Brought to you by:

FORTINET

AI & SASE

for dummies®

A Wiley Brand



Discover how AI is transforming SASE

Secure the use of AI across your organization

Put AI to work for better security

Fortinet Special Edition

Steve Kaelble

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 our customers 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. Collaboration with esteemed organizations from both the public and private sectors, including Computer Emergency Response Teams ("CERTS"), government entities, and academia, is a fundamental aspect of Fortinet's commitment to enhance cyber resilience globally. 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.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



AI & SASE

Fortinet Special Edition

by Steve Kaelble

for dummies®
A Wiley Brand

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

AI & SASE For Dummies®, Fortinet Special Edition

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

Copyright © 2026 by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Fortinet is a registered trademark of Fortinet, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

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

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.dummies.com/custom-solutions. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-46603-0 (pbk); ISBN 978-1-394-46604-7 (ebk); ISBN 978-1-394-46605-4 (ebk)

Publisher's Acknowledgments

Project Editor: Jennifer Bingham
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Cynthia Tweed
Content Refinement Specialist: Athiyappan Lalith Kumar
Special Help: Nicole DiDio, Alexandra Mehat, Rami Rammaha, Ramnath Shenai

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

You don't need a book to tell you that artificial intelligence (AI) is revolutionizing the world around you. You can feel the impact in aspects of your personal life as well as at the workplace, where AI capabilities are finding their way into almost everything.

AI is adding to an information technology (IT) environment that was already getting incredibly complex — and beyond being a hassle, complexity is increasingly a risk. Unified secure access service edge (SASE) is an intriguing antidote to some of the complexity of IT architecture. It brings networking and security, which have historically been two separate worlds, into a unified, intelligent, cloud-delivered platform.

Specifically, SASE unites software-defined wide area network (SD-WAN) technology for connectivity with security service edge (SSE) for cloud-delivered security. It's not just stitched together but unified to ensure that connectivity, security policies, and user experiences are consistent everywhere, regardless of the specifics of the users, the apps, or the data.

About the Book

This book, created by experts in the world of networking and security, explores how AI is transforming the landscape and why unified SASE is ideal for an increasingly AI-driven operation. It spells out the fundamentals of SASE and all of the helpful components that align effectively. It discusses the challenges of securing AI in your operations, the dangers posed by malicious actors who also are very keen on the benefits of AI, and the promises of using AI to help secure your environment and thwart the bad guys.

Read on to learn why it's important to zero in on the user's digital experience and productivity, not just the in-the-weeds details of how IT is functioning. The book outlines the building blocks of an intelligent unified SASE architecture. And it sums up the smartest ways to bring an AI-ready unified SASE implementation to life in your organization.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Foolish Assumptions

In writing this book, a few assumptions were made about you, the reader:

- You may be a chief information officer, a chief information security officer, or anyone who works in those areas.
- You can see that AI is changing how your enterprise connects, secures its IT, and operates successfully.
- You want to learn more about how unified SASE can help manage this transformation safely and efficiently.

Icons Used in This Book

In the margins of the book, you see some artsy icons. Their purpose in life is to provide direction.



REMEMBER

This icon spotlights a key point that you won't want to miss, even if you're in a hurry.



TIP

You picked up the book for helpful hints, and this icon points out some actionable advice.



WARNING

The world of IT is filled with dangers and roadblocks, and this icon highlights a pertinent caveat.



CASE STUDY

Details about how you can use AI and unified SASE.

Beyond the Book

You have about 48 pages of insights ahead of you, but this isn't by any means all you need to know about AI, networking and security, and unified SASE. Check `Fortinet.com` for more information about solutions to your network security concerns, your generative AI security needs, and your journey toward implementing unified SASE.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Speeding up transformation with AI
- Understanding unified SASE
- Seeing how AI is helping attackers
- Employing AI for a stronger defense

Chapter 1
Reshaping Security and Networking with AI

Artificial intelligence (AI) is reshaping the enterprise information technology (IT) environment like almost nothing else in history. It's accelerating transformation while greatly changing how traffic flows, what identities are in play, what the infrastructure looks like — and how malicious actors operate.

This chapter explores how the traditional separation of networking and security is no longer practical, how unified secure access service edge (SASE) fits into the picture, how AI is boosting the acumen of attackers, and how it can help you build a stronger defense.

Transforming at the Speed of AI

It was certainly a game-changer back when organizations began to really embrace cloud computing. The shifts felt seismic at the time, and it was clear that the cloud was more than just a technology trend or minor fad.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

AI is here to tell you, "You ain't seen nothing yet." It's one of the most momentous shifts since those early days of cloud, and truth be told, AI is changing enterprise information technology far faster than the cloud ever did.

Cloud computing meant a new place for applications to run, but AI is revolutionizing the way applications behave. Infrastructure evolved into distributed networks when the cloud started catching on, but AI has brought to the forefront the idea of autonomous software that generates content and makes decisions and interacts with systems and moves data. While the cloud expanded enterprise networks, AI is bringing fundamental change to what moves across those networks.

In other words, AI brings a whole new operating model to the forefront, not just another workload to protect. The opportunities to innovate seem nearly endless and the productivity promises are enticing. But AI also brings in new security risks, new networking demands, and new operational challenges — what AI wants and needs is beyond what traditional architectures were designed to accommodate.



REMEMBER

And AI is making those demands seemingly overnight, far faster than the technology transformations of yesteryear. In the old days, you had time to catch your breath as mainframes evolved into client-server computing, and as that model evolved into virtualization, then led its way to the cloud. Every step along that evolution changed the enterprise infrastructure, a little bit at a time, but AI is impacting everything pretty much everywhere at the same time.

It's changing how employees work, how applications are designed, how data moves around. It's changing the ways that identities are used, the ways IT operates, and unfortunately, the ways that cybercriminals attack.

Rather than waiting around for users to trigger each step in a process, AI systems are out making things happen, based on a user request. Ask an AI assistant to tackle a task, and there may be a bunch of backend operations that involve software-as-a-service (SaaS) applications, vector databases, internal knowledge bases, cloud storage, and external models.

The result is a continuous stream of application programming interface (API) calls and database queries and cloud requests,

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

generated by large language models (LLMs), autonomous agents, retrieval systems, and orchestration platforms. That means a network that's a whole lot busier, and not entirely predictable.

It's not just more traffic, but wholly different kinds of traffic. The old assumptions guiding network architecture are out the window, as enterprises find themselves responsible for securing interactions among people, devices, apps, APIs, AI models, and agents — all connecting across multiple clouds and tapping into sensitive data.


TIP

To stay secure in this brave new world, organizations must have visibility into exactly which AI services employees are using, what data is involved, which AI agents are in the mix and what resources they are accessing, whether sensitive information is being directed outside of approved environments, and whether AI-generated actions are happening in full alignment with the organization's policies.

