Achieving consistent connectivity and security can be difficult when trying to integrate solutions from different vendors. Instead, a platform-centric, single-vendor SASE solution enables the consolidation of technologies and converges networking and security functions to drive operational efficiency. It is also important for organizations to deploy a SASE solution that can be seamlessly integrated into their larger networking and security architectures to ensure secure and reliable connectivity and deliver superior user experience wherever needed.

WARNING

As with any new opportunity, vendors invariably pop up looking to fill an urgent need and capture a piece of the new market. However, many of these solutions fall short of their promised benefits. Some rely on immature technologies or inadequate capabilities. Many operate as isolated, standalone solutions that don't integrate with existing security technologies or the expanding hybrid network. Few enable organizations to build a seamless solution that reduces rather than complicates solution sprawl. For organizations trying to manage a rapidly expanding and highly dynamic hybrid network, adding yet another set of technologies to manage can overwhelm limited IT resources. The manual controls, scripts, and limited threat intelligence used by many SASE vendors can't keep up with today's rapidly evolving threat landscape, leaving organizations vulnerable.

IN THIS CHAPTER

- Looking at the changing workforce
- Bringing together networking and security functions
- Eliminating inefficiencies in traditional WAN architectures
- Reducing vendor sprawl and operational complexity
- Ensuring consistent security and user experiences
- Leveraging a single agent
- Simplifying consumption and management

Chapter 2
Understanding the Need for Single-Vendor SASE

In this chapter, you learn how the hybrid workforce, the move to the cloud, vendor sprawl, and other trends are driving the need for a single-vendor SASE solution.

Securing the Hybrid Workforce

A hybrid workforce is the new reality for many businesses today. The percentage of workers worldwide that now permanently work from home doubled since 2021 according to a recent article in *Security Magazine*. A recent Tech Republic survey shows that 83 percent of business and IT leaders see hybrid work as a mainstay of future operations, and 42 percent think that more than half of their workforce will remain permanently hybrid.

At the same time, the number of applications and services that organizations have migrated to the cloud for greater efficiency, cost-savings, and elasticity has grown significantly. As much as half of all spending across applications, infrastructure software, business process services, and system infrastructure markets will have shifted to the cloud by 2025 according to ZDNet.

But these rapid changes to how businesses operate have created new problems for cybersecurity teams. A recent Help Net Security survey reveals that 80 percent of security and business leaders feel their organizations are more exposed to risk due to remote work. This is borne out by data reported by *Forbes*, showing that the overall volume of attacks increased by 31 percent, fueled by cybercriminals trying to exploit rapid changes to business networks. The number of successful data breaches also grew last year, eclipsing the previous annual record by 23 percent according to the Identity Theft Resource Center (ITRC).

Protecting today's rapidly evolving hybrid work environments calls for robust, purpose-built security — such as Secure Access Service Edge (SASE).

Converging Networking and Security

Modern networks have evolved and today are nothing like the networks most security solutions were originally designed to protect. During the early stages of the pandemic, the main focus for enterprises was to provide connectivity for remote workers. Post-pandemic, this focus has now shifted to increased performance, greater efficiency, and improved security, which require enterprises to rethink their security strategy and posture. The notion of a perimeter has all but disappeared as users now commonly access corporate resources while working from anywhere — the corporate office, a branch location, a home office, coffee shop, even on vacation at an airport or hotel. And the resources they access aren't necessarily in a corporate data center. IT resources — including business-critical applications and workloads — are increasingly hosted in public clouds. Even with aggressive public cloud adoption, existing private clouds have not been fully displaced. Enterprises are not yet ready to completely give up on their on-premises datacenters, leading to hybrid cloud and multicloud environments composed of several public cloud vendors.

These highly dynamic environments are expansive and constantly evolving to support an organization's digital acceleration efforts, work-from-anywhere (WFA) strategies, and other top business priorities.

In response to these rapid changes, many security and network teams have become accustomed to overlaying point security solutions onto their hybrid networks. Yet doing so has led to increased management complexity, performance bottlenecks, poor user experience, and the potential introduction of new exploitable gaps or vulnerabilities. But hybrid, rapidly evolving networks are here to stay, so a better approach to security and networking is needed.

Instead of simply consolidating solutions and vendors, networking and security convergence can deliver many benefits for security and network teams. The result is that organizations can provide a reliable and consistent user experience while improving security, reducing complexity, and finding efficiencies.

REMEMBER

Security and networking must continue to converge to allow organizations to adapt to today's rapid pace of new priorities and evolving business needs.

Integrating SD-WAN and Cloud-Delivered Security

The combination of new digital tools, cloud adoption, and WFA users requiring remote access has made it impossible for traditional wide area network (WAN) architectures to handle traffic demands at the network edge. Traditional WANs used expensive multiprotocol label switching (MPLS) connections and centralized security services because the applications were located in on-premises datacenters. This traditional WAN architecture requires network traffic from branch locations to be backhauled through the corporate data center, creating bottlenecks and inefficiencies that degrade the user experience.

Software-defined wide area networking (SD-WAN) provides significant advantages over MPLS, both in terms of bandwidth and cost, by dynamically selecting from a variety of Internet connections — for example, Ethernet, 5G, 4G Long-Term Evolution (LTE), and broadband. With SD-WAN, these direct connections

to cloud and Internet resources bypass the inefficient hub-and-spoke architecture of traditional WANs — as well as the centralized security services that require branch (that is, the "spoke") traffic to be backhauled through the corporate egress point. This wide-open exposure to threats requires robust security — and many of today's SD-WAN networking solutions have little-to-no built-in security. The focus of the majority of SD-WAN solutions today is providing an efficient user-to-application experience — not delivering native security.

As a result, many organizations add disparate security tools to address the security shortcomings of their specialized SD-WAN networking devices. This siloed approach increases both capital expenditures and operational costs while increasing complexity and creating potential gaps for cyberattacks to slip past defenses. As threats continue to grow in number and sophistication, integrated security is increasingly essential for any WAN transformation project.

A platform-based approach to SD-WAN includes advanced networking and security capabilities that are explicitly designed to interoperate as a unified system — ideally running on the same operating system and managed via a single pane of glass. This ensures that all traffic is inspected, and any threats or anomalous behaviors are shared between every product in the ecosystem for maximum protection. A comprehensive secure SD-WAN platform can also consolidate a range of point products — including routers, firewalls, WAN optimization devices, and access proxy for zero-trust network access (ZTNA) — into a single product, simplifying architecture and reducing capital investment costs.

