Brought to you by

CISCO

Secure Access Service Edge (SASE)

for dummies®
A Wiley Brand

3rd Cisco Special Edition

Explore the benefits of SASE

Provide secure user experiences

Reduce cost and complexity

Lawrence Miller

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that is revolutionizing the way organizations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry leading AI-powered solutions and services, Cisco enables its customers, partners and communities to unlock innovation, enhance productivity and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all. Discover more on The Newsroom and follow us on X at @Cisco.

Cisco SASE offers a unified, single-vendor approach for secure hybrid work. Combining market-leading SD-WAN with powerful Secure Access (SSE), Cisco delivers a seamless and secure user experience everywhere. This integrated approach consolidates tools, boosts security efficacy, enhances agility, and provides end-to-end visibility. Cisco SASE is a core part of our Universal ZTNA strategy, extending zero trust access across your entire environment – users, devices, and applications – powered by deep integrations with identity and network controls. Register for a live workshop where you'll get hands-on access to Cisco's SASE solution and get ready to accelerate your journey to zero trust.

Secure Access Service Edge (SASE)

3rd Cisco Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Secure Access Service Edge (SASE) For Dummies®, 3rd Cisco Special Edition

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

ISBN 978-1-394-36668-2 (pbk); ISBN 978-1-394-36669-9 (ePDF);
ISBN 978-1-394-36670-5 (ePUB)

Publisher's Acknowledgments

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager: Jeremith Coward

Content Refinement Specialist: Umeshkumar Rajasekhar

Introduction

Today's IT teams face a common challenge: figuring out how to securely connect and enable roaming users, devices, and software-as-a-service (SaaS) apps without adding complexity or degrading end-user performance. Likewise, users in remote and branch offices expect the same user experience and level of network performance and security as users in central locations. IT must develop strategies to connect and protect users — wherever they work and on any device they use — from a variety of threats, including identity-based attacks, malware infections, command-and-control callbacks, phishing attacks, unauthorized access, and generative artificial intelligence (GenAI) app usage among others.

This book delves into the proven way to balance security, the user experience, and complexity: secure access service edge (SASE). As a tested and mature architecture, it delivers software-defined connectivity and multiple security functions from the cloud that are simple, scalable, and flexible to meet the unique needs of your business.

The goal of this book is to help you gain a deep understanding of the latest trends, the new challenges they bring, and how technologies have evolved to address them, including the need for flexible zero-trust enforcement. Finally, the book comes full-circle to show how Cisco's SASE approach can help your business today and in the future.

About This Book

This book is composed of six chapters that explore:

- Key networking and security trends and their associated challenges (Chapter 1)
- Different networking and security options and key considerations (Chapter 2)
- How an SD-WAN architecture addresses modern networking challenges (Chapter 3)
- How a security service edge (SSE) complements SD-WAN security components and addresses today's security challenges (Chapter 4)

- The Cisco approach to SASE (Chapter 5)
- Key SD-WAN and cloud security takeaways (Chapter 6)

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

Icons Used in This Book

Throughout this book, you'll 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 — along with anniversaries and birthdays!


TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff nerds are made of!


TIP

Tips are appreciated, 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 to help you avoid potentially costly or frustrating mistakes.


CASE STUDY

This icon points out specific use cases for SASE technology.

Beyond the Book

There's only so much information that can fit in 48 short pages, so if you find yourself at the end of this book thinking, "Gosh, this was an amazing book; where can I learn more?" check out `https://www.cisco.com/site/us/en/solutions/secure-access-service-edge-sase/index.html`.

IN THIS CHAPTER

- Considering how networking and security have changed
- Addressing modern network and security challenges

Chapter 1
Networking and Security: Evolution and Challenges

Today's enterprise network must meet the demands of secure, agile, high-performing, and on-demand cloud connectivity. To do this, the market has moved on from single-purpose point products to multifunction networking and security solutions tightly integrated in a cloud service offering.

But you still need to deploy security services how and where you choose with the capability to control and secure direct-to-Internet access, cloud applications, Internet of Things (IoT), and central, remote, and roaming users alike — without the need for additional hardware. As organizations adopt artificial intelligence (AI)-powered tools, including generative (Gen)AI, they grapple with new challenges around governanace, data safety, and compliance. In parallel, identity attacks are surging, exploiting gaps in fragmented frameworks. Additionally, companies are being held accountable for managing both new technologies and security with global privacy mandates that demand real-time visibility and control over who accesses what, and from where.

This chapter expands on these trends and the challenges that have defined secure access service edge (SASE) as the go-to approach.

The Way We Work Has Changed

Several key trends have reshaped the networking and security landscape.

Secure, multicloud networking

Organizations are looking to converged networking and security solutions in order to be more agile and resilient in the face of heightened disruption and uncertainty


TIP

According to Cisco's 2024 *Global Networking Trends Report*, organizations are prioritizing integration of networking and security domains. The study found that 76 percent of organizations plan to deploy a SASE architecture that integrates SD-WAN and SSE in the next two years and 52 percent said that the integration of network security into broader IT functions is their top priority.

Hybrid work/return to office

With hybrid work as a mainstay and return-to-office mandates on the rise, organizations need the tools to provide seamless, secure access for employees, contractors, third-parties, and IoT devices, no matter the location. The days of all users working together in the same place — company headquarters — are long gone. As organizations expand into new markets, acquiring smaller companies and their office footprints, the number of remote and branch offices grows, too. Remote office employees need to be protected as well as their counterparts at main office locations, even if their network traffic is going directly to the Internet instead of backhauling it to the corporate data center.


REMEMBER

A branch office is a dedicated business (non-home) site that has more than one employee. This location may be connected to a central data center via a wide-area network (WAN) or may connect directly to the Internet. Branch offices typically receive some level of technology support from headquarters locations and most (although not all) typically have one or more on-site servers to provide users with file, print, and other IT services.

Some branch office locations may be connected to a main office over a multiprotocol label switching (MPLS) WAN link. However, it's common for remote offices to connect to the main office over a virtual private network (VPN), and a secondary direct Internet access (DIA) link may serve as a backup to the primary MPLS link. Additionally, branch offices may use DIA links — going directly to the Internet and bypassing the VPN — which can create security gaps if not properly managed with the right set of security functions.


TIP

As companies become more decentralized, the growing population of remote workers and branch offices needs a proven network and security method that meets all needs of the diverse user group.

Roaming users

Laptop computers have supplanted desktop computers to become the primary endpoint for many business users. In addition, mobile computing has untethered workers as mobile devices have become more powerful than many desktop computers and their use has proliferated.

Because of these technology trends, many forms of work can now be performed from practically anywhere, and organizations increasingly recognize that work is an activity, not a place. According to Cisco's *2024 Cybersecurity Readiness* Index, 91 percent of employees across organizations are using multiple networks to connect to work. In fact, nearly one in three employees (29 percent) move between at least six networks weekly. This makes security professionals nervous — around four out of five organizations (82 percent) cite remote logins as a heightened threat vector, with the main concerns being the use of unsecured Wi-Fi networks, the inability to monitor threats across multiple networks, and the use of unmanaged devices.


REMEMBER

A *roaming user* is any worker who works from a home office or from another noncorporate location (such as at a customer's office or on the road). Roaming users may use corporate-owned devices and/or personal devices, accessing the corporate network via a VPN or connecting directly to the Internet to access cloud applications in order to perform their job functions.