Seeing How Unified SASE Fits In

Networking and security have had their own separate histories and evolutionary stages. Networking teams have been given the task of moving traffic efficiently, while security teams have been all about inspecting the traffic and keeping it safe.

They may have arrived from different perspectives, but their work has become increasingly intertwined as users and apps and data and workloads are moving among clouds, from one remote location to another, among branch offices, and along edge environments. AI turbocharges this convergence.

That's because AI is born to be speedy and efficient. An AI assistant requires secure, fast, and policy-driven access to information wherever it might live, whether that's in a data center, a SaaS application, in a cloud environment, or countless places.

Making that happen requires networking and security to operate hand-in-hand. That happens to be a key promise of unified SASE.


REMEMBER

Note that first word, unified. Unified SASE represents the convergence of networking and security into a single, intelligent, cloud-delivered platform. It's no longer sufficient to stitch together separate networking products and security point solutions. Unified

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

SASE integrates these functions so that connectivity, security policies, and user experiences can remain consistent wherever the users, apps, or data might be.

This idea already was becoming critical as workforces became more hybrid and distributed, as multicloud environments became the norm, as SaaS applications and edge computing usage grew. AI-powered services and autonomous agents just make it all the more important to link networking and security.

Unified SASE gets rid of the complexity that comes from disconnected security products. Traditional environments have often needed separate consoles, multiple policies, and manual coordination. That kind of inefficiency just doesn't cut it as AI speeds up the action and expands the interactions among users, identities, applications, APIs, and machines.

Unified SASE can deliver intelligent policy enforcement close to the users and the applications. It brings the relief of simplicity, along with centralized visibility and control.

Defending Against AI-Powered Threats

John Adams, an American Founding Father and the second U.S. president, famously observed that "Every problem is an opportunity in disguise." Albert Einstein made a similar observation. And Winston Churchill called out as pessimists those who see things the other way around and think of opportunities as being problematic.

Not to be pessimistic in the Churchillian sense, but the fact is, the opportunity of AI does bring with it some problems and challenges. Your employees use AI to accelerate productivity, and your cybersecurity teams are greatly aided by AI-enabled monitoring, investigations, and responses. That said, cybercriminals are increasingly adept at using AI to do their dirty work much faster and on a much larger scale.



WARNING

Attackers are turning to AI to discover vulnerabilities, amplify their reconnaissance, automate their social engineering, write especially persuasive phishing messages, create malware that's more effective and evasive, and plan polymorphic attacks that confound defenses by continually adapting their behavior. Just

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

like the good guys, the bad guys are using AI to smash through technical barriers.

All the while, AI capabilities have organizations introducing shiny and tempting new assets that are in need of protecting. Securing users and applications isn't enough, given this bigger attack surface. Security teams now must watch over the technology of AI and the tools that it taps into, such as:

- LLMs
- Generative AI applications
- AI assistants and agents
- AI infrastructure
- APIs
- Training and inference environments
- Corporate data accessible by AI
- Sensitive prompts

Consider an autonomous AI agent that has been designed to access customer relationship management systems, financial databases, human resources platforms, SaaS applications, and cloud platforms. If that agent is compromised, it could violate governance policies, expose sensitive information, and take other dangerous actions.

More problems arise from employee use of unauthorized or shadow AI tools. They could have the most innocent intentions but end up uploading confidential info into public AI models, or they might let personal AI assistants access business applications and information.



TIP

Visibility is the first step in addressing these dangers. You need to know what AI apps are being used, what data is flowing into those tools, and how such actions square with security policies.

You also need visibility into the agents themselves, because they're able to independently call APIs, chain together workflows, and tap into sensitive information. It's vital to know which agents are active and what identities they use. You need to know the resources they can access and what rules apply to those resources. And you need to be able to spot abnormal behavior and then figure out if it indicates a malfunction or a compromise.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

As you do with human users, you must apply zero-trust principles across all identities, applications, APIs, networks, and data. You must secure your AI activities and protect against malicious AI activities. What's a great tool for doing that? AI.

Using AI to Simplify and Automate Operations

Back to paraphrasing and updating John Adams and Einstein, if AI is increasingly a problem, it's also offering a solution. It's one of the most effective tools ever imagined for addressing security challenges.

Think of the telemetry across the modern IT environment — logs and alerts from all the networks, endpoints, cloud workloads, SaaS applications, security platforms, identity tools, APIs, and other elements. There's no way human analysts can keep up with all of that effectively, but AI is fantastic at diving into big datasets to spot meaningful patterns.

AI-driven analytics can boil down thousands of isolated alerts and correlate activity across many security domains. As AI silences duplicate alerts, it sees potential attack paths and prioritizes potential problems. Alert fatigue gets a rest.


TIP

When it spots issues, AI can recommend responses and even launch autonomous remediation when appropriate. It can isolate endpoints that are compromised and block malicious traffic. It can enrich threat intelligence and hunt down attack origins. It ups the response speed by trimming manual actions.

At the same time, AI can watch over network and application performance, notice congestion and configuration issues, and identify connectivity problems. This is known as *digital experience monitoring*, and it helps IT move from reactive fixes to proactive optimization.

When your IT professionals have the bandwidth to think proactively and strategically, they can really have a positive impact on operational efficiency. AI can automate repetitive tasks, basic investigations, recommendations, and remediations. Human expertise can then be applied to higher-value business problems.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Exploring unified SASE
- Unifying the platform
- Defining the components of unified SASE
- Seeing why it's a great idea
- Making the work simpler

Chapter 2
Understanding Unified SASE Fundamentals

Unified secure access service edge (SASE) is a key part of addressing the networking and security challenges posed by artificial intelligence (AI) and other complexities of today and tomorrow. This chapter digs further into how it addresses those issues. You learn how unified SASE differs from traditional SASE, how the integrated platform comes together and what it includes, and why it is so effective at simplifying operations, policy enforcement, and visibility.

Seeing How Unified SASE Is Different

Once upon a time, there was SASE. That story goes back, well, a little over half a decade, when the term was first coined to describe a solution to an emerging concern about how enterprise information technology (IT) environments were evolving.

As workers and their activities moved more toward decentralized models and into the cloud, enterprises needed to find a better way to route traffic. In the mid-2010s, a promising answer seemed to be software-defined wide area networks (SD-WAN), which

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

allowed for more efficient traffic management using software and the cloud. It's a great concept, but what SD-WAN didn't bring were the advanced levels of security needed for that kind of an environment.

The light-bulb idea was to merge SD-WAN networking with security, turning it into a single cloud service. That idea got its name in 2019: SASE, pronounced "sassy" for short.

Still, not everyone at the time needed the networking part of that deal, so within a couple of years another term emerged to describe just the security tools. That would be security service edge (SSE), and it was hailed as a healthy step forward from the days of hardware-heavy network defenses.