Consolidating Vendors and Reducing Operational Complexity

Managing multiple vendor relationships is a challenge in itself. However, the issue is more troublesome than simply juggling vendors. Operationally, working with different vendor products and services is complex and costly. Security tooling has always been very disparate; every new problem would yield a new vendor or a new product category altogether. This situation has led

to multiple, one-off point solutions being adopted by enterprises in the relentless pursuit of a best-of-breed defense-in-depth strategy. The reality is that this approach has led to a complex environment in which security tools are loosely integrated at best, security analysts are unable to efficiently and effectively correlate events across the different tools, and the organization's security posture is weakened by their inability to maximize the security efficacy of the plethora of security tools they have amassed.

Different vendors have different licensing models, maintenance contracts, support fees, and more. Network and security teams must also learn different operating systems, admin interfaces, and command syntax across these siloed point solutions. Finally, correlating events across different security tools requires deep integration and automation that may not be possible with siloed tools, further increasing mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR), and ultimately slowing down and limiting the effectiveness of incident response.


TIP

Single-vendor SASE — the delivery of networking and security capabilities from one vendor in a unified solution — is a prime example of consolidation that helps network and security teams drive operational efficiency, reduce costs, and eliminate needless complexity.

Delivering a Consistent Security and User Experience

A single-vendor SASE solution should be easily integrated into the organization's larger network and security architecture rather than working as a one-off solution. Ideally, the security protocols and policies within the SASE solution should be identical to those used elsewhere in the network. Systems managers should also be able to integrate their SASE solution with existing technologies to optimize their security and network operations through seamless interoperability.


REMEMBER

Consistent network operations and security controls enable a superior user experience for workers — no matter where they work from or what device they use.

Unified Agent

Enterprises have deployed multiple agents over time for different security capabilities — such as secure web gateways (SWG), cloud access security brokers (CASB), endpoint protection platforms (EPP), and endpoint detection and response (EDR) — as each technology has been developed over the years and introduced to the market at different times. Onboarding a different agent for different scenarios and configurations can quickly increase complexity and become expensive to maintain. A single-vendor SASE solution should provide a single agent that can be used to deliver all the capabilities and features of the solution — including ZTNA, SD-WAN, cloud access security broker (CASB), firewall-as-a-service (FWaaS), endpoint protection, and more — all without any user intervention; redirecting traffic to protect assets and applications through cloud-delivered security.

Ease of Consumption and Management

SASE is delivered as a hosted and managed service by a vendor in the cloud; this allows enterprises to benefit from an operating expense (OpEx) based model, rather than capital expenditures (CapEx). With numerous features defined under SASE, enterprises should get a flat license tier with all features included. With SASE, enterprises can consolidate multiple point security products with fewer management consoles to monitor. Ideally, on-premises firewalls, virtual firewalls, SD-WAN devices, and cloud-delivered security, should all be managed from a single management console with a unified agent.

IN THIS CHAPTER

- Increasing performance and resilience in corporate WANs
- Securing web usage
- Leveraging NGFWs in the cloud
- Implementing ZTNA
- Gaining visibility and control of SaaS applications
- Reducing management complexity with a single, unified console

Chapter 3
Identifying the Key Components of a Single-Vendor SASE Solution

In this chapter, you learn about the most important capabilities and features in a single-vendor SASE solution.

Secure Software-Defined Wide Area Networking

Software-defined wide area networking (SD-WAN) offers the capability to use available WAN services more effectively and economically — giving users across distributed organizations the freedom to better engage customers, optimize business processes, and innovate. WAN innovation with additional carrier links can be leveraged to provide redundancy, load balancing,

and optimization of application traffic. It also makes WAN management more cost-effective. Most SD-WAN vendors don't provide security beyond a stateful firewall; thus, the branch's attack surface is exposed due to Internet connectivity, hence it becomes vital to ensure the SD-WAN solution also delivers native security.

TECHNICAL STUFF

Key SD-WAN capabilities include the following:

- **Automated path intelligence:** Application awareness enables prioritized application routing across network bandwidth based on the specific application and user. SD-WAN service-level agreements (SLAs) should be easily defined by dynamically selecting the best WAN connection, including Long-Term Evolution (LTE)/5G wireless WAN options, for specific business requirements. For low- to medium-priority applications, organizations can specify the quality criteria, and the solution will select the corresponding link. For high-priority and business-critical applications, organizations can define strict SLAs based on a combination of jitter, packet loss, and latency metrics.
- **Automatic failover:** Multipath technology can automatically fail over in a subsecond to the best primary WAN path, including LTE/5G wireless WAN options. This automation should be built into the solution, and occur immediately, which reduces complexity for end-users while improving their experience and productivity.
- **WAN path remediation:** WAN path remediation utilizes forward error correction (FEC) and packet duplication to overcome adverse WAN conditions such as poor or noisy links. This enhances data reliability and delivers a better user experience for applications like voice and video services. FEC adds error correction data to the outbound traffic, allowing the receiving end to recover from packet loss and other errors that occur during transmission. Packet duplication sends copies of packets on alternate available paths, including LTE/5G wireless WAN options. This improves the quality of real-time applications.
- **Application prioritization:** With the capability to define application-specific business policies, the best possible utilization of bandwidth can be ensured by adding precise quality of service (QoS) prioritization for critical applications, while rate-limiting noncritical applications that can negatively impact performance and end-user experience.

- **Next-generation security:** With every SD-WAN branch and its associated local Internet connections, an organization expands its attack surface. As local breakouts are becoming common in SD-WAN deployments for cloud traffic, an SD-WAN solution should offer native security features — such as next-generation firewall (NGFW), intrusion prevention system (IPS), web filtering, high-speed Secure Sockets Layer (SSL), Transport Layer Security (TLS), and IP Security (IPsec) virtual private network (VPN) — which can scale to thousands of sites.

Secure Web Gateway

A secure web gateway (SWG) provides a secure web experience to protect users, devices, and applications from both internal and external threats. Using one solution rather than several disparate point products offers a number of benefits, including simplified management and reduced costs, while maintaining a strong security posture. SWG capabilities provide an end-to-end secure web experience with uniform resource locator (URL) filtering, data loss prevention (DLP), and advanced malware protection

In a SASE architecture, an SWG is implemented for every single device connected to your network. SWG uses domain name system (DNS) information and other technologies to identify the sources of unwanted traffic.