More network traffic

New apps, including public cloud storage, video conferencing, and GenAI, are data-intensive and generate large amounts of network traffic to support the increasing demand from employees. This increased traffic load is putting an ever-greater strain on existing network infrastructure and centralized security processes. This increased strain can reduce performance, lower productivity, and hinder the overall user experience. The load isn't the only consideration. Users need secure access to applications, but for GenAI in particular, organizations may not have the necessary controls to protect from data leakage and other risks as employees overshare sensitive information.

Understanding Networking and Security Challenges

This past decade has also presented many new networking and security challenges requiring innovative solutions to address them effectively.

Rising costs of traditional networking architecture

The traditional function of a WAN was to connect users at the branch or campus to applications hosted on servers in a centralized data center. Typically, dedicated MPLS circuits helped ensure security and reliable connectivity. However, these dedicated circuits are costly to provision and maintain, especially when compared to the widespread availability of other, less costly transport options available to businesses today.

MPLS is a routing transport that provides high availability and performance, reduces load on routers, and speeds up traffic delivery. MPLS provides more reliable quality-of-service (QoS) for bandwidth-heavy or latency-sensitive applications. MPLS technologies are applicable to any network layer protocol (hence the name, "multiprotocol") and are often used by enterprises, for example, to backhaul business-critical network traffic from branch offices to the data center.

Inefficiencies in the centralized network model

A centralized network model made sense when the enterprise data center was the primary destination for users to access applications and data across the network. Internet traffic was relatively insignificant and could easily be handled over the existing MPLS circuits. Network traffic could be routed and prioritized as necessary to ensure efficient, reliable performance — while limited and expensive IT staff resources such as networking and security teams could centrally manage the network for all locations.

Traditionally, an organization would backhaul (that is, reroute) network traffic from branch offices to headquarters to apply security policies, often using MPLS links. But in the digital era, this approach just isn't efficient. As businesses increasingly adopt software-as-a-service (SaaS) applications, as well as platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) resources and workloads delivered from multiple clouds, the user application experience has suffered. Backhauling Internet-bound traffic to apply security policies at the data center can be slow and isn't an efficient or effective way to handle the unprecedented explosion of Internet traffic that cloud adoption brings.

Traffic destined for the Internet is effectively backhauled across the MPLS network to a headend (such as a corporate headquarters or data center) that directs it through a set of security checks and then provides Internet access. Unfortunately, this process also acts as a bottleneck.

Existing WAN links that backhaul traffic to a security stack in a central location using MPLS are unable to handle increasing bandwidth demands from users who need fast, reliable access to the Internet. To address the growing need for DIA to cloud-based apps, many organizations are either investigating, or already using, broadband DIA at branch locations instead of backhauling this traffic over MPLS. TeleGeography, a global telecommunications market research and consulting firm, reported in its 2024 *WAN Manager* survey that DIA is gaining ground on MPLS, with 49 percent of sites using DIA compared to 41 percent for MPLS. Although these DIA links address performance issues associated with backhauling traffic to a headend location, they're often provided by local Internet service providers (ISPs) as broadband links. It's important to check into resiliency, QoS prioritization, and service level agreement (SLA) guarantees.

Performance issues with "run-the-business" SaaS apps

Many SaaS apps today, like Salesforce, Microsoft 365, and Workday (to name a few), have become core "run-the-business" enterprise apps. Backhauling SaaS traffic to a corporate headend creates network congestion and latency. This, in turn, causes performance issues that result in lost productivity and user frustration. Complexity in the WAN may cause additional performance issues due to less-than-optimal routing decisions, improper traffic classification and prioritization, and inefficient policy enforcement.


TECHNICAL STUFF

Modern SaaS applications are often built on a microservices architecture that can be comprised of hundreds, or even thousands, of microservices spanning multiple cloud locations. Each of these microservices has the potential to add latency as data travels back and forth between them and the application.

When users experience performance issues with corporate-approved apps, they often turn to unauthorized and potentially risky apps to get their jobs done. This shadow IT (or shadow AI if GenAI is involved) culture in which the IT department — and security controls — are circumvented is a big problem. According to a survey conducted by `Beezy.net`, 32 percent of employees use shadow IT, such as unapproved communication and collaboration tools to perform work. More than 1,200 cloud services are used in the average large enterprise today, and the Enterprise Strategy Group reports that as much as 98 percent of those services are unsanctioned and unvetted SaaS apps.

Too many siloed IT tools and integration challenges

IT teams are frequently inundated by mountains of data from stand-alone, point connectivity, and security products that don't integrate with other products and require different knowledge levels and skill sets to operate and maintain. In fact, Cisco's 2024 Cybersecurity Readiness Index reported that 67 percent of organizations indicated they have ten or more solutions deployed in their security stacks, and a staggering 80 percent acknowledge that multiple point solutions impede their team's efficiency in detecting, responding to, and recovering from security incidents.

This becomes even more complex when headcount is limited — 46 percent of companies reported to have more than five positions unfilled at the time of the survey. This lack of integration, interoperability, and people-power makes it difficult, if not impossible, for IT personnel to manage the network and monitor and correlate security and threat information in realtime.

REMEMBER

These challenges have grown exponentially as connected branch and remote offices have proliferated. Each location typically requires a router and firewall at minimum. In remote and branch locations, these devices are often purchased as commodity components that provide limited functionality and remote management capabilities. When implementing DIA at remote locations, there is a need to deliver the right level of security to users — web security, firewalls, data loss prevention, and so on. However, it may not be practical and cost-effective to buy a separate stack of security appliances for each location. Even if some of these components in branch locations do include security tools, there are usually no IT personnel in these locations to maintain them. To improve security of these dynamic environments, security measures will need to be shifted to the cloud where they can be applied and managed centrally.

Security talent shortage and increasing personnel costs

The worldwide shortage of security professionals and the high ongoing investment necessary to train and retain qualified security staff is a very real problem for organizations everywhere. The World Economic Forum's Global Cybersecurity Outlook 2025 reported that 67 percent of organizations reported a moderate-to-critical skills gap in cybersecurity.

New cyberthreats taking advantage of security gaps

Advanced cyberthreats, including ransomware, remote access Trojans (RATs), and advanced persistent threats (APTs), have evolved to take advantage of the lack of visibility and control in the modern hyperdistributed network. Remote and branch users are particularly susceptible to many of these threats because

organizations have moved away from a centralized security model and are often unable to enforce consistent security policies across the network. Limited security capabilities and IT staff in remote locations make these users even more susceptible to a successful breach or attack. Cybercriminals understand that remote workers are typically more vulnerable and thus target remote locations and roaming users.

WARNING

According to Cisco's *2024 Cybersecurity Readiness* Index, approximately four out of five organizations (82 percent) cite remote logins as a heightened threat vector, with the main concerns being the use of unsecured Wi-Fi networks, the inability to monitor threats across multiple networks, and the use of unmanaged devices.

TIP

Modern organizations need to consider innovative networking and security options to successfully address the challenges in today's enterprise network. You can find more information on this in Chapter 2.

IN THIS CHAPTER

- Using MPLS where needed
- Getting innovative with SD-WAN
- Addressing security threats with SWGs and SIGs
- Introducing the secure access service edge

Chapter 2
The Evolution of Networking and Security Solutions

The convergence of network and security technologies and workflows is now a top priority. It's also a best practice as security concerns expand due to continued cloud adoption. During the pandemic, many IT teams deployed point solutions to meet time-sensitive needs. Although that was manageable in the short term, the long-term problems of inefficiency and complexity needed to be solved. Because of this need, organizations began adopting a new platform approach that integrated security and networking. Benefits of this architecture include seamless management and the flexibility and power to deploy networking and security services how and where you choose. The platform also provides end-to-end control and secure Internet access, management of cloud applications, and protection for roaming users while reducing strain on resources and eliminating the need for hardware.