To make this short story even shorter, SASE pretty quickly became a defining concept in modern enterprise security. But of course, IT stories tend to keep evolving before the ink is dry (to dig up an especially analog metaphor, just for the sake of nostalgia).



WARNING

Traditional SASE offerings have in some cases been created by hooking together separate networking and security technologies. To the accounts payable department, that may make them seem like a single subscription, but under the hood they're still separate products, each with its own management console and operating system, running separate policy engines and tapping separate data stores.

Unified SASE isn't just a collection of services stitched together after deployment (for more on what unified means in this context, see Chapter 1). It's not a collection of point products conveniently served as a package deal. It's a consolidated, cloud-delivered platform, marked by networking and security services that are built on a common architecture.

The next section gets into more specifics about what unified SASE includes. The point to understand is that this is an architectural model, not a product or a conveniently packaged group of products. It's a response to the differing ways that various SASE products were created.

Some providers of nonunified SASE got there by assembling existing components they had built or acquired. Some integrated different product lines. But without being born on a common architecture, these creations often have still felt like a group of

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

disparate tools, with separate management consoles, distinct policy engines and operating systems, telemetry and reporting that are disconnected, and configuration work that might have to be duplicated.



REMEMBER

Unified SASE has a shared platform that includes common management, policy enforcement, and telemetry. Take a simple situation, such as a user device connecting to a cloud platform, and imagine what that means. There's no need for the unified SASE to check multiple products, because it can on its own evaluate identity, device posture, application, conditions of the network, sensitivity of the data, current threat intelligence, and the organization's access policies.

Decisions can thus be made more quickly, more simply, and more accurately. And looking ahead, adopting future capabilities, such as whatever magical thing AI will bring next, can happen far more efficiently and effectively.

Creating a Single Platform

To be a bit more specific about what unified SASE really unifies, consider it as a marriage between two major families of technology into a single cloud-based platform:

- SD-WAN for connectivity
- SSE for cloud-delivered security

The following sections take a deeper dive into these two families of origin.

Evolving into SD-WAN

As described in the brief history lesson above, SD-WAN was a dramatic evolution in the field of enterprise networking. Before the cloud emerged, applications largely lived inside corporate data centers, sharing a home with the data they crunched, and serving the needs of employees who generally went to work in some corporate facility.

Today, applications and their data could live any number of places outside the corporate data center, if there still even is one. Amazon

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Web Services, Google Cloud Platform, Microsoft Azure, to name a few of the possibilities. Countless software-as-a-service (SaaS) applications handle the action from all kinds of places.

The users, meanwhile, are all over the place, too. They already had ventured into branch offices and customer sites and hotels and airports. Some spent at least a bit of time in home offices (and when the COVID pandemic hit, an increasing number of them went remote and never came back).

Traditional wide-area network architectures weren't built for this kind of complexity and far-reaching distribution. Traffic that had to run through a centralized data center before reaching cloud applications suffered from latency that was annoying or worse.


REMEMBER

SD-WAN, on the other hand, ditches the fixed network paths and instead evaluates all of the available connections, picking the best path based on specific application needs and network conditions. It employs intelligent application steering, dynamic routing, and automated failover.

It knows that all traffic isn't equal. Different uses have different technical requirements. Business-critical traffic needs to be prioritized ahead of other traffic. Applications perform better, and users are happier.

Setting up SSE

It goes pretty much without saying that every connection needs protection. That was a whole lot easier to achieve back in the days when all of the goodies lived inside the castle walls of the data center, and security was centralized.


REMEMBER

Because the action today happens outside the castle, SSE delivers cloud-based security services closer to users, rather than forcing all the traffic back through centralized security appliances. With SSE, there's no longer a need for multiple hardware devices. Instead, there are cloud-delivered services that are outlined on the next page or two, and security policies can follow users wherever they are working.

Seeing why the integration matters

Both SD-WAN and SSE have vital functions to deliver and problems to solve. Your technology simply works a whole lot more

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

effectively when they're on the same page, aligned within the same architecture in the cloud.

Working hand-in-hand, SD-WAN and SSE can allow networking decisions that immediately incorporate vital security context. Security decisions can likewise take network conditions and other details into account.



REMEMBER

In a unified approach, such essential things as identity information, application awareness, and threat intelligence are available across the platform, rather than being stuck in a home base somewhere. And there is no competition as to whether networking or security is in control, because they're both working collaboratively.

Describing Key Components of Unified SASE

This section dives into some of the key capabilities and components of unified SASE. The concepts bring into one happy household an alphabet soup of security and networking capabilities:

- **Zero-trust network access (ZTNA):** Zero trust is a critical concept that needs to be applied universally and continuously. With ZTNA, users don't necessarily get broad network access after authentication; it only grants access to specific, authorized applications. Sessions are continuously verified, with the system watching over user identity, device health, and policy compliance.
- **Secure web gateway (SWG):** This capability keeps users safe as they browse the web. It filters out malicious websites, stops dangerous downloads, checks encrypted traffic, and makes sure acceptable-use policies are followed.
- **Cloud access security broker (CASB):** Typical organizations these days may rely on hundreds of SaaS applications, and CASB provides visibility into those services. It applies security policies, watches for shadow IT, and tries to eliminate risky application usage.
- **SaaS security posture management (SSPM):** Securing users is one thing, but not all organizations keep close

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

enough tabs on SaaS configuration. It's too easy to be exposed by misconfiguration of various cloud services, so SSPM evaluates configurations continuously. It looks for risky settings and makes remediation recommendations.

- **Digital experience monitoring (DEM):** Just because your environment is secure, it doesn't mean it is operating at tip-top efficiency. DEM follows how users are actually experiencing their work and their applications, checking out endpoints and networks and cloud services and app performance.
- **Firewall-as-a-service (FWaaS):** A firewall used to be tied to a physical appliance, but today's cloud-delivered firewalls can keep an eye on traffic no matter where the user is. This component provides such capabilities as intrusion prevention, application control, Secure Sockets Layer inspection, threat detection, and network segmentation.
- **GenAI security:** Bringing generative AI into the picture adds a whole raft of new security requirements. Unified SASE must be able to identify AI applications, monitor their usage, enforce applicable policies, and be sure sensitive information doesn't end up where it's not supposed to be.
- **Data loss prevention (DLP):** DLP keeps a close watch on sensitive information and ensures that there aren't unauthorized disclosures through web traffic, cloud applications, AI interactions, or endpoints.

Recognizing the Benefits



WARNING

To see why unified SASE is a beneficial approach, this section starts by exploring what life is like with a more disparate solution. Though SASE was definitely an upgrade in theory, a system that doesn't fully unify networking and security means security administrators may still feel like they're dealing with multiple separate products. They might be juggling:

- Several separate management consoles
- Different policy engines for each component
- Multiple operating systems
- Multiple telemetry sources
- Reports that are inconsistent

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Configurations that have to be done separately in different places

Add another product and you get another dashboard. That also means more logs to monitor, policies that need to be re-created, identity information that might not exist from one area to the next. A network event might require manually correlating logs from several products in order to grasp what happened. That's a lot of dashboards, a lot of duplicated work, and a lot of overhead to support.