Firewall-as-a-Service

Firewall-as-a-Service (FWaaS) is a firewall solution delivered as a cloud-based service that allows companies to simplify IT infrastructure. It provides NGFW capabilities like web filtering, advanced threat protection (ATP), IPS, and DNS security.

In many ways, FWaaS is much like a hardware firewall that you would deploy in an on-premises environment. However, FWaaS comes with distinct advantages, such as the capability to scale nearly instantaneously to suit an expanding network. You can also have new services provisioned that you previously did not need. Additionally, FWaaS provides organizations with flexibility to scale up and down depending on usage trends and seasonality.

FWaaS provides the same security features as a standard hardware firewall appliance but uses software in the cloud. This is particularly helpful when trying to secure flexible, constantly changing SD-WAN solutions. Users don't have to connect to a physical firewall. Instead, their transmissions are protected by cloud-hosted software, ensuring consistent security no matter where they're located.


TECHNICAL STUFF

Much like a NGFW, FWaaS filters network traffic to safeguard organizations from both inside and outside threats. Along with stateful firewall features such as packet filtering, network monitoring, IPsec, VPN support, and Internet Protocol (IP) mapping features, FWaaS also has deeper content inspection capabilities that include the ability to identify malware attacks and other threats.

Zero-Trust Network Access

Zero-trust network access (ZTNA) is used to identify users and devices and authenticate them to applications. Because ZTNA is more of a strategy than a product, it includes several technologies working together. Multifactor authentication (MFA) identifies all users.

On the physical side, ZTNA includes secure network access control (NAC), access policy enforcement, and integration with dynamic network segmentation to limit access to network resources.

And on the cloud side, ZTNA supports things like microsegmentation with traffic inspection for secure east-west communications between users, and always-on security for devices both on- and off-network.

By combining physical and cloud-based ZTNA services, organizations can ensure secure access and the enforcement of policy, whether devices and users are on- or off-premises.


REMEMBER

ZTNA is an essential tool for protecting today's distributed resources and hybrid workers. A ZTNA solution must authenticate users everywhere, grant explicit access to specific applications, provide constant monitoring, and take countermeasures when something unexpected occurs during established communication channel.

Cloud Access Security Broker

A cloud access security broker (CASB) is software that sits between users and their cloud services to enforce security policies as they access cloud-based resources. CASB differs from firewalls that organizations use to monitor and filter their network. CASBs can identify strange or unusual user activity and provide organizations with cloud access control. Unlike firewalls, CASBs provide deep visibility into cloud environments and offer granular control of cloud usage. CASB solutions are broadly categorized as two offerings: application programming interface (API) based and in-line. Both offerings are essential in a SASE solution to provide holistic security for SaaS applications. API-based CASB provides additional insights into users' SaaS activities causing it to be generally delayed, whereas in-line provides instantaneous enforcement for any user traffic pushed to SaaS locations.

REMEMBER

CASBs are increasingly being used to protect against cloud security risks, comply with data privacy regulations, and enforce corporate security policies. They're increasingly important to organizations as employees use personal, unmanaged devices to access corporate networks from new, disparate locations, which creates even more cloud security risks.

As an integral part of a SASE solution, CASB provides four important functions to help organizations secure their cloud services, including:

- **Visibility:** A CASB solution provides comprehensive visibility of cloud application usage, such as device and location information, to help organizations safeguard data, intellectual property, and users. It also provides cloud discovery analysis, which enables organizations to assess the risk of cloud services and decide whether to grant users access to applications. This allows the organization to establish more granular controls over their cloud environments by providing different levels of access based on a user's device, location, and role within the business.
- **Compliance:** Organizations now have a wide range of cloud supplier options and likely use several different vendors for various solutions. However, organizations remain responsible for ensuring regulatory compliance around the privacy

and safety of their data, regardless of whether they outsource services or manage it themselves. CASBs help organizations ensure compliance with the increasingly stringent, constantly evolving requirements of data and privacy regulations. Using a CASB solution allows organizations to pinpoint the compliance risks they face and understand what they need to do to address those risks.

- **Data security:** On-premises DLP solutions are effective in protecting data but can't extend that protection to cloud services. Organizations therefore must combine a CASB application with their DLP tool to gain visibility of sensitive data moving between and across their on-premises and cloud environments. This enables organizations to monitor user access to confidential information, regardless of where it is on their network. Through a combination of features and technologies like access control, collaboration control, DLP, encryption, information rights management, and tokenization, organizations can minimize the loss of sensitive data.
- **Threat protection:** CASBs enable organizations to protect against insider attacks from authorized users by creating a comprehensive regular usage pattern that can be used as a baseline of normal activity. Using machine-learning techniques, CASBs can then detect unusual activity as soon as a user gains improper access or attempts to steal data. CASBs also use adaptive access control, dynamic and static malware analysis, and threat intelligence to block and prevent malware attacks.

Single Console

Of course, a single-vendor SASE solution should be easily managed from a single management console that provides access to all the features and capabilities of the solution listed above without requiring administrators to switch between different management consoles, dashboards, and command-line interfaces (CLIs).


TIP

This management capability should extend to hybrid on-premises and cloud environments to ensure maximum interoperability and efficiency.

IN THIS CHAPTER

- Securing Internet access for remote and hybrid workers
- Providing secure access to public and private cloud resources
- Protecting SaaS applications and data
- Transforming the branch

Chapter 4
Exploring Single-Vendor SASE Use Cases

Although many vendors may tell you that a Secure Access Service Edge (SASE) deployment is a straightforward "set-it-and-forget-it" process, anyone with any IT experience knows nothing is ever as easy as it seems — and the devil is often in the details. Understanding the primary use cases your SASE solution needs to address is a valuable way to refine your evaluation of potential solutions.

In this chapter, you learn about common use cases and how Fortinet customers are addressing their networking and security challenges with single-vendor SASE.

Secure Internet Access (SIA)

The enterprise attack surface has greatly expanded as remote and hybrid work have now become the status quo, requiring companies to provide workers with direct Internet access from anywhere. Organizations need a solution capable of following, enabling, and protecting users no matter where they or the websites they use are located.