In this chapter, you learn how networking and security evolved from traditional wide area networks (WAN) to software-defined (SD)-WAN and from secure web gateway (SWG) appliances to

cloud-based SWGs or multifunction cloud-native secure service edge (SSE). There is also information about the combined concept of the secure access service edge (SASE).

Looking at Traditional WAN Technologies

Multiprotocol label switching (MPLS) played a pivotal role in shaping enterprise networking by offering reliable, high-performance connections, especially during the rise of centralized data centers. However, in today's hyperdistributed landscape — where applications, data, and users are spread across on-premises environments, multiple clouds, and remote locations — MPLS is showing its age. Its high costs, rigidity, and limited scalability make it ill suited for modern needs. With growing latency issues and a lack of agility, MPLS struggles to keep pace with dynamic workloads and cloud-first strategies. As connectivity and security demands surge across diverse locations and endpoints, organizations face significant challenges in maintaining seamless, secure access across the distributed environment.


TIP

Because of MPLS's shortcomings and the fact that circuits come with a higher cost than other transports, enterprises today need to evaluate where these more expensive circuits should be used. MPLS networks are typically provided by Internet service providers (ISPs) and other service providers — both the well-known telecoms and the not so well-known smaller companies. For many companies, lower cost Internet circuits will be sufficient for the majority of network traffic.

Many organizations inevitably install a secondary direct Internet access (DIA) link at their branch locations to offload some of this Internet traffic. Such a solution increases recurring costs and introduces still more complexity. Network traffic may not necessarily be routed across the best link at a given time, and bandwidth on one link or the other may be underutilized.

On the security side, Internet-bound traffic needs to be minimally secured by DNS-layer security or a firewall, but it may also require web-content filtering, data loss prevention, real-time malware detection, and other security services. The lack of visibility and a centralized policy enforcement point make it difficult, if not impossible, for security teams to ensure a secure and compliant operating environment (see Figure 2-1).

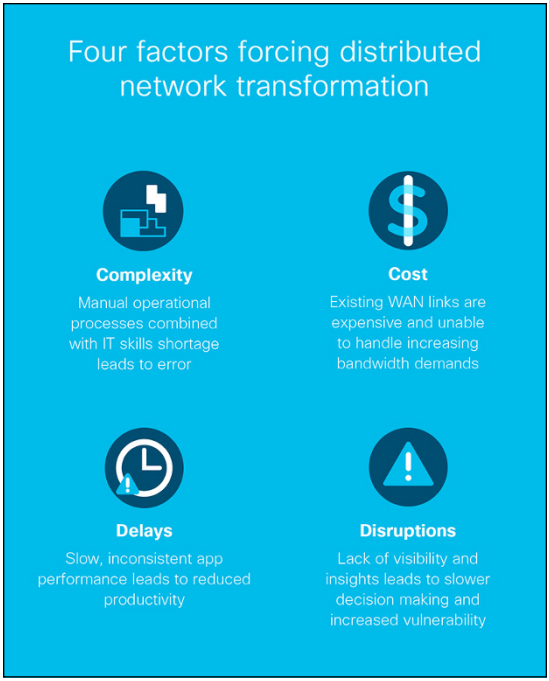


FIGURE 2-1: Challenges with current WAN architectures include complexity, cost, delays, and disruptions.

Exploring SD-WAN Solutions

SD-WAN emerged as a transformative solution to the limitations of traditional networking. Its cost-effective, agile, and cloud-friendly connectivity for distributed environments also positioned it as a foundational element of SASE. SD-WAN combines and optimizes WAN technologies such as MPLS and broadband Internet connections. This allows organizations to efficiently route network traffic to multiple remote branch locations while providing enhanced monitoring and management capabilities. SD-WAN monitors network traffic across all available links in real time and dynamically selects the best route for each data packet traversing the network. In recent years, SD-WAN has addressed the growing complexity at the edge of digital infrastructure with a unified, software-driven approach. It allows networking teams to manage and

automate the connectivity, configurations, and policies across all users, transports, devices, applications, clouds, and data centers in multiple locations from a centralized dashboard. In addition, it empowers networking and security teams with advanced intelligence and analytics that help resolve or prevent issues before they impact the user experience.


TIP

SD-WAN solutions are often praised for reducing costs and improving routing efficiency, but its true value extends far beyond that. Additional considerations and capabilities include:

- Routing traffic across different links based on destination and/or cost
- Improving security by integrating with advanced threat protection and zero-trust principles
- Connecting with ease to cloud providers like AWS, Azure, and Google Cloud
- Addressing the explosion of remote workers (the "branch of one") with flexible routing and traffic management options
- Meeting rapidly changing business needs with the capability to quickly build up and tear down branch locations
- Aggregating multiple links to provide greater total bandwidth
- Rerouting traffic across an alternate link when a link is congested, unstable, or down
- Prioritizing certain application traffic, such as voice and video, to ensure quality of service

CISCO SD-WAN EXAMPLE

Cisco SD-WAN empowers organizations to securely connect users, devices, and applications across any location, with a unified platform that delivers seamless multicloud access, robust zero-trust security, artificial intelligence (AI)-driven predictive operations, and comprehensive end-to-end visibility. Built on a SASE-Ready architecture, Cisco SD-WAN enables businesses to:

- Ensure zero-trust security with microsegmentation and distributed policy enforcement across users, devices, and apps.
- Seamlessly connect to multicloud environments with automated cloud onramps.
- Enhance agility and scalability with a cloud-managed, SASE-ready architecture that adapts to evolving business needs.
- Leverage AI-driven predictive operations and real-time visibility for proactive network management.

Tackling Internet Security Threats

The threat landscape is more complicated than ever, pushing organizations to tackle security threats beyond ransomware and phishing. Advancements in artificial intellingence (AI) and the mainstream availability of generative (Gen)AI apps are empowering malicious actors to deploy more sophisticated and targeted attacks. These include credential stuffing, supply chain attacks, AI-supported social engineering, and cryptojacking. Organizations struggle to respond because they're often slowed down by overly complex network and security stacks. This is especially the case when systems are operating separately without being designed for the scale of users and their devices, as well as Internet of things (IoT) devices connecting to the network, cloud applications, and data.

REMEMBER

Traditional security models, built for centralized data centers, can't keep up with the distributed landscape where users, devices, and data are spread among physical and cloud locations. SSE provides a consolidated set of cloud-delivered security services — including secure web gateway (SWG), cloud access security broker (CASB), and zero-trust network access (ZTNA) — to protect users against web-borne threats and data loss. By enforcing least privilege access and inspecting traffic inline, SSE ensures that users only access what they're authorized to, regardless of location or device. This approach not only strengthens security but also simplifies operations, reduces complexity, and supports seamless, secure access in a work-from-anywhere world.

SASE: Combining Network Connectivity with Cloud Security

According to Gartner, by 2027, 65 percent of new SD-WAN purchases will be part of a single-vendor SASE offering, up from just 20 percent in 2024. Convergence isn't a mere technical adjustment. It's a strategic imperative to combat threats, deliver consistent experiences, and meet operational goals — and a main driver of SASE adoption. The SASE concept extends the notion of multiple security capabilities, unified and delivered in the cloud, by adding SD-WAN capability. A SASE solution can secure users from any location or device as they access the Internet, software-as-a-service (SaaS) apps, and private apps, while delivering a secure SD-WAN fabric across disparate connections and simplified, centralized management (see Figure 2-2).