Now imagine a unified approach. Having all of the capabilities listed in the last section is fantastic, but one of the biggest benefits of unified SASE is the way all of those capabilities work together.



REMEMBER

Expect your unified architecture to have just one operating system and a single management platform. You'll deal with one data model, a single telemetry repository, and just one unified policy framework.

All of those powerful components, with all of their capabilities and distinctions and acronyms, no longer require separate administration. You enjoy centralized policy creation, with no need to tailor policies to specific components and figure out how well they play together. There's shared threat intelligence and consistent enforcement across all of your many cloud environments, remote users, locations and branches, and endpoints.

Investigations get much simpler and more powerful when you have shared telemetry. No more need to piece together logs from multiple products. Analysts are, instead, able to see events in context. Troubleshooting is far more efficient and speedy.

AI takes these advantages and runs with them even further. AI's great at absorbing contextual information, and with a unified platform, that means richer data for analytics, automated monitoring and remediation, and intelligent decision-making.

Simplifying Your World

Complexity is far more than just an annoyance or an inconvenience. In the world of cybersecurity, complexity has become one of the biggest risks.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



WARNING

The desire or need to add more security point products is ongoing. But every time a product is added, it brings another console and administrator, another policy language, and another software update with the risk of another misconfiguration.

Unified SASE reduces the burden because it brings with it a single operational framework when it comes to connectivity, access control, web security, cloud security, data protection, monitoring, and increasingly AI-assisted operations. That's a relief and a convenience, but the increased simplicity is also an antidote to the risks of complexity.

Protection is consistent regardless of where users connect, thanks to unified policy enforcement. Threat detection is upgraded, thanks to shared intelligence. Compliance reporting is less of a headache because centralized visibility brings simplicity.

Integrated automation, meanwhile, puts a dent in repetitive administrative work. Add in AI-driven analytics and you're better able to see and identify issues before they turn into outages or security incidents.

Unified SASE is also a bridge to whatever the future might bring, both in terms of threats and security improvements. One thing you can bet on is an ever-increasing adoption of AI and autonomous agents, along with edge computing and cloud-native applications. Don't expect hybrid work to go away, either.



TIP

Disconnected products make that future murkier, because the complexity will only grow. Unified SASE, on the other hand, is better able to evolve as the business and the landscape evolve — without the need to add another tool or management console.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Making AI and its traffic more secure
- Inviting nonhumans to the network
- Addressing threats powered by AI
- Automating the work of SASE
- Foiling the top security issues

Chapter 3
Securing AI and Using AI for Security

What are the odds that your enterprise generative artificial intelligence (GenAI) applications will experience multiple security incidents? Pretty high, according to experts — like one chance in four over the next few years. With those odds, betting on traditional networking and security is a gamble.

This chapter explores how unified secure access service edge (SASE) is a much safer bet for securing your business against AI. It explores the proliferation of nonhuman users, describes how malicious actors are getting good at AI, looks at how AI is upping the SASE game, and discusses how SASE derails security threats.

Securing GenAI Applications and AI Traffic

AI is transforming enterprise technology more rapidly and profoundly than just about any innovation ever has. To imagine anything quite this earth-shattering, you'd have to go back to the

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

days when personal computers started taking over for mainframe terminals, or when the internet made it possible to work from a coffeeshop.

History books or studies of biological or geological or cultural evolution often classify monumental change into distinct eras. You can do that with descriptions of AI in the enterprise, too, but the big eras of AI seem to pass with the blink of an eye:

- **The chat era:** It was late 2022 when employees started plugging questions into ChatGPT, then some competitors.
- **The copilot era:** Pretty soon AI was embedded into productivity applications, so employees didn't necessarily need to chat with a GenAI chatbot. Organizations started dabbling more in their own large language models (LLMs), too. You could peg this era's start date as 2023.
- **The agentic era:** Here's where it became increasingly common for AI to do things on its own, taking actions rather than just responding to queries. Start the clock on this era around 2025.



REMEMBER

That's three significant eras in three or four years. Though AI has been around for some time in earlier incarnations, in the short few years since the dawn of public use of ChatGPT, organizations have now moved from careful experimentation to embedding AI into all kinds of everyday operations.

There are employees tapping into AI to draft reports, build marketing campaigns, summarize meetings, interact with customers, "vibe coding" applications, and many other things. With a pretty much full embrace of agentic AI, enterprises are setting up autonomous agents that plan and execute tasks, call application programming interfaces (APIs) and interact with applications, check in with other agents, and complete multistep workflows.

There may be an employee request that gets the ball rolling for AI work, or maybe a workflow is triggered when an agent notices a certain situation. Either way, there may then be dozens or even hundreds of interactions across databases, applications, cloud services, and other systems.

In the course of getting the job done, AI may be searching proposals, looking into customer relationship management (CRM) system data, checking sales forecasts, searching knowledge bases, generating presentation slides, scheduling meetings, or performing any

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

number of other tasks. An employee making an AI request may not even have a clue what's going on behind the scenes.

That means a network that once primarily carried human-to-application interactions is now carrying a ton of traffic that doesn't involve humans at all. It may be application-to-application traffic, AI-to-application, AI-to-AI, APIs having a chat, or cloud services exchanging data.

If a traditional network wasn't built for this kind of machine-to-machine communications, you can bet that traditional security architectures also weren't designed to protect autonomous interaction. Given that this AI genie isn't going back into the bottle (nor would a smart enterprise want it to), the challenge becomes creating the guardrails that allow for confident AI deployment at scale.


TIP

What's needed is the architectural foundation provided by unified SASE. The platform is increasingly critical for safe AI adoption, allowing secure connections, consistent policy enforcement, complete visibility, and full operational control for users, devices, applications, data, APIs, and AI systems.

Dealing With New "Users"

Who's using your network? In older times, the answer was generally limited to a list of a few kinds of users that were mostly made of flesh and bones. Employees were in the network. Customers were tapping in. Partners and contractors may have had access, too. Perhaps there were some service accounts running jobs, too, but all in all, those were simpler times, compared to today.

These days, humans are most definitely not the only users on the network. They aren't necessarily the busiest users, either. On today's networks, the real busybodies may be AI agents, automation platforms, APIs, LLMs, browser-based agents, cloud workloads, microservices, Kubernetes workloads, IoT devices, and various other machine entities or nonhuman identities (NHIs).

This fundamental change in network traffic and the entities involved creates a vastly different situation for those whose job is security. It was one thing to authenticate all the humans (which already was challenging enough). Now, organizations must

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

authenticate, authorize, monitor, and govern this new population of digital users.