Unlike virtual private networks (VPNs), SASE provides more than an encrypted tunnel to address advanced cyberthreats. SASE includes a portfolio of enterprise-grade security solutions — including a secure web gateway (SWG) to monitor and protect data and applications against web-based attack tactics, firewall-as-a-service (FWaaS), uniform resource locator (URL) filtering, deep Secure Sockets Layer (SSL) inspection to analyze content to and from sites using Hypertext Transfer Protocol Secure (HTTPS), domain name system (DNS) security, anti-phishing, antimalware, and sandboxing — designed to inspect traffic and detect and respond to both known and unknown threats.

CASE STUDY

CUSTOMER SUCCESS STORY

As with many companies today, remote working has become part of "business as usual" for this software company, as has the greater use of cloud-based applications and services. Securing such decentralized working models and tools requires a different approach than traditional perimeter-based security.

Challenges

At the time, the company was using several technology vendors to supply its networking and security systems, each with its associated professional services fees. By consolidating into a single partner, the company hoped to build a more cost-effective approach while also reducing the overall complexity of its networking environment.

Solution

The company invited Fortinet to a selection process along with two competitors. Fortinet won the client on the back of a week-long proof of concept (POC) trial where its technology was tested against alternatives and found to be the better solution. Today, the company has consolidated its networking and security systems on the Fortinet Security Fabric. Its new infrastructure comprises the Fortinet Secure SD-WAN solution, combining the replacement of its multiprotocol label switching (MPLS) connections with integrated on-premises and remote security provided through FortiGate next-generation firewalls (NGFWs).

The solution is controlled and configured centrally through FortiManager, which enables centralized management with automation-driven network configuration, visibility, and security policy management. The company

also benefits from high-performance data analytics, logging, and reporting delivered through the FortiAnalyzer solution.

The company is extending its new security capability to remote workers through 10,000 FortiSASE licenses, enabling secure Internet access for remote users through a cloud-based SWG. FortiSASE further protects the organization by enabling Zero Trust Network Access (ZTNA), which protects applications by only allowing access to trusted identities.

Results

By consolidating onto a single-vendor SASE, the company unlocks a broad range of benefits. Down to just one strategic partner, the business stands to secure a projected 50 percent reduction in the total cost of ownership (TCO) of its network and security environment.

From a security perspective, the company gains from the increased performance, integration, and automation that is enabled by the Fortinet network and security convergence. Importantly, thanks to the FortiSASE single-vendor platform, this security capability extends to remote users, combining seamless, direct secure access to the Internet (and to applications) for workers with complete control for the security team. As a result, employees are benefiting from an improved remote working user experience even as security has been enhanced.

The security team also enjoys an improved user experience. With a consolidated solution, the management of the network and security infrastructure is considerably simplified. In addition, the Fortinet solution increases network visibility for the security team, providing them with complete control over the security infrastructure.

The company started out looking to reduce the cost of its network and the complexity of its multivendor solution. By consolidating networking and security, it has achieved these goals while also benefiting from next-level security for its remote workforce.

Secure Private Access (SPA)

To successfully address modern enterprise requirements, a flexible SASE solution that offers fast and secure connectivity to corporate applications, whether deployed at a private data center or in the public cloud, is essential. A SASE solution with integrated

ZTNA provides explicit per-application access to authenticated users without requiring a persistent VPN tunnel. Granting access based on identity and context, combined with continuous validation, enables effective control over who and what is on the network.

At the same time, a SASE solution should offer the benefit of seamless integration with software-defined wide area networking (SD-WAN) and NGFW solutions to enable a superior user experience for corporate applications by automatically finding the shortest path to those resources — powered by intelligent steering and dynamic routing capabilities from the SASE points of presence (PoPs).


TIP

Look for a single-vendor SASE solution that only requires a single agent, combining traffic redirection, ZTNA, endpoint protection, and more in a single tool.


CASE STUDY

CUSTOMER SUCCESS STORY

Wellington Catholic District School Board (WCDSB) consists of 18 elementary schools, 3 secondary schools, and an alternative education program. The board meets the educational interests of more than 8,000 students across 26 sites in the City of Guelph and the County of Wellington in Ontario, Canada.

Challenges

In 2017, the Ministry of Education in Ontario launched the "Broadband Access for All Students" initiative, with the goal of delivering one Megabit per second of connectivity to every student across the province.

Solution

To meet this goal, WCDSB deployed the Fortinet Secure SD-WAN across its 26 locations. As a result, the district could use broadband Internet links instead of its legacy MPLS connections, which were more expensive to run.

Peter VanDorp, Cybersecurity Analyst at Wellington Catholic District School Board, explains that this change led to an immediate benefit for end users: "We no longer had to filter based on whether applications were using too much bandwidth. Thanks to Fortinet, we only

need to block when there is a legitimate need, not because the network cannot handle it."

Today, the district uses almost entirely Fortinet Security Fabric solutions for its security and network infrastructure including the FortiGate NGFWs, FortiSwitch secure Ethernet switches, FortiAP access points, FortiManager centralized management, FortiAnalyzer for logging and analysis, the FortiNAC network access control agent, and the FortiClient endpoint agent.

In 2021, the Ministry of Education in Ontario created a reference architecture for schools within its jurisdiction to secure remote learning for staff and students as a result of the COVID-19 pandemic. Within that reference architecture was a recommendation to work with cloud-based SASE solutions.

VanDorp explains: "The aim of the reference architecture was to ensure that school districts could provide exactly the same level of protection for students and staff outside of schools as they are used to on school premises. That meant finding the right balance between locking down the network and ensuring that users could work and study freely."

Offering remote learning capabilities on this scale was a significant challenge. "At that time, we had great security within the network perimeter thanks to the Fortinet Secure SD-WAN," says VanDorp, "but apart from providing VPN tunnels back to our FortiGate NGFWs for some of our office staff, we had no remote working capability at all."

As outlined in the Ministry's reference architecture, SASE could provide a solution to this challenge. As a cloud-based solution, it can simplify the management and configuration of the security processes required for remote learning including endpoint protection, extending antivirus across the distributed perimeter, and putting in place robust deep packet inspection (DPI) capabilities.