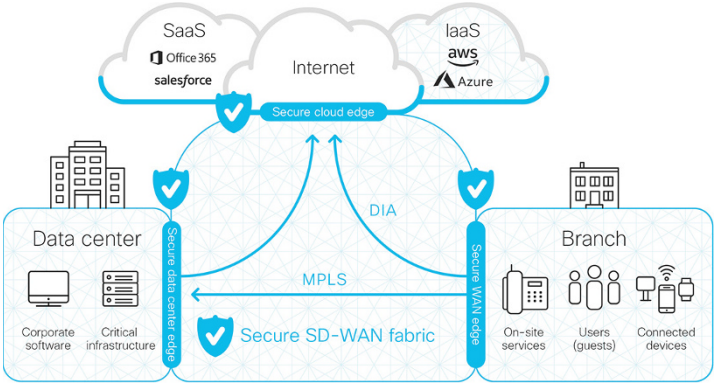


FIGURE 2-2: SD-WAN is a critical networking element in SASE solutions that can direct traffic for the protection of cloud, data center, and branch edge networks.

IN THIS CHAPTER

- Looking at secure connectivity challenges in the cloud era
- Recognizing key characteristics and benefits of SASE
- Getting started with SASE

Chapter 3
SASE: Combining Networking and Security Functionality

This chapter covers the challenges created in the new network architecture model, what functionality you need for secure connectivity, what issues you need to consider when deploying your solution, and how a secure access service edge (SASE) solution can help.

Recognizing Secure Connectivity Challenges

Network security is no longer confined to the data center — it's shifting to the cloud. As work moves outside the office and applications move to the cloud, the tried-and-true perimeter-based security model just can't keep up. To be successful, IT teams need to change their approach to controling and securing users, apps, devices, and data — anywhere and everywhere.

Today, the wide-scale use of cloud applications has become fundamental to business operations at all locations. Gartner predicted,

"Worldwide end-user spending on public cloud services to total $723.4 billion in 2025, up from $595.7 billion in 2024." The centralized security approach has become impractical because of the high cost of backhauling traffic and the resulting performance issues for branch locations.

To overcome these cost and performance issues, many organizations are adopting a more decentralized networking approach to optimize performance at remote locations. This enables a more efficient direct Internet access (DIA) path for these offices but also highlights a set of new security challenges, including:

- **Gaps in visibility and coverage:** Centralized security policies can't be effectively managed and enforced in a decentralized network. This is because most traffic from branch locations to the cloud and Internet doesn't cross a centralized policy enforcement point. This results in visibility and coverage gaps, which increase the risk of a successful breach or a compliance violation.
- **Volume and complexity of security tools:** Security teams already struggle to keep up with cybersecurity threats. Many of them have a large number of point solutions that are difficult to integrate and manage. These point products generate thousands of alerts, making it very difficult, if not impossible, for analysts to keep up. As a result, many alerts go untouched.
- **Limited budgets and security resources:** IT and security budgets are already constrained. Deploying multiple, costly point security solutions — such as firewalls, secure web gateways (SWGs), intrusion detection and prevention systems (IDS and IPS), and data loss prevention (DLP) — to multiple locations and remotely managing these solutions with limited security resources is both impractical and ineffective.

Key Characteristics and Benefits of SASE

The SASE concept consolidates numerous networking and security capabilities and functions — traditionally delivered in multiple, siloed point solutions — in a single, fully integrated cloud-native platform using a software-defined wide area network (SD-WAN) and cloud security (see Table 3-1).

TABLE 3-1 SASE Combines Core Capabilities Provided by SD-WAN and Cloud Security

SD-WAN	Cloud Security
Centralized management. A centralized, highly visual dashboard that facilitates device configuration, network management, monitoring, and automation. Includes zero-touch provisioning at the network edge.	Zero-trust network access (ZTNA). A security framework that mitigates unauthorized access, contains breaches, and reduces attackers' lateral movement across the network. ZTNA should be coupled with strong identity and access management to verify users' identity and establish device trust before granting access to authorized applications.
Cloud on-ramp automation. A simplified way for multicloud connectivity using an automated on-ramp to seamlessly connect to multiple public clouds of choice, like AWS, Azure, or Google Cloud, and cloud interconnect providers, like Equinix or Megaport.	**Secure web gateway (SWG).** A gateway that logs and inspects web traffic to provide full visibility, URL filtering, and application control and protection against malware.
Enhance user experience with application experience optimization. The ability to improve WAN performance through Application Quality of Experience, reducing latency and maximizing throughput. Features like TCP optimization, data redundancy eliminiation, and forward error correction ensure reliable application performance, boosting productivity, while minimizing costs and protecting critical business applications.	**Cloud-delivered firewall with intrusion prevention system (IPS).** Software-based, cloud-deployed services that help manage and inspect network traffic.
Flexible and scalable infrastructure. A wide range of physical and virtual platforms that deliver high availability and throughput, multigigabit port options, 5G cellular links, and powerful encryption capabilities. Optimizes WAN traffic by dynamically selecting the most efficient WAN links that meet the service-level requirements.	**Cloud access security broker (CASB).** Software that detects and reports on cloud applications in use across a network, exposing shadow IT and enabling risky software-as-a-servie (SaaS) apps and specific actions, such as posts and uploads, to be blocked.

(continued)

TABLE 3-1 *(continued)*

SD-WAN	Cloud Security
Artificial intelligence (AI) enhanced troubleshooting. Robust AI and machine learning (ML) for optimizing network performance, automating routine manual tasks, and accelerating troubleshooting. Provides intelligent alerting, self-healing, and predictive Internet rerouting capabilities.	**Data loss prevention (DLP).** Software that analyzes data inline or in cloud apps to provide visibility and control over sensitive data being pushed or pulled beyond the organization's network or cloud.
Integrated security. Comprehensive, integrated security with robust on-premises and cloud-delivered capabilities, ensures centralized policy management, distributed enforcement, and enhanced threat defense for branches, remote users, and cloud applications, all while fostering collaboration between NetOps and SecOps.	**Remote browser isolation (RBI).** Software that isolates web traffic from user devices to mitigate the risk of browser-delivered threats.
Identity-based policy management. Identity-based microsegmentation to enforce zero-trust policies based on user identity, device posture, and application context with unified policy for central control and distributed enforcement.	**DNS-layer security.** Software that acts as the first line of defense against threats on the Internet, blocking malicious DNS requests before a connection to an IP address is even established. Strong DNS security can greatly reduce the number of threats a security team has to triage on a daily basis.
End-to-end visibility and assurance. Have networking, security, and observability converged in one solution so you can see more and proactively solve more. Rapidly identify and resolve performance issues from the endpoint to the application, even across networks not under your direct control.	**Threat intelligence.** Threat researchers, engineers, and data scientists who use telemetry and sophisticated systems to create accurate, rapid, and actionable threat intelligence to identify emerging threats, discover new vulnerabilities, and interdict threats in the wild before they spread, with rule sets that support the tooling in your security stack.