WARNING

And yet, organizations haven't always intuitively been cautious enough about the digital NHIs. If these new entities were humans, organizations would certainly treat them with a cautious attitude. You don't just hand a brand-new employee the keys to the whole place. AI agents and all of the other NHIs out there need the same kind of careful onboarding and governance as any human. They might be out there on the network retrieving customer information, checking into financial reports, searching engineering documents, turning in purchase requests, exchanging data, even writing software.

Because they're doing high-value things, they're high-value targets for potential attackers. They need the same kinds of authentication, authorization, and monitoring that humans get.

That's why it's dangerous to think of AI agents like they're software applications. They're not. They're independent actors, and they all need their own individual identities.

Ensuring each agent is uniquely identified helps security systems answer key questions such as which applications the agent should be allowed to access, which databases it can search, which APIs it may call, which files it has permission to retrieve, which actions it's allowed to take, and which other agents it may communicate with. Individual identities help ensure clear rules can be established and then followed. Agent identities provide accountability.

And when agents have identities, it also becomes more possible to enforce concepts such as *least privilege*. This time-honored concept is just as applicable to machines as it has been to humans. No identity gets permission to do anything beyond what's needed for its assigned task.



REMEMBER

Zero trust is a related and also time-honored security tradition that must carry over from humans to NHIs. Every request and action from every entity, human or otherwise, must be treated with zero trust. Everything must be evaluated, considered, and approved based on the current context.

As NHIs take over more and more of the traffic on the network, and more and more attention from security teams, it's worth noting the kinds of communication patterns that are increasingly prevalent — patterns that didn't even exist until recently:

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Human to AI:** This one is easy to spot because humans are in this loop. A person asks an AI assistant to do something, and off it goes. That leads to some of the other communication patterns on this list.
- **AI to application:** Once an agent gets started on its task, it likely will interact with enterprise applications, such as the CRM system, inventory systems, or project management software. These interactions may happen through APIs, which are critical security boundaries.
- **AI to AI:** Agentic AI is great at collaborating. Specialized agents often work together, and the human that got the ball rolling may not have a clue how many agents are involved and how they're communicating.
- **Browser agent to cloud:** Browser-based AI may interact directly with websites and software-as-a-service (SaaS) applications. It may get into a browser session like a human would, and fill out forms, grab information, send support requests, and perform all kinds of other tasks.


TIP

Unified SASE can strengthen the management and protection of NHIs through a variety of capabilities. Bringing in protections such as zero-trust network access, continuous device assessment, identity-aware policy enforcement, and application-specific access controls, and you get a better handle on this new world where machines are at least as prevalent as humans, if not more so. The platform doesn't assume that authenticated identities should automatically gain broad access, but maintains continuous evaluation of identity, context, and behavior.

Equally important, unified SASE ramps up the visibility needed to secure this environment that welcomes a diversity of humans and intelligent machines. It simply no longer works to manage networking, identity, APIs, AI, and security using separate products. Unified SASE brings those disciplines together.

Defending Against AI-Powered Threats

The details of the battles may change, but there's one key plotline that runs through pretty much every story of IT security threat evolution. Some new technology innovation comes along, enterprises excitedly figure out how they'll benefit from it, and then

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

cybercriminals learn how to either target that technology or use it to their advantage.

AI is carrying that storyline forward, and putting it on steroids. Businesses are finding all kinds of ways to innovate with AI, and though they're still early in the plot, they're already enjoying great gains in productivity, improvements in customer experiences, and amazingly automated workflows. But malicious actors are working just as quickly to use AI in their attacks — and they, too, are getting better at what they do, and faster, and more adaptive and harder to stop.



WARNING

It's wild to think of cybercriminals honing skills and upping their game through technological brilliance, but it's how this story is unfolding. Like any business, they're boosting productivity with the help of AI. Yesterday's attacks may have taken a team of attackers a good bit of time to prepare and execute, but today they can be accomplished in minutes. AI helps attackers turbocharge their work in such areas as:

- Writing much better and more persuasive phishing emails along with convincing social engineering scripts
- Writing malicious code and fake websites that look great
- Ramping up vulnerability research through automation
- Discovering high-value targets
- Running attacks in multiple languages

These aren't necessarily new tactics, but they're being achieved much more quickly. Also, a widespread, sophisticated attack doesn't need as many people to achieve success, which either cuts the bad-guy overhead or frees up malicious actors to launch more attacks.

And, hate to say it, but they're achieving quality improvement through AI, just like legitimate businesses. Consider how easy it used to be to spot a phishing attempt purely through the laughably bad grammar and spelling, awkward sentences, even errors in company names. AI can easily come up with authentic-looking fake emails, employing persuasive personalization, and translating into different languages.

The quality improvement cycle has hit the malware department, too. Attackers have always sprung into action looking for ways

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

to get past new security defenses and detection techniques. AI is accelerating that work, quickly coming up with countless variations in an effort to find the new attack approaches. Polymorphic malware can change its appearance and behavior to adapt to defensive tools.

Here's the part of the story where the good guys regain the edge. AI turns out to be an incredibly powerful tool when it's in the hands of the defenders. Unified SASE is one way they leverage the positive power of AI, bringing AI-driven analytics and response into the common architecture along with identity, networking, security, and telemetry components.


TIP

Indeed, just as modern cyberattacks are increasingly AI-driven, threat prevention and response can be, too. The security service edge (SSE) aspect of unified SASE uses the AI technologies of today and tomorrow — combined with applying yesterday's great ideas of zero trust and least privilege to all identities — to stop malicious actors from succeeding. There's more detail in the next section on how to harness AI and automation for cyber protection.

Simplifying and Automating Unified SASE

Spend some time in a network operations center (NOC) or security operations center (SOC) and you know how cacophonous and overwhelming it can be. The professionals there deal with countless alerts and immense volumes of log entries. They have to handle performance issues, conduct security investigations, field help desk tickets, correctly revise configurations, and report it all out to the compliance folks.

All of that work is necessary. And any one of those alerts could be a harbinger of doom. But as IT infrastructure expands and becomes vastly more complex — with cloud complications and hybrid work and SaaS applications and AI — it's increasingly beyond human capacity to handle the volume and the noise.


REMEMBER

Fortunately, the AI that is making things more complicated also brings with it some of the best ways to get a handle on the challenges of network and security operations. Unified SASE is a tremendous opportunity to tap into the power of AI-assisted troubleshooting, autonomous remediation, digital experience monitoring, and policy optimization.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

That power is vital for more than one reason. On a day-to-day basis, it can bring relief to the humans involved in network and security operations, and help their work be more productive and effective. From a bigger-picture perspective, it helps the whole process move from a reactive posture to a more predictive and proactive approach.