Other business drivers for moving to a SASE architecture included leveraging managed solutions to free internal resources from configuring and maintaining devices to focusing on security strategy, delivering a predictable pricing structure with lower and simplified budgeting, and increasing scale, control, and flexibility in security and networking.

(continued)

(continued)

Results

By selecting its installed security partner for its SASE evolution, the district has realized significant time savings. "There was a minimal learning curve for us with FortiSASE," comments VanDorp. "That meant we could deploy much faster, which saved us time and money." The district has unlocked a 30 percent reduction in overall TCO in part due to the smooth integration of FortiSASE, as well as savings in training time, which amount to 2,000 hours annually.

VanDorp adds: "By partnering with Fortinet, we deployed SASE while cutting costs. We essentially shifted our FortiClient investments into our new SASE capability."

Moving to FortiSASE has made it far easier for the board's IT team to manage the district's security and network infrastructure. As VanDorp explains: "FortiSASE delivers true single-pane-of-glass management, and we have found it easy to use. We can now deploy DPI with a single click of a button, which saves us time and effort."

Being able to manage and address everything from a single location is particularly important for WCDSB as it only has a small team, and resources are tight. "In education, every dollar that we spend on technology is a dollar that is not going to the classroom for learning. That is always something that is back of mind," VanDorp adds.

A core aim of this deployment was to ensure that staff and students have everything they need for secure, effective digital learning. VanDorp reports that the user experience has improved dramatically following the implementation of FortiSASE, so much so that the IT team regularly receives positive feedback from end users.

Secure SaaS Access (SSA)

A SASE solution must enable secure access to critical resources regardless of where applications, devices, users, and workloads are located. With growing enterprise dependence on software-as-a-service (SaaS) applications, an effective cloud-delivered security solution must protect mission-critical data and secure and safeguard cloud-based information. An effective solution should

support next-generation dual-mode CASB, supporting both inline and application programming interface (API) based capabilities to overcome shadow IT challenges and secure critical data. With this in mind, look for a SASE solution that offers visibility into key SaaS applications, provides reports of risky applications, ensures granular control of applications to secure sensitive data, and detects and remediates application malware across both managed and unmanaged devices.

REMEMBER

Shadow IT refers to IT activities undertaken outside of the typical IT infrastructure and typically without the IT or security department's knowledge or explicit authorization. In most cases, shadow IT involves users "doing it themselves" when it comes to IT including downloading, installing, and running their own applications (either in the cloud or on their local devices), troubleshooting issues, and managing security configurations. Potential shadow IT risks include:

- Data loss and inconsistent data
- Regulatory compliance issues
- Unknown and unpatched security vulnerabilities
- Insufficient and/or ineffective security measures
- Unplanned downtime
- Inefficient procurement
- Undocumented/unofficial "shadow" business processes

CASE STUDY

CUSTOMER SUCCESS STORY

This customer is one of the largest assisted reproduction groups in the world. It currently has more than 100 clinics in 12 countries and is the leading center for reproductive medicine.

Challenges

The problem was that its security system, which was centered on a basic proxy tool, only provided a bare minimum of protection to users. The organization's security team was also concerned that they had little control of employees' devices when they worked outside of the company's branch locations. The security team, therefore, went

(continued)

(continued)

on the hunt for a more secure way to enable its global remote workforce to access software-as-a-service (SaaS) applications securely.

Solution

They had long been a Fortinet customer, having deployed FortiGate NGFW devices to provide industry-leading security and protection at the network edge. In addition, the organization uses FortiAnalyzer as a tool for logging and reporting. Based on its exceptional experiences with Fortinet technology and expertise, the company invited Fortinet to propose a solution to its remote working security requirements.

Following a successful POC, and in close cooperation with Fortinet system engineers, they deployed FortiSASE, the Fortinet single-vendor SASE solution.

FortiSASE is an architecture that combines networking and security capabilities for remote users with secure Internet, cloud, and data center network access. FortiSASE comprises technologies including Firewall-as-a-Service (FWaaS), SWG, ZTNA, and cloud access security broker (CASB). And, it offers a consistent user experience for both on-premises and remote security to reduce security gaps and configuration overhead.

Results

The combination of FortiSASE and ZTNA is proving the perfect mix for them to achieve their security goals for remote workers. The FortiSASE agent-based approach is a significant improvement to the company's legacy proxy solution, supporting multiple use cases including endpoint protection, ZTNA, and traffic redirection, which enables the company to maximize remote worker security from the cloud.

As well as being the perfect fit from a security perspective, the Fortinet licensing approach, which is based on each device agent, is ideal for the client's deployment.

Finally, the expertise of Fortinet systems engineers proved to be a significant benefit throughout the rollout of the solution. The Fortinet

team worked closely with the client to conduct field tests during the POC phase, and to ensure that the end solution met the client's requirements perfectly.

By extending Fortinet security protection to the cloud with the FortiSASE solution, this global healthcare provider has ensured business continuity for all employees and the devices that regularly access SaaS applications, as well as the company business applications. The result is a remote working solution that is more secure than its legacy solution and provides a better end-user experience.

Branch Transformation

Over the past decade, organizations have embraced the cloud. This strategic trend has impacted network traffic patterns at branch offices. Traditionally, enterprises have adopted a router-centric approach using Multiprotocol Label Switching (MPLS) circuits to connect branch offices securely and reliably to a central headquarters or datacenter location, where their applications were hosted. However, this approach isn't suitable for accessing cloud applications because it adds latency as all traffic is inefficiently backhauled through the datacenter rather than directly to the cloud application, thereby causing an unpredictable user experience.

To transform the branch experience, organizations are increasingly using SD-WAN to drive intelligent application steering at the branch office. A secure local Internet breakout is also needed to ensure all traffic is inspected, including encrypted traffic, to protect the branch, its users, and their devices. A secure SD-WAN solution, powered by one operating system and unified management, that can transform and secure the network — while providing the flexibility to enable organizations to transition to SASE, is critical to minimizing disruptions and protecting existing investments.

CASE STUDY

CUSTOMER SUCCESS STORY

Waste Management, Inc. is the nation's largest waste management and environmental services company providing services that range from collection and disposal to recycling and renewable energy generation. Founded in 1968, the company is headquartered in Houston, Texas. Its more than 43,000 employees support nearly 21 million residential, industrial, municipal, and commercial customers throughout the United States and across Canada.