Potential business benefits of the SASE concept include the following:

- Reduce cost and complexity
- Enable secure remote and mobile access to private and SaaS apps plus other Internet services

- Provide latency-optimized, policy-based routing
- Improve security with consistent policy
- Update threat protection and policies without hardware and software upgrades
- Restrict access based on user, device, and application identity
- Increase network and security staff effectiveness with centralized policy management
- Deliver a consistently seamless user experience anywhere

These benefits are critical for organizations that need to address the modern networking and security challenges of an increasingly cloud-first, distributed, mobile, and global workforce.

HOW ROSEN HOTELS & RESORTS IMPROVED PROTECTION BY CONSOLIDATING WITH CISCO

CASE STUDY

The IT team at Rosen Hotels & Resorts was using disparate tools and solutions to manage company network access. These tools left gaps that were vulnerable to attacks and exposed resources to unnecessary risks. The team faced major issues such as: lack of visibility into network traffic, inability to segment the network, limited integration, and no visibility into user behavior.

Rosen Hotels & Resorts was also growing quickly. Its IT team realized they needed centralized tools to adequately monitor network traffic, proactively defend against threats, and protect sensitive resources. They needed a partner to help them consolidate network and security. That partner is Cisco.

With Cisco's help, the IT team expanded protection across the network for users and their devices when logging in remotely. Cisco's solution blocked malicious websites and enabled users to safely access the Internet from anywhere — a major benefit.

(continued)

(continued)

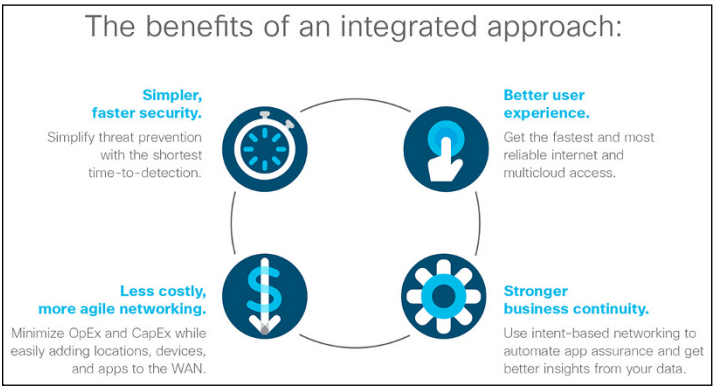
"Cisco offers a great solution for our company in protecting the end user," Manny Simancas, director of IT Infrastructure at Rosen Hotels & Resorts said.

With Cisco as its security partner, Rosen Hotels & Resorts has since experienced less network downtime, increased flexibility, and improved protection for its 25,000 users.

Simancas said, "Having a consistent partner in Cisco has provided visibility to the network and has reduced the amount of management that the team was spending trying to fix things that weren't working with third-party tools. It's a win-win."

Starting Your SASE Journey

SASE is a broad concept. To keep things simple, you should look for options that are flexible, allowing you to iteratively make changes at your pace and progress toward your organization's goals. That being said, two major SASE concepts are consolidation and simplification, so it makes sense to chart a course that includes both networking and security elements from a single vendor. There are many technical, cost, and end-user performance advantages to this type of combined approach (see Figure 3-1).



Source: Cisco

FIGURE 3-1: The benefits of an integrated networking and security approach.

With these combined benefits in mind, it makes sense to look at how to begin a holistic, phased SASE adoption plan.

To successfully adopt a SASE architecture, organizations must start with a clear roadmap that allows for incremental progress and measurable results. A practical first step is to explore the benefits of SD-WAN. The solution offers a more cost-effective, flexible, and efficient alternative to traditional networking by optimizing traffic routing and simplifying network management. Starting a trial deployment can demonstrate its impact on networking service costs, performance, and the overall workload on IT teams. As you evaluate SD-WAN, it's equally important to plan for how you'll secure the resulting traffic flows, particularly from a growing number of remote branches and roaming users.

As the network evolves, security must evolve with it. In tandem with SD-WAN, identify a vendor with a robust network technology portfolio that can support a broad range of network-as-a-service (NaaS) capabilities as your needs grow. Look for a cloud-native solution that can flexibly improve or even replace your current security stack capabilities. Search for a solution that can handle a broad set of security tasks and present data in a single console to help simplify deployment, investigations, and ongoing maintenance tasks.

WARNING

Ensure that solution providers can handle on-premises and cloud enforcement so that you don't have to struggle with the same problems of static, siloed security.

IN THIS CHAPTER

- Exploring key components in the security service edge
- Integrating networking in a SASE solution with SD-WAN

Chapter 4
Knowing What to Look for in a SASE Solution

This chapter explores the two sides of the secure access service edge (SASE) coin: the security service edge (SSE) and software-defined wide-area network (SD-WAN).

Security Service Edge

An SSE solution secures access to the web, cloud services, and private applications. Some key capabilities include access control, threat protection, data security, security monitoring, and acceptable-use control enforced by network-based and application programming interface (API) based integration. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

An SSE includes the following components:

- **Zero-trust network access (ZTNA):** The zero-trust security framework takes a "never trust, always verify, enforce least privilege" approach to security. ZTNA verifies user identities and establishes device trust before granting access to

authorized applications, which helps prevent unauthorized access, contain breaches, and limit an attacker's lateral movement on your network. ZTNA requires a strong, cloud-based, multifactor authentication (MFA) approach to security.

- **Secure web gateway (SWG):** A cloud-based web proxy or secure web gateway (SWG) provides security functions such as malware detection, file sandboxing and dynamic threat intelligence, Secure Sockets Layer (SSL) decryption, application and content filtering, and data loss prevention (DLP).
- **Cloud access security broker (CASB):** A CASB helps control and secure the use of cloud-based, software as-a-service (SaaS) applications, enabling organizations to enforce their security policies and compliance regulations. CASBs provide insight into cloud application use across cloud platforms and identify unsanctioned use within an organization. CASBs use auto-discovery to detect the cloud applications in use and identify high-risk applications and users, as well as other key risk factors. CASBs typically include DLP functionality and the capability to detect and provide alerts when abnormal user activity occurs, to help stop both internal and external threats.
- **Firewall-as-a-service (FWaaS):** FWaaS is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. This typically includes Layer 3 and Layer 4 (IP, port, and protocol) visibility and control, along with Layer 7 (application control) rules and IP anonymization.
- **Domain name system (DNS) layer security:** Domain name system (DNS) resolution is the first step when a user attempts to access a website or other service on the Internet. Thus, enforcing security at the DNS and Internet Protocol (IP) layers is the first line of defense against threats and is a great way to stop attacks before users connect to bad destinations. DNS layer security is often, but not always, referenced when analysts discuss an SSE solution. However, because it's a highly effective first layer of security, it's wise to consider it as part of your overall SASE solution.

TECHNICAL STUFF

DNS is the system that maps Internet hostnames to IP addresses. For example, when a user enters `www.cisco.com` in a web browser, DNS translates cisco.com to the IP address associated with that website (96.7.212.119).

REMEMBER

Cisco SASE is part of Cisco's Universal ZTNA which extends the benefits of a SASE solution for branch and remote access to an entire platform powered by tight integrations with Cisco ISE, Cisco Firewall Threat Defense, Cisco Identity Intelligence and Cisco Duo.

Software-Defined Wide Area Network

SD-WAN is an intelligent, software-defined approach to wide area networking that enables organizations to dynamically optimize application performance and security across diverse transport services, including MPLS, cellular (LTE/5G), and broadband. It leverages centralized policy management and real-time application awareness to intelligently steer traffic, ensuring optimal connectivity to on-premises, cloud, and software-as-a-service (SaaS) applications, while simplifying operations and enhancing security posture.