To that second point, it moves the mindset dramatically. With a more distributed and complex architecture, waiting for issues is really just asking for trouble. With the power of AI and automation, it's no longer just a matter of finding out when things have gone wrong — attacks or downtimes or other performance issues — then addressing them and making improvements when the need becomes apparent. Intelligent systems such as unified SASE are constantly on the watch for subtle deviations and tiny warning signs, and can often spot them much earlier than humans can.

Consider a typical help desk call, reporting that an application isn't working properly. The human on the phone has lots of questions that need to be answered to get started figuring out what's wrong and what to do about it.

AI-assisted troubleshooting means the platform may already know what device or devices might be having issues, what the network connection quality is, details such as signal strength and SD-WAN path selection, what recent authentication activity has taken place, how the endpoint and browser are performing, and more. The platform is always gathering pertinent information, and by the time someone picks up the phone to report trouble, a unified SASE platform is not only aware of the issue but also has solutions in mind, thanks to AI.

The platform is similarly always looking for tiny clues that might indicate a potential breach or attack or inadvertent misconfiguration that left a door open. These clues may have been buried in the mountain of alerts and logs that humans have had trouble keeping up with.

So, AI can come in armed with diagnoses and potential solutions. It also can go ahead and implement some of those solutions through autonomous remediation. There are issues routine enough that human intervention isn't really needed — the platform can take care of it, or at least get a quick start. Sometimes a

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

redirection of traffic can do the trick, or maybe a temporary access restriction is needed to ensure zero-trust policies are followed.

If malicious activity is suspected, AI can immediately block communications. If an agent is acting in unusual ways, AI defenses can step on the brakes until the behavior is evaluated. AI isn't making business decisions, but it can certainly handle routine operational decisions and uphold policies.

Speaking of policies, you know that security policies have not always been easy to manage. And like everything else, it gets all the more complicated as the environment becomes more complex, with more applications and devices and cloud services and, now, AI agents.

AI offers an answer to that challenge, too. Intelligent unified SASE systems can uplift the work of policy enforcement in a number of ways. First of all, by keeping constant watch over broadly distributed environments, AI can make it easier to spot noncompliance before it turns into big trouble.



TIP

Beyond that, AI can analyze patterns across networking, identity, security, cloud services, and user behavior. That is a big help in policy optimization, not just enforcement. AI analysis helps point to rules that are obsolete, zero-trust policies that need to be tightened, excessive permissions that need to be reined in, shadow AI that needs to be addressed, duplicate configurations, and in general, things that could stand to be simplified.

Digital experience monitoring is another of the ways that unified SASE can tap into AI and automation to make work life better. For more on that, see Chapter 4.



CASE STUDY

HOW AI CAN ASSIST

To offer a quick example of how these ideas can work in the real world, consider how FortiAI-Assist works across the whole Fortinet Security Fabric platform, adding intelligent analytics and automation to networking and security operations.

Within FortiAnalyzer, FortiAI-Assist has a big picture view of unified logs, alerts, telemetry, and intelligence from across the platform, for

(continued)

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

(continued)

AI-powered triage, investigation, and threat response. From a perch inside FortiManager, FortiAI-Assist automates complex tasks and boosts operational efficiency. Within FortiSOC, agentic AI automatically investigates alerts, guiding and even executing remediation.

AI capabilities from FortiAI-Assist boost the SIEM and SOAR analyst experience, offer insight into cloud coverage capabilities and threats, and greatly enhance data collection and identification of network anomalies.

Tackling the OWASP Top 10



REMEMBER

The Open Worldwide Application Security Project (OWASP) is all about increasing IT security, and a big part is understanding risks. Its Top 10 lists are essentially required reading for security professionals. Unified SASE helps enterprises address many of the threats on the OWASP lists, including prompt injection or sensitive information disclosure.

- **Prompt injection:** Simply put, this is the AI equivalent of social engineering or phishing. It tricks AI into breaking the rules by sticking malicious instructions into seemingly innocuous AI prompts (direct injection) or within other info sources ingested by AI (indirect injection). Unified SASE can build guardrails that inspect prompts before they get to the model, checking for hidden and dangerous requests, enforcing policies, and evaluating responses.
- **Sensitive information disclosure:** This is one of the things that prompt injection might be trying to achieve, but disclosure of sensitive information can also occur quite accidentally. It can happen through the use of shadow AI, or even when using approved services. Unified SASE can use data loss prevention to identify confidential data before it is allowed to leave. Cloud access security brokers can offer visibility into AI applications. Secure web gateways can watch AI-related traffic.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Watching the experience
- Checking the role of SD-WAN
- Defining what we mean by "fast"
- Learning the art of monitoring apps
- Acting effectively when things go wrong

Chapter 4
Leveraging Experience-Driven SASE

The customer experience is an incredibly important focus for most enterprises. In the information technology (IT) world, the user experience is an increasingly critical success metric, too. This chapter explores how unified secure access service edge (SASE) can be used to drive the optimal digital experience across the organization. It checks out the role of monitoring (so you're not just waiting for disgruntled phone calls), where the software-defined wide area network (SD-WAN) fits into the picture, what we mean when we think of "fast" IT, details of monitoring different kinds of applications, and taking action when something goes awry.

Monitoring the Digital Experience

There was a time when the definition of IT success was mostly a matter of whether the network was up, whether servers were running properly, and whether applications were available and functioning properly. Check those basic boxes and you could assume that employees and customers had what they needed to be productive and happy.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Like everything else, the digital workplace today is much more complicated. Even if an employee's laptop is reliable, the internet connection solid and fast, and cloud application access uninterrupted, work may be sluggish due to a slow collaboration platform, or latency issues introduced by a regional internet provider or an overloaded cloud service.

The employee doesn't really know what the problem is, nor does she care. She just knows something is slowing down her progress. Her experience isn't optimal — and who doesn't get frustrated by a subpar technological experience?

That's why organizations aren't just measuring the nuts and bolts of the infrastructure. They're keeping tabs on the overall experience, through what's known as digital experience monitoring (DEM).



REMEMBER

DEM is one of the components of experience-driven SASE. The overarching point is that although network uptime and device status and things of that nature are important, they're also just a means to a greater end, which is actual user productivity and satisfaction.

A broader, more holistic view is the purpose of DEM. Yes, unified SASE keeps a close watch on whether firewalls are functioning, servers are serving, internet circuits are available, routers are moving traffic, and that kind of thing. But DEM wants to answer such queries as:

- How quick are user logins?
- Just how responsive is a particular application?
- How much time do transactions take to complete?
- Is the videoconferencing working well?

Consider what happens behind the scenes when an employee launches a cloud application. That request starts on the keyboard of the laptop. It moves across Wi-Fi, through an internet service provider, gets to a SASE point of presence, works its way through all of the appropriate security services and checks, heads out into the cloud infrastructure, then reaches the application. If all goes well, that journey takes a blink of an eye, but if performance gets held up in any of those places, the employee exclaims, "This application is so slow today!"