Challenges

It was imperative that Waste Management had the capability to expand and contract network communications as needed. By converting their router-based WAN infrastructure to the Fortinet Secure SD-WAN solution, Waste Management was able to leverage the Fortinet Security Fabric to tie its security and networking elements together.

Solution

Waste Management, Inc. deployed Fortinet SD-WAN and SD-Branch solutions. "Waste Management is using Fortinet Secure SD-WAN and SD-Branch solutions to build an efficient, scalable, and secure architecture that can seamlessly span our entire distributed operations. Efficient and scalable SD-WAN connectivity and an integrated security architecture managed through a single-pane-of-glass provide enhanced visibility and control and scalable protection against today's growing cybersecurity risks — all while significantly reducing our operational expenses," says Erika Walk, Senior Director Digital Business Services at Waste Management, Inc.

Results

Adopting Fortinet SD-WAN and SD-Branch solutions for branch transformation has enabled Waste Management, Inc. to reduce overall cost by 65 percent, improve performance by close to 38 times, increase visibility to reduce time to remediate user-impacting issues, and eliminate expensive third-party services with a single interface and unified management of SD-WAN optimization and security.

IN THIS CHAPTER

- Embarking on the secure networking journey
- Introducing Fortinet Universal SASE
- Simplifying management and delivering superior user experiences
- Connecting wireless, wired, and 5G to SASE
- Correlating events and response with unified logging and automation
- Taking advantage of the cloud consumption model
- Enabling enterprise-grade, best-in-class security

Chapter 5
Going Further with Fortinet Universal SASE

In this chapter, you learn about Fortinet Universal Secure Access Service Edge (SASE) — Fortinet's vision for expanding single-vendor SASE.

The Secure Networking Journey

Single-vendor SASE is a journey that starts with next-generation firewalls (NGFWs) and software-defined wide-area networking (SD-WAN). Fortinet Universal SASE extends the single-vendor SASE approach to additional use cases including on-premises infrastructure and remote users, delivering a comprehensive SASE offering to secure users, access, edges, and devices anywhere, while delivering a robust return-on-investment (ROI),

consistent security posture, and improved user experience. Driven by a security and networking convergence approach, Universal SASE enables a simple, secure networking journey.

Most Comprehensive SASE Solution

Fortinet single-vendor SASE offers a full set of networking and security capabilities including secure web gateway (SWG), universal zero-trust network access (ZTNA), next-generation dual-mode cloud access security broker (CASB), firewall-as-a-service (FWaaS), and Secure SD-WAN. Powered by FortiOS, FortiGuard artificial intelligence (AI) powered security services, unified management, and a unified agent drive operational efficiency and deliver consistent security everywhere. Single-vendor SASE ensures the utmost security for all edges, devices, and users, whether they are accessing the web, corporate applications, or software-as-a-service (SaaS) applications.

Fortinet broadens its single-vendor SASE approach and introduces Universal SASE (see Figure 5-1). Universal SASE is a comprehensive SASE offering — securing users, access, edges, and devices anywhere while delivering a robust ROI, consistent security posture, and improved user experience. Powered by the unique Fortinet security and networking convergence approach, it offers organizations a simple secure networking journey towards SASE.

Universal SASE offers a cutting-edge AI-powered solution specifically designed for the hybrid workforce, combining the power of cloud delivery, unified management, and logging, with comprehensive features such as Universal ZTNA, SD-WAN integration, OT/IoT security, LAN/WLAN/5G security, and Digital Experience Monitoring with a flexible licensing model.

The following sections discuss the features and capabilities of the Universal SASE solution.

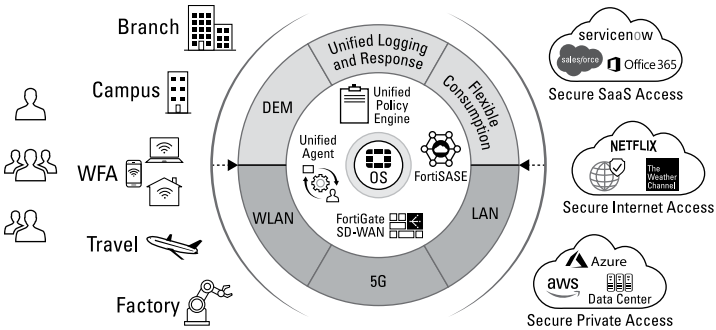


FIGURE 5-1: Fortinet Universal SASE.

Unified Management and Digital Experience Monitoring

Universal SASE enables visibility across both on-premises and remote users, ensuring the security of the modern hybrid workforce. With FortiManager, organizations can leverage a unified policy engine and management system that spans all edges and users, regardless of their location.

FortiAnalyzer, in conjunction with Fortinet SASE, provides centralized logging and response capabilities for networking and security across the entire organization. This enables organizations to gain a complete understanding of their network and security events, facilitating effective incident response and mitigation.

By incorporating FortiMonitor, Universal SASE offers Digital Experience Monitoring (DEM) functionality, which empowers organizations with unified visibility into users' experiences as they interact with applications and devices. DEM encompasses endpoint devices, on-premises networking, users, and applications, enabling organizations to obtain a comprehensive view of the end-user experience and translate it into measurable business outcomes.

REMEMBER

Fortinet Universal SASE, together with FortiManager, FortiMonitor (DEM), and FortiAnalyzer, empowers organizations with the necessary tools to overcome the challenges associated with hybrid work, including ensuring complete visibility, consistent security, and optimum end-user experiences.

Expanded Edge and Access Integration with Wireless, WLAN/5G, OT/IoT, and Switching

FortiAP secure WLAN access points, together with FortiExtender WLAN/5G products and FortiSwitch next-generation switches, integrate with Fortinet Universal SASE, providing LAN/wireless WAN (WWAN)/5G integration with SASE. This enables secure microbranches where access points (APs) or switches send traffic to the FortiSASE solution for comprehensive security of all devices at the site, without the need to install any other software or agent for consistent experience.

TIP

A recent survey found that 42 percent of OT security professionals believe that lack of visibility is the biggest challenge for managing OT risks. Because it is impossible to protect the network from a threat you can't detect, complete real-time visibility across the organization is a crucial first step in securing endpoint devices.

Universal SASE profiles every endpoint connected to the network, including the physical location and type of device. Universal SASE can alert the security admin about a compromised OT or IoT device and secure them seamlessly with support for IoT signatures and securing OT/IoT devices connected at the edge via FortiExtender.