You can learn more about SD-WAN in Chapter 2.

IN THIS CHAPTER

- Extending SASE with Cisco Universal ZTNA
- Taking an incremental approach with Cisco SD-WAN and Cisco Secure Access
- Simplifying security with Cisco Security Cloud Control

Chapter 5
Exploring How Cisco Delivers SASE

Understanding that customers will be at different stages of their secure access service edge (SASE) journeys, Cisco provides a variety of options to ease the transition to modern application access. Cisco offers a unified SASE solution that combines high quality software-defined wide area network (SD-WAN) with its security service edge (SSE) solution — for flexible enforcement in highly distributed environments. This chapter discusses Cisco SASE solutions in detail.

Cisco Universal ZTNA

Cisco's Universal zero-trust network access (ZTNA) is a comprehensive solution that enables users and devices to securely connect to any application, anywhere — ensuring a consistent experience. It unifies identity-first, zero-trust access for modern and legacy apps, Internet of Things (IoT)/operation technology (OT) devices, and complex network environments, combining advanced performance, policy assurance, and end-to-end visibility to eliminate complexity and protect critical assets. Plus, it supports flexible enforcement, in the cloud or on-premises, so sensitive data is protected, and governance objectives met.

Cisco's approach helps teams modernize application access with integrated ZTNA and virtual private network (VPN)-as-a-service, extend identity context to include users and things, and build operational resilience through end-to-end digital experience monitoring and policy assurance.

Integrated Solution for Greater Customization Flexibility

For organizations that prefer taking an incremental approach to their SASE deployments, Cisco offers a complete ecosystem of modular networking and security solutions, as well as individual SASE components, providing maximum customization flexibility.

Cisco Secure Access: Multifunction, cloud-native SSE

Cisco Secure Access is a cloud-delivered security SSE solution, grounded in zero trust, that provides seamless, transparent, and secure access from anything to anywhere. By unifying multiple security functions into a single service, Secure Access helps businesses of all sizes embrace direct Internet access (DIA), secure access to applications, and extend protection to roaming users and branch offices.

REMEMBER

By integrating security functions together, and enabling interoperability with other products from Cisco and third-party vendors, Secure Access significantly reduces the time, cost, and resources required for deployment, configuration, integration, and management versus a stack of stand-alone security products.

Cisco Secure Access provides full SSE security functions managed from one cloud-based console with a unified policy model. Capabilities include (see Figure 5-1) the following:

- **Secure web gateway (SWG):** Cisco Secure Access includes a cloud-based proxy that logs and inspects web traffic for greater visibility, control, and protection. Features include:
  - Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations.
  - Scan downloaded files for malware and other threats.

- Sandboxing analyzes unknown files.
- File type blocking (for example, blocking downloads of .exe files).
- Full or selective TLS decryption to protect from hidden attacks and infections.
- Granular app controls to block specific user activities in select apps (for example, blocking file uploads to Dropbox, attachments to Gmail, posts/shares on Facebook).
- Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address.
- Multimode protection of Internet-based software-as-a-service (SaaS) apps with customizable controls and traffic path options.

» **Cloud access security broker (CASB) and data loss prevention (DLP):** Secure Access helps expose shadow IT and shadow artificial intelligence (AI) use by detecting and reporting on cloud applications in use across your environment. Insights help manage cloud adoption, reduce risk, and block the use of offensive or inappropriate cloud applications. Other highlights include:

- Detect, report on, and granularly control selected cloud apps in use, including generative AI (GenAI) chatbots. Manage cloud adoption and block offensive, nonproductive, risky, or inappropriate cloud apps to adhere to compliance needs and reduce threats.
- Discover, block, and revoke authorization of risky plug-ins and extensions from OAuth-based authorization to Microsoft 365 and Google tenants.
- Reports on vendor category, application name, and volume of activity for each discovered app.
- Tenant restrictions control the instance(s) of SaaS apps that groups/individuals can access.
- Discover, block or easily configure granular access and policy controls for usage of over 1200 generative artificial intelligence (GenAI) apps.
- Use AI to protect AI. For example, identify and mitigate leakage of sensitive financial, mergers and acquisition, and patent-application data.

- **DNS-layer security.** At the DNS layer, Cisco Secure Access blocks requests to malicious and unwanted destinations before a connection is even established — stopping threats over any port or protocol before they reach your network or endpoints. As a cloud-delivered service with over 50 global points of presence (PoPs), Cisco DNS-layer security offers the following features:
  - Accelerates network performance, because it is the only SSE in the industry featuring recursive DNS service.
  - Protects Internet access across all networked devices and office locations on the corporate network, with mobile device protection off the corporate network for roaming users, hybrid workers, and IoT.
  - Provides detailed reporting for DNS activity by type of security threat or web content.
  - Protects in real time against data exfiltration using AI- based mitigations against DNS tunneling.
  - Enables rapid rollout to thousands of locations and users for immediate protection. Initial configuration with network appliances takes just three clicks.
  - Provides visibility in reports and applied policies — down to the user level — by leveraging the Cisco Secure Client, Virtual Appliances, and third-party integrations.
- **Firewall-as-a-service (FWaaS):** With Cisco Secure Access's firewall, all activity is logged, and unwanted traffic is blocked using IP, port, and application rules via its Layer 3 and 4 protection plus Layer 7 application visibility and control. To forward traffic, you simply configure an IPsec tunnel from any network device. Management is handled through the Secure Access dashboard, and as new tunnels are created, security policies can automatically be applied for easy setup and consistent enforcement throughout your environment. Cisco Secure Access's cloud-delivered firewall provides:
  - Layer 3 and 4 access control rules for securing users/groups, networks or devices to access Internet, private networks and/or private apps.
  - Customizable IPS profiles with Snort 3.0 support. Enforce per rule IPS inspections on traffic patterns matched by a rule, for both Internet and private access.
  - Visibility and control over Layer 7 apps, application protocols, and ports/protocol, with a constantly growing base of apps identified.

- Decryption prior to inspections, for Internet or private access traffic.
- Bidirectional file inspection and file type controls for traffic between users and private apps.
- Scalable cloud compute resources eliminate appliance capacity concerns.

» **Interactive threat intelligence:** Cisco Talos, one of the world's largest commercial threat intelligence teams, continuously runs AI, statistical, and machine learning models against its massive database of threat data and analysis to provide insight into cyberthreats and improve incident response rates.

Investigate, available via API, leverages Talos data to help security teams programmatically access and analyze this threat intelligence to speed incident investigation and response. Investigate provides the following:

- Insight into the context around threats (domain and IP analysis, threat scores, domain categorizations, historical data).
- A map of attacker infrastructure by associating attacks with specific domains, IPs, ASNs, and malware.
- Predictions of where threat actors might stage future attacks.
- Custom queries and greater context for faster decision making and remediation.

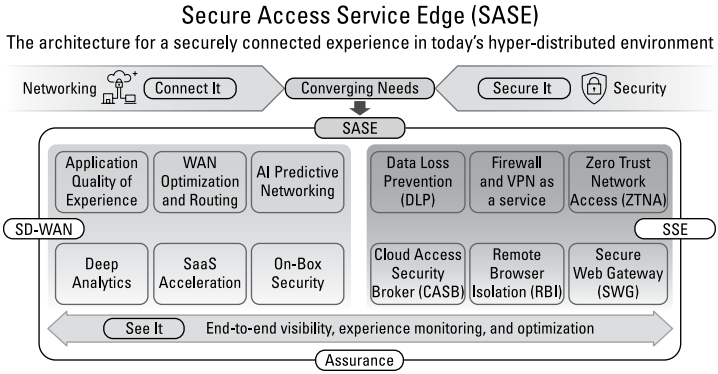


FIGURE 5-1: Cisco Secure Access delivers SASE security capabilities and more.