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

In a world that is increasingly all-digital, tracking availability is just not enough. DEM enabled through unified SASE provides much better visibility and more effective solutions.

DEM is watching the whole path, not just disconnected bits of infrastructure. The platform gathers telemetry from all of the endpoints and networks and paths and points of presence and cloud services that lie between the user and the app, and as a result has a good idea what's causing any particular performance problem.

The issue with that slow app might involve a networking consideration or it could be related to security, or a little bit of both. A unified platform puts all of the possibilities on the table, converging both worlds so that they can jointly focus on performance and experience.



REMEMBER

One more benefit of unification is the greater capability to turn telemetry into operational intelligence. DEM can transform countless individual measurements from all over the experience and reach conclusions about operational performance. DEM can spot the meaningful patterns and how they impact users. Troubleshooting thus becomes faster and more effective.

Seeing Where SD-WAN Fits In

DEM measures the experience, and having native SD-WAN integrated into unified SASE is one of the keys to optimizing that user experience, no matter what the network conditions might be. If DEM is like a car's dashboard, SD-WAN is like an intelligent navigation system, integrated for the most effective journey. It's looking ahead and watching road conditions, then picking the best route for getting to the destination efficiently.

SD-WAN is an entirely different animal from the enterprise networks of the past. When applications lived mostly inside corporate data centers and users worked largely at a corporate location, a static network could do the trick. These days users are anywhere and everywhere, maybe in the headquarters or branch office, maybe at home, maybe in a coffeeshop or a museum or an airport. Applications may be in countless places, too, most of them far from the data center.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Given that reality, it's not a surprise that conditions are always changing. Congestion is here at one point in time, there at another. Network circuits can become overloaded, cloud services might have regional slowdowns, applications may move. This afternoon's best path will likely be different from tomorrow morning's.



REMEMBER

No worries, that's the whole reason for having SD-WAN. Like the intelligent navigation system in the car, it's always evaluating available paths and intelligently selects which one is going to deliver the best experience. It's considering latency and packet loss, jitter and bandwidth, the requirements of applications and the mandates of policies. It's always ready to take advantage of a better path (and unlike the navigation system that might tell you to exit now to avoid a jam ahead, SD-WAN is handling the steering for you).

In fact, what it's doing is often called *application steering*, while others will call it *dynamic path selection*. It's never going to assume that a prior great path will be the best path right now.

AI, of course, makes everything more complicated, and you need SD-WAN that's up to the challenge. A single AI prompt may result in multiple application programming interface (API) requests, glances into knowledge bases, communications with agents, cloud interactions, data updates in business systems — all happening pretty much at once, many of the interactions quite latency sensitive.



TIP

Networks, therefore, need to be able to spot AI traffic and treat it appropriately. Fortunately, SD-WAN can intelligently discern whether traffic is application-related, video, voice, AI, or whatever. It then can properly prioritize and handle the distinct needs of that particular traffic type.

Again, this is all part of what you should expect from unified SASE; the architecture available from Fortinet is an example. It's vital to have an integrated approach that combines secure SD-WAN with cloud-delivered security services, with a common management system and operating platform. You want all of the pieces and parts — including SD-WAN, security service edge (SSE), DEM, and AI-assisted operations — to share telemetry and intelligence. What you *don't* want are disconnected networking and security products.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Rethinking What Fast Means

These days everyone wants everything as fast as possible. Back in the early days of Amazon, people were astonished that they could order practically anything online and have it two days later, but it became a pretty normal thing. Next thing you knew, there was routine one-day delivery. Now, your bored kid can ask you for new toy golf clubs and you're likely to find multiple vendors able to have them on your doorstep within the hour.

In this environment, no wonder everyone wants their digital experience to include fast connections and app launches and all of the other operations needed. The need for speed is a no-brainer, but the reality isn't quite as simple as building a superhighway.



REMEMBER

Fast, you see, isn't only about internet speed. There are all kinds of factors beyond bandwidth that influence user experience. Latency plays a key role, along with such variables as packet loss, application response times, domain name system performance, cloud service health, and more factors. Even if network speeds seem normal, you may not get fast (though you may get furious). The user perspective is what rules.

Better bandwidth is like a highway with more lanes. But although bandwidth essentially measures how much data can move across a connection, it doesn't necessarily determine how long it takes for data to get where it's going. Here are other factors to consider when figuring out how to achieve fast:

- **Latency:** This is essentially how long it takes for data to get from one point to another. Latency issues can wreak havoc in all sorts of situations, but they're especially obvious to users of certain applications. If your videoconference keeps freezing up or the audio is delayed, you're living a latency issue. It's less dramatic if an AI assistant takes longer to act due to a latency issue, but it still can be annoying.
- **Packet loss:** Sometimes you mail a letter and it never arrives. That's also the case with data on the network. That's packet loss, and when information gets lost on the trip, systems will retransmit missing data. The fix takes time, though. You may not notice this speed enemy when internet browsing, but it'll cause trouble with your videoconference or database transaction.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Jitter:** This isn't so much about speed as it is about consistency. Jitter refers to variations in network delay. If you're driving and are behind a slowpoke, that can be irksome, but what's really maddening is someone who brakes and accelerates and brakes and accelerates. They may average out to a decent speed, but if you're behind them, they'll drive you crazy.
- **Non-network problems:** When you're not getting fast results, it isn't always the network's fault: The application servers could be overloaded. There may be bottlenecks in authentication. Internet routing may be causing trouble. Browser extensions may be standing in the way. There could be DNS resolution delays.

AI adds new challenges to the quest for speed. Responsiveness can vary due to a model's inference time, how long it takes to dig into a knowledge base, authentication, prompt complexity, API response times, and other factors.

All the more reason to build the most connected, unified infrastructure such as unified SASE. And all the more reason to pay attention to the digital experience. People have a need for speed, no matter what, but their patience can vary depending on what they're digitally doing.

Monitoring Different Apps Differently

There are different needs of different kinds of apps when it comes to networking and security operations. For example, users won't stand for much latency in a videoconference, when delayed audio or locked-up video tend to spoil the meeting.



REMEMBER

The business of monitoring applications also varies significantly from one app type to another. For example, the approach for software-as-a-service (SaaS) applications differs a good bit from the way you monitor privately hosted applications. When the organization doesn't control the infrastructure, as with SaaS applications, there are visibility challenges.

Indeed, applications can be found all over a broad landscape. Some of them are still running in the corporate data center (which is, of course, where virtually everything used to run).

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Other applications are operating in public cloud infrastructure. And many are delivered as SaaS applications that are managed entirely by someone else.

Employees routinely use the apps, lots and lots of them every day, and they most likely have no idea where the apps reside. But the teams in charge of monitoring IT operations certainly know that they're in multiple places.