Unified Logging and Response

FortiAnalyzer provides centralized logging and response capabilities for networking and security across the entire organization. This enables organizations to gain a complete understanding of their network and security events, facilitating effective incident response and mitigation.

With advanced logging and reporting capabilities, FortiAnalyzer centralizes security analytics across the Fortinet Security Fabric and provides security automation via Fabric Connectors and application programming interfaces (APIs). It also includes easy-to-implement security workflow automation to accelerate operations.

These unique features enable an organization to maximize the impact and effectiveness of a lean security team without extensive

configuration. FortiAnalyzer, a core part of the Universal SASE, force multiplies teams, simplifies security operations, and allows enterprises at any stage of security operations center (SOC) maturity to smoothly integrate security visibility and automation.

Flexible Consumption

With single-vendor SASE, organizations can shift their investment costs from capital expenditure to operating expenditure, enabling a more flexible pay-as-you-go consumption-based model that aligns to your business growth and evolving requirements. A simple tiered licensing model enables organizations to predict a cost-to-business growth correlation and use of security — rather than tying up capital in excess hardware.


TIP

Universal SASE brings even more flexibility in purchasing and budgeting by also being part of the FortiFlex program. FortiFlex is a points-based licensing program that delivers the capability for organizations to dynamically adjust the deployment of solutions and services. As a result, organizations gain flexibility to deploy only what they need and shift services as requirements change. Points are charged based on daily use. FortiFlex delivers usage-based licensing designed to empower organizations with the flexibility to right-size their services and spend in securing their cloud and hybrid environments. FortiFlex simplifies deployment decisions with the freedom to dynamically deploy, scale in/out, and scale up/down without needing to size for exact services and solutions ahead of time.

Best-in-Class Security Everywhere

Fortinet Universal SASE brings:

- Operational efficiency in today's complex environment
- Consistent security across on-prem and remote users with unified management and analytics
- Fully integrated and comprehensive networking and security solutions for all edges, users and devices
- Simplified licensing and usage-based pricing for flexible and planned budget and purchasing

Chapter 6
Ten Evaluation Criteria for Single-Vendor SASE

Here are ten important criteria and business benefits you should consider when evaluating a single-vendor SASE solution.

Unified Management

A cloud-based SASE management system should provide comprehensive visibility, reporting, logging, and analytics to ensure efficient web security operations and reduce mean time to detect (MTTD) and mean time to respond (MTTR). However, having yet another management console to monitor may place unnecessary burdens on IT teams, especially if SASE security elements operate as siloed point solutions.


TIP

The key to limiting the financial damage associated with a data breach is to reduce MTTD and MTTR. According to the IBM Security *Cost of a Data Breach Report 2022*, the average total cost of a data breach in the U.S. is 9.44 million and the average data breach lifecycle (MTTD + MTTR) is 277 days. Organizations that successfully reduced the data breach lifecycle to less than 200 days were able to reduce the average cost of a data breach by nearly 27 percent.

For organizations managing a hybrid environment, SASE remote user management should converge with on-premises management. Such consolidation can be even more effective when components deployed in the SASE cloud can interoperate with on-premises solutions, ensuring consistent policy orchestration and enforcement.

REMEMBER

SASE technologies should be easily integrated into the organization's larger network and security architecture rather than working as a one-off solution. Ideally, the security protocols and policies within the SASE solution should be identical to those used elsewhere in the network.

Leading Security

When assessing any SASE solution, the functionality and performance of its security elements need to be effective. A complete, single-vendor SASE solution should include the following full stack of security capabilities and tools. Also, it is important to make sure that every single SASE Point of Presence can provide the entire security stack for improved performance and response time.

- **Firewall-as-a-service (FWaaS):** Any SASE solution should include a next-generation firewall (NGFW) that delivers high-performance secure sockets layer/transport layer security (SSL/TLS) inspection and advanced threat detection techniques via the cloud, establishes and maintains secure connections for distributed users, and analyzes inbound and outbound traffic without impact on user experience.
- **Domain name system (DNS) security:** DNS security identifies and isolates malicious domains to prevent threats from entering the network.
- **Intrusion prevention system (IPS):** IPS should be used to actively monitor the network, looking for malicious activities attempting to exploit known vulnerabilities.
- **Data loss prevention (DLP):** DLP prevents end-users from moving sensitive information outside the network — whether maliciously or accidentally — to ensure that the network and data are both secure.

- **Secure web gateway (SWG):** SWG secures web access against both internal and external risks. It also needs to automatically block threats, even those embedded in encrypted traffic — including TLS 1.3 — with high-performance SSL inspection.
- **Zero-trust network access (ZTNA):** Enterprise-grade security should be added on top of virtual private network (VPN) and extend ZTNA to work from anywhere (WFA) users. This allows the SASE solution to inherently integrate with preexisting VPN solutions and extend zero-trust application access to off-network users.
- **Sandboxing:** Whether sandboxing is executed in the cloud or on an appliance, it provides crucial protection, especially against previously unknown threats.
- **Cloud access security broker (CASB):** CASB provides visibility, compliance, data security, and threat protection for cloud-based services used by an organization. It provides policy-based insights into users, behaviors, and data stored in SaaS applications.

Reliable Vendor

As cyberthreats continue to evolve and become increasingly sophisticated, security vendors must invest in both new and existing solutions to counter these threats. Look for a single-vendor SASE that has a broad portfolio of security solutions that are fully integrated in a unified fabric, demonstrating an ongoing commitment to its SASE solution rather than a "one-off" siloed solution.

Unified Agent

Onboarding a different agent for each use case can quickly become complex and expensive to maintain. A SASE solution should provide a single agent that can be used for multiple use cases — including secure Internet access (SIA), secure private access (SPA), and secure software-as-a-service (SaaS) access (SSA) — while automatically redirecting traffic to protect assets and applications through cloud-delivered security.

REMEMBER

Simplifying the user experience is always key to successful adoption in any security or networking solution. Look for a SASE solution that provides a unified agent for all endpoint security features and secure connectivity to the cloud and the applications. A unified agent simplifies operations and improves overall user experience.