Cisco Secure Access and SD-WAN integration

Cisco provides extensive integration between Cisco Secure Access and Cisco SD-WAN (Viptela and Meraki), as well as third-party SD-WAN providers such as VMware VeloCloud, HPE (Aruba) Silver Peak, and Palo Alto Networks Prisma. For organizations that prefer the flexibility of their own customization of SASE (as opposed to using a singular, unified SASE solution), the Secure Access and SD-WAN integrations provide automation that enables security administrators to infuse effective cloud security simply and rapidly throughout the SD-WAN fabric to protect branch offices and roaming users.


TIP

The integration of Cisco SD-WAN with SSE offers a robust, secure, and efficient networking solution that addresses both connectivity and security challenges in today's increasingly digital and distributed business environments. Key benefits include:

- **Seamless connectivity and security:** Cisco SD-WAN provides efficient network connectivity, while SSE offers essential security services like secure web gateways and zero-trust access. Together, they ensure secure and efficient data transfer across the network.
- **Centralized management and zero trust:** With Cisco Security Cloud Control, centrally managed network and security policies simplify the enforcement of consistent security measures. Integration with zero-trust frameworks ensures trust verification for all access requests.
- **Optimized performance and scalability:** SD-WAN optimizes application performance by intelligently routing traffic, and SSE applies security without compromising speed. Combined, it is scalable and adapts to changes in network demand and security needs.
- **Enhanced visibility and analytics:** The integration provides comprehensive visibility into network performance and security events, enabling quick identification and response to issues, traffic optimization, and security compliance assurance.

Cisco SD-WAN: Flexible Cloud-Managed Networking

Cisco's approach to SASE leverages a cloud-scale SD-WAN architecture (see Figure 5-2) designed to meet the complex needs of modern WANs in three key areas:

- Advanced application optimization that delivers a predictable application experience as the business application strategy evolves
- Multilayered security that provides the flexibility to deploy the right security in the right place, either on-premises or cloud-delivered
- Simplicity at enterprise scale, which enables end-to-end policy from the user to the application over thousands of sites

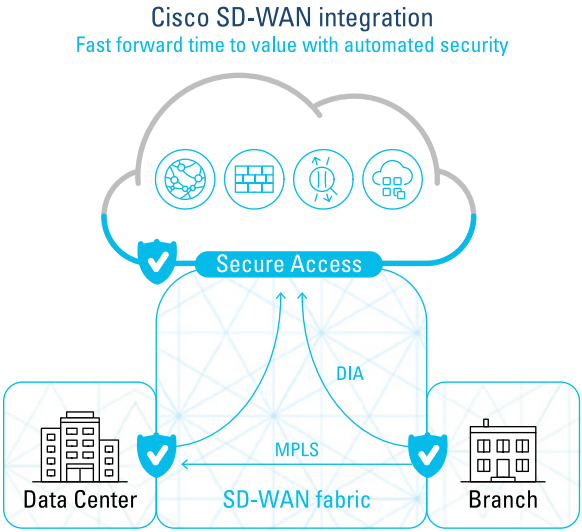


FIGURE 5-2: Cisco SD-WAN cloud-scale architecture.

Cisco Security Cloud Control

Cisco Security Cloud Control (SCC) is a cloud-native, AI-powered, centralized management solution for Cisco's security offerings, so teams can effectively manage their security posture across on-premises and cloud environments. It enhances visibility, scalability, and efficiency by unifying security functions and automating processes, such as device provisioning and policy updates. With centralized management of the Hybrid Mesh Firewall — a widely distributed security framework — it defends against advanced threats, safeguards applications, and enforces zero-trust segmentation across data centers, campuses, and IoT settings.

Security Cloud Control also supports Universal ZTNA, delivering consistent zero-trust enforcement across both cloud and on-premises infrastructures. By integrating networking and security, it streamlines operations for hybrid workforces and maintains consistent ZTNA policies tailored to each application. This comprehensive approach ensures cohesive security across diverse devices and solutions. Additionally, the Cisco AI Assistant simplifies rule management and helps reduce risk. Security Cloud Control establishes a dynamic, resilient defense system that evolves with your network, boosting both protection and operational performance.

DISCOVER YOUR ENTIRE IDENTITY POPULATION WITH CISCO IDENTITY INTELLIGENCE

Threat actors are successfully compromising some of the largest organizations in the world by targeting the blind trust between authentication and access solutions. Cisco's Identity Intelligence solves this weakness by bringing together identity, networking, and security to protect the complex identity stack.

Cisco Identity Intelligence runs on top of existing identity stores and provides unified visibility, as well as AI-driven analytics. You can

discover your whole identity population, clean up vulnerable accounts, eliminate unused and risky privileges, detect behavior anomalies, and block high-risk access attempts — without ripping out and replacing your current solutions.

By integrating with Cisco's broader security architecture, Identity Intelligence uses telemetry data from various sources such as endpoints, network infrastructure, and cloud environments. This allows organizations to create detailed identity profiles that include not just usernames, but also attributes like device types, locations, behaviors, and access patterns. By enriching security policies with this identity context, Cisco helps organizations enforce zero-trust principles — ensuring users only access what they need, when they need it, and from secure environments.

IN THIS CHAPTER

- Recognizing the changing nature of work and networking
- Dealing with cloud-delivered apps and services
- Addressing modern threats and attracting and retaining top security talent
- Getting started with SASE

Chapter 6
Ten Key Takeaways

Here are ten key takeaways about software-defined wide area networking (SD-WAN) and cloud security to keep in mind.

Support Return to Office and Roaming Users

The changing nature of work, marked by return to office mandates mixed with the continuation of hybrid work, is reshaping how organizations approach networking and security. As employees report on site, there is a greater emphasis on ensuring they not only have seamless access to resources from anywhere, but that their technology supports collaborative work. As a foundation to this, organizations rely on highly distributed and diverse applications that run over networks they don't manage — such as public Internet, cloud services, and home Wi-Fi.

Make DIA Work with SD-WAN

The majority of network traffic today occurs either within the data center itself (east-west traffic) or from an organization's various locations to the cloud via the Internet (north-south traffic). As a result, backhauling network traffic from remote or branch locations over multiprotocol label switching (MPLS) wide-area network (WAN) links, or roaming user traffic over virtual private network (VPN) connections, is no longer an efficient or viable option. To overcome these limitations, organizations are using direct Internet access (DIA) broadband links for their remote, branch, and roaming users, allowing faster, more direct access to software-as-a-service (SaaS) applications without the performance degradation and latency of traditional backhaul models. By layering in SD-WAN to secure and optimize DIA connections, organizations can dramatically improve application performance, reduce latency and bandwidth costs, and strengthen their overall security postures.

Be Careful with GenAI Apps

As generative artificial intelligence (GenAI) applications gain traction across industries, organizations must ensure users are engaging with these powerful tools safely and securely. With sensitive data increasingly flowing through GenAI-powered services, enforcing strong security and data protection measures is critical. One essential piece of the puzzle is flexible enforcement, also known as hybrid private access. This approach allows organizations to apply zero-trust principles locally — enabling branch users to access the Internet directly, rather than backhauling traffic to a central HQ for security enforcement. Not only does this improve performance and user experience, but it also supports compliance with data privacy mandates such as the General Data Protection Regulation (GDPR) by keeping data within appropriate geographic boundaries and applying policy controls closer to the user.