For privately hosted applications, monitoring may be easiest and visibility the highest. These are apps that remain fully under the organization's control. They might be internally developed business applications, some types of engineering software, certain healthcare applications, manufacturing systems, and in some cases, enterprise resource management systems.

IT owns the infrastructure and therefore has lots of visibility into everything, from server utilization to database performance to storage to network traffic to security controls.



REMEMBER

SaaS applications are a whole different story. Examples might include services such as Salesforce, Workday, ServiceNow, Microsoft 365, and Zoom. The enterprise has control over important aspects such as user identities, endpoint devices, security policies, local networks, and internet connectivity. But the IT department has zero control over the servers or cloud infrastructure or storage architecture. The local IT folks also aren't in charge of software updates and maintenance schedules.

AI applications present monitoring challenges of their own, because they often connect multiple systems. A single request might tap into resources and systems all over the place.

Experience-driven SASE can help resolve the monitoring differences and challenges by correlating telemetry from across many places: networking, security, cloud infrastructure, applications, endpoints, and AI. That makes it more feasible to focus on the user and the experience, without being bogged down by the technology complexities.

Adapting monitoring techniques to align with different application architectures simplifies the work of administrators, who enjoy a unified operational view. Speaking of user experiences, these users can appreciate how SASE changes their days.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Acting When Something Goes Wrong

IT teams spend much of their time trying to keep things from going wrong, which is as it should be. But they also must be ready for the inevitable, because things do go wrong. They just do. The response is what matters the most at this point.



REMEMBER

Unified SASE, turbocharged by AI and automation, shifts from monitoring into action when something goes wrong. Continuous monitoring means that problems are detected automatically. That telemetry and monitoring data become intelligence for generating actionable insights.

Automatic failover helps maintain business continuity when there are network issues, and the *automatic* part of it means that it happens without user intervention. Network failures thus turn from potential disasters into routine operational conditions that can be quickly resolved, and modern SD-WAN steers traffic to healthier paths.

AI and automation resolve common performance issues. And in situations when human judgment is required, AI has already handled investigations and provided summaries and recommendations.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Automating with AI
- Getting ahead on remediation
- Connecting what used to be disconnected
- Using AI to help people be better

Chapter 5
Building an Intelligent Unified SASE Architecture

Taking your company in the direction of unified secure access service edge (SASE) will be an achievement to celebrate, but don't think of it as a finish line. It's just the beginning of benefiting from an environment that learns and adapts and helps your information technology (IT) teams make smarter decisions.

This chapter explores the key role that artificial intelligence (AI) can play in your SASE architecture, how it helps you fix problems before the humans have even noticed they're having problems, how much you gain from unifying functions that have always been disconnected, and how AI accelerates the processes of troubleshooting and decision-making.

Tapping into AI

As you bring your intelligent unified SASE architecture to life, the first step into the future is building an understanding of the places where AI can really deliver exceptional value to your networking

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

and security. Many humans use AI almost daily to help them navigate the challenges of life, but when it comes to network and security operations, AI is far more than just a chatbot that delivers really good answers.

Far more than that, it's your new operations analyst, one who never sleeps or takes vacation or runs out for coffee. It's happily on the job 24/7, reviewing the vast volumes of information that's flowing through your network and security environment.

AI is keeping watch over users, endpoints, networks, cloud workloads, the performance of software-as-a-service (SaaS) and other applications, software-defined wide area network (SD-WAN) connections, security alerts or events, and overall metrics gauging the digital experience. All the coffee in the world couldn't charge up human analysts enough to cover all that with watchful eyes, but AI is up to the task.

That's not intended as an insult to humans. It's just that with the vast amounts of data from many places, there are ways a machine can process and analyze the information that are far beyond the capabilities of human brains.


TIP

AI-powered capabilities can automate operations and reduce complexity. AI can identify patterns, anomalies, and emerging issues that humans might miss. It will automatically handle routine operational tasks that in the past have consumed lots of valuable IT human resources and created alert fatigue. With AI on your team, you upgrade your threat detection and response in ways that correlate signals across users, devices, applications, networks, and cloud environments. And as your AI carefully eliminates the false positives, it prioritizes events to be sure the highest-risk issues are where they should be — at the top of the to-do list.

To that first point, AI is fantastic at connecting dots. As it analyzes network and security telemetry in real-time, it knows what's normal and what might be an anomaly. It does what humans used to have to do in terms of correlating signals from many different places, but it does so with machine speed, handling an unbelievable volume of data. Raw data quickly turns into intelligence.

Because it's processing the data and alerts, while correlating and spotting duplicate or false alarms, AI puts a huge dent in the alert fatigue that plagues human analysts. Alert fatigue isn't just a

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

hassle — it's a risk, because too many minor or useless alerts will inevitably get in the way of the real deal that needs real attention.

Incorporating an AI-driven unified SASE platform can automate lots of routine operational work. It's not eliminating prudent activities, but is taking them off the plate of people who probably weren't enjoying those tasks, anyway.

As it ramps up and speeds up the threat detection and response, it automates portions of the investigation process. The results of its analytical capabilities can help spot configuration inconsistencies, validate software updates, notice performance anomalies, put the spotlight on capacity concerns, and provide recommendations for policy changes.

Humans, meanwhile, get to spend more time focusing on bigger picture things. Their brainpower can think about architecture, planning and innovating, and pondering business priorities.

Remediating Proactively

You can't fix problems unless you know about them, right? That's a sensible concept, but it is a bit behind the times. Traditional IT operations have spent much of their day reacting to issues, which they typically have learned about when someone called the help desk. Experience-driven unified SASE turns that process upside down.



REMEMBER

Because the system is focused on digital experience monitoring (DEM), it's on the lookout for subtle changes that often show up in the data well before any user actually notices an issue. Could be a gradual and tiny increase in latency, or a bit of a rise in packet loss. Maybe an app is responding just a tad slower than usual, perhaps a few hundred milliseconds. No one is likely to notice these blips in their digital experience, but the AI-powered platform can spot tiny trends, correlate them, and figure out where they're heading.

With these insights, the platform can launch into proactive remediation. It can investigate and often fix issues before anyone notices a productivity hit. You're no longer waiting for a help desk call — and in fact, that help desk call never has to happen because the problem was nipped in the bud.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Proactive remediation can happen when the system reports a potential problem. But in many cases the remediation can be automated. The response may involve automatically rerouting traffic, recommending alternate security paths, triggering automated diagnostics, initiating failover procedures if needed, and then checking to be sure the experience has improved.

It's not just faster troubleshooting. It's often preventing the need for troubleshooting.

Consolidating Vendors

To reiterate an important point, unified SASE is unified. It's a consolidation of platforms into one SASE architecture. It's pulling together the work of a broad range of vendors that had accumulated over