Validated by Third-Party

Cybersecurity solutions like single-vendor SASE help enterprises protect their data and employees. But with so many vendors to choose from as well as layers of marketing hype, footnoted claims, and qualified conditions, it's not surprising that chief information officers (CIOs) and chief information security officers (CISOs) often get confused when evaluating the right cybersecurity solutions for their business.

The good news is that there are objective sources of information that can help organizations make more informed purchasing decisions. Third-party testing and validation can help CIOs and CISOs find security solutions that do what they say they do and meet the specific infrastructure needs of their organization.

Unbiased, third-party testing involves evaluation by qualified, independent researchers with data-driven guidance to help organizations ensure security efficacy across a broad spectrum of solutions. Because organizations often don't have the time or resources to do in-depth testing on their own, third-party testing gives them objective data to make informed decisions about the products they need to protect their critical assets.

REMEMBER

For years, Fortinet has been committed to independent testing and validation. Rigorous and reputable outside evaluation is critical to raising the bar for the security industry as a whole and helps ensure that our customers can make informed buying decisions.

Validated by the Market

Look for a SASE vendor that is proven in the market — as evidenced by a growing customer base and increasing market share over time. Although new players may introduce innovative new

solutions to the market, it's important to work with a security vendor that has a proven track record and a demonstrated commitment to its customer base. Peer reviews and analyst validation/reports also provide valuable insights.

Deep, Native Integrations

Most organizations will continue to operate a hybrid network for the foreseeable future, combining traditional IT infrastructure with cloud-based resources. However, vendor sprawl within these enterprise environments reduces visibility and control.

Security and networking components that operate in siloes can't be automated, and SASE solutions that don't work with the rest of the network mean that IT teams can't track and secure communications end to end. Rather than trying to build a multivendor SASE solution, with its attendant challenges for implementation, integration, and management, look for a single-vendor solution that converges networking and security into a unified solution out of the box.

A single-vendor SASE solution should offer deep native integrations with all SASE components including secure software-defined wide area networking (SD-WAN), secure web gateway (SWG), Firewall as a Service (FWaaS), zero-trust network access (ZTNA), and cloud access security broker (CASB).

Lower TCO and OPEX model

Organizations recognize that they must converge networking and security to reduce complexity and overhead while enabling the agility and flexibility they need to adapt to the rapidly evolving digital marketplace. While the direct savings associated with vendor consolidation — including fewer licensing fees and maintenance costs — are relatively obvious, other significant and tangible saving are perhaps less apparent, such as reduced complexity, lower support costs, and consistently superior user experiences leading to greater productivity — all driving a lower total cost of ownership (TCO) in single-vendor SASE.

Organizations are also looking into moving to an operating expense (OPEX) model for controlled budget and easy purchasing, and they should look for solutions that provides user-based licensing and flexible purchasing.

Improved User Experience

A SASE solution must also seamlessly hand off connections between the cloud and on-premises devices, allowing access and security policies to follow the user rather than terminating at the edge of the network. Only by converging networking and security end to end can organizations implement a comprehensive zero-trust architecture. Extending the unique approach of security-driven networking to the cloud edge ensures consistent security and superior user experience everywhere.

REMEMBER

Consistent network operations and security controls enable superior user experiences for workers, whether they are on or off the network.

Simple Purchasing and Onboarding

SASE considerations should not just focus on how it is used, but also on how you pay for it. Simple tiered licensing with usage-based payment enables organizations to predict a cost-to-business growth correlation and use of security, rather than tying up capital in excess hardware. Simplified onboarding and endpoint management should combine efficient operations with granular analytics and include pre-generated and on-demand reports — including granular logging and events across user, endpoint, and applications for efficient troubleshooting.

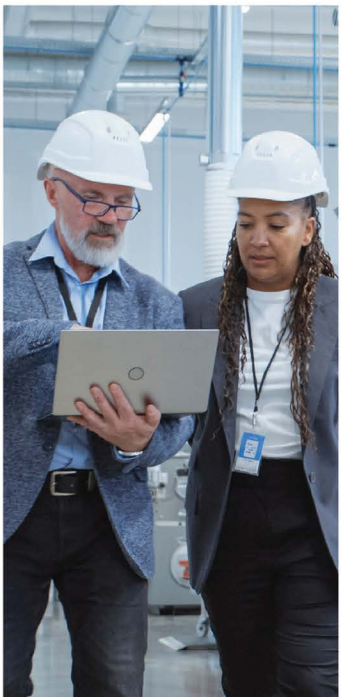
FORTINET

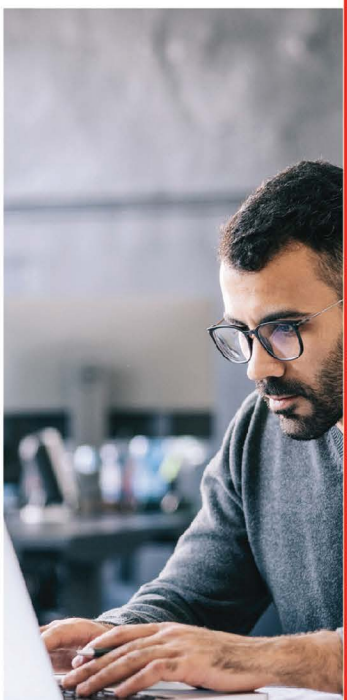
Fortinet Universal ZTNA

FortiSASE includes ZTNA for remote users and branch locations, but ZTNA should not be a "sometimes" policy. ZTNA policies should control user access to applications from any location, which is why Fortinet enables Universal ZTNA. Universal ZTNA applies ZTNA checks for every application session and continues to verify users and devices, no matter where the user is located.

Learn more about Universal ZTNA and Zero Trust Access with the Dummies Guide to Zero Trust Access (2nd Edition).

Learn more at www.fortinet.com/ZTNA





Provide secure, reliable, and consistent access to corporate assets

This book introduces you to single-vendor SASE — the delivery of networking and security capabilities from one vendor in a unified solution. It's a prime example of consolidation that helps network and security teams drive operational efficiency, reduce costs, and eliminate needless complexity. Who doesn't want that?

Inside...

- Examine security gaps created by a hybrid workforce model
- Simplify consumption and management
- Reduce complexity with a single, unified console
- Secure access for remote and hybrid workers
- Correlate events and response with unified logging and automation

FORTINET

Lawrence Miller 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 200 *For Dummies* books on numerous technology and security topics.

ISBN: 978-1-394-22516-3
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.