REMEMBER

When you're considering secure access service edge (SASE) solutions, it's important to evaluate not only solutions that are just delivered by the cloud, but also solutions that were "born" in the cloud (that is, cloud native).

See SD-WAN's Role in SASE

A SASE architecture can only be achieved through the combination of SD-WAN with cloud security. In other words, you can't have SASE without SD-WAN!

SD-WAN provides:

- Simplified multicloud connectivity using an automated on-ramp to seamlessly connect to multiple public clouds of choice.
- Improved WAN performance through Application Quality of Experience (AppQoE), reducing latency and maximizing throughput.
- Cross visibility among platforms to provide awareness into cloud security via the SD-WAN console and vice versa.
- Integrated security with robust on-premises and cloud-delivered capabilities, ensuring centralized policy management, distributed enforcement, and enhanced threat defense.
- Identity-based microsegmentation to enforce zero-trust policies based on user identity, device posture, and application context.

Understand That Network Architecture Faces New Demands

SD-WAN as a stand-alone networking solution is great for solving enterprise networking challenges, particularly in remote and branch locations. SD-WAN enables organizations to set up new sites quickly without having to wait weeks or months to provision new MPLS WAN links. Instead, a local Internet service provider (ISP) can provide a DIA link, often within just a couple of days.

But agility and simplicity introduce new challenges for enterprise security teams. In the rush to get connected, security may be an afterthought to the business. Once the Internet connection is live,

the business is ready to go — with or without security. And if the SD-WAN solution doesn't have built-in security capabilities, the security team may need to ship a separate firewall and/or other security appliances to the remote office. Plugging in one appliance is fine but two or three — well, that's just asking for too much!

Look for a Solution That Reduces Cost and Complexity

In the not-too-distant past, enterprise security teams routinely deployed best-of-breed point security solutions from different vendors to address single purpose needs — firewalls, secure web gateways (SWGs), intrusion detection and intrusion prevention systems (IDS and IPS), web content filtering, domain name system (DNS) security, data loss prevention (DLP), distributed denial-of-service (DDoS) prevention, and malware protection, to name just a few. These stand-alone products all have different operating systems and management consoles and typically provide only limited, if any, integration with other security products.

Unfortunately, in the pursuit of a "defense in depth" strategy, many organizations end up with "defense ad nauseam" as these various siloed security tools add complexity and often create performance issues in the network.


TIP

Avoid patchwork at all costs. A true SASE solution integrates networking (SD-WAN) and cloud security capabilities. Simply looking to add multiple best-of-breed point products that make up a SASE architecture may lead to more complexity than your original architecture.

Don't Compromise on Network Performance

A key consideration for organizations implementing a SASE architecture is addressing the requirement for a better user and application experience. SD-WAN, a core component of this

architecture, enables the quality of experience by intelligent network selection. Ultimately, the user experience is what drives successful adoption of digital transformation initiatives in an organization. Poor network performance guarantees a poor user experience and drives frustrated employees to turn to potentially risky shadow IT apps and solutions. In the event of a performance breakdown, organizations need edge-to-app visibility — especially over networks they don't manage to quickly uncover the root cause of access issues.

SD-WAN enhances the quality of the application and user experience by enabling traffic steering and dynamic failover, resulting in greater enterprise productivity and agility within a SASE architecture.

In the hybrid workforce world, a key focus for many enterprises is application performance because it drives employee and ecosystem productivity, as well as customer satisfaction. With the increase in cloud adoption, the first thing users want is easy and reliable access to their SaaS cloud business applications — which is all about using the most optimized path to those applications. This is where SD-WAN plays a big role. Although security inspection is important, before you even send the traffic out, you need to make sure that users utilize a thin or lightweight edge SD-WAN appliance to identify their application, prioritize that application, and then steer the traffic to the most optimized path.


TIP

Ensure that your network and security platform can deliver the performance (and security) your users require to stay productive — whether they're in the headquarters location, a remote or branch office, or roaming on a mobile device.

Also, consider choosing a solution that allows you to see how a policy change will affect the organization before enabling the change. That way, organizations can avoid downtime risks.

Always Keep Security Top-of-Mind

Cyberthreats are becoming more advanced and attackers are employing new techniques to exploit vulnerabilities and breach targeted networks. Phishing emails that were once easily

identifiable by their spelling and grammatical errors have become much more difficult to spot. Ransomware has become far more prevalent as well, with ransomware-as-a-service (RaaS) making it easy for practically anyone to launch an attack. And these are among some of the less sophisticated threats today. Organized crime and nation-states launch far more advanced attacks using vast resources — and their attacks can take years to detect and eradicate.


TIP

In a SASE architecture, the SD-WAN collects and transports vital telemetry (such as data about user, device, application, cloud, security, and so on) to apply and enforce cohesive, real-time, intelligent networking and security policies across all domains.

Make Life Easier for Your Operations Team

The worldwide shortage of qualified security professionals is a trend that will continue for the foreseeable future. The good news for security professionals is that there will be well-paying security jobs for years to come. The bad news is that the already difficult job of securing an enterprise network is only getting harder as threats are getting more advanced, and the proliferation of siloed security tools requires specialized knowledge and experience that must constantly be updated and refreshed.

Attract and retain top talent by implementing innovative networking and security solutions that integrate functionality in a single, cloud-delivered platform and make life easier for your entire operations team.

Start Every Journey with a Single Step

With Cisco Secure Access, you can start small with DNS-layer security and build up with additional capabilities from there as your organization is ready.

A fully integrated SD-WAN and cloud-native security solution can help organizations address the networking and security challenges of the cloud and mobile computing era. Secure access service edge (SASE) provides advanced networking and security functionality in a single pane of glass, enabling enterprise networking and security teams to confidently build out their networks with the agility that modern businesses require.


TIP

Learn more about Cisco's approach to SASE at `https://www.cisco.com/site/us/en/solutions/secure-access-service-edge-sase/index.html`.

Market-leading SD-WAN meets identity-first SSE. That's Cisco SASE. Networking and security together.

Your users are everywhere. Your applications are everywhere. But how do you deliver connectivity everywhere—securely?

It just got easier. Cisco SASE brings networking and security together on one platform, so that now, you can deliver every kind of access—for all your workers, all your apps, across all kinds of networks—seamlessly and securely.

Ready to jump start your journey to SASE?

Get hands-on access to our technologies in our Zero Trust workshops. Register today.

Discover simplified networking and security

Secure access service edge (SASE) is a framework for integrating networking and security to meet the demands of modern, distributed organizations. By combining capabilities such as software-defined wide-area networking (SD-WAN), secure web gateways (SWG), cloud access security brokers (CASB), zero trust network access (ZTNA), and firewall-as-a-service (FWaaS), SASE delivers seamless, secure connectivity for users, devices, and applications — anywhere they are. This transformative approach reduces complexity, enhances scalability, and provides consistent security for organizations of all sizes.

Inside...

- Simplify network and security management
- Enable secure remote access
- Leverage SD-WAN capabilities
- Optimize network performance
- Protect all users and devices
- Implement zero trust network access
- Gain end-to-end visibility and protection

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

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

ISBN: 978-1-394-36668-2
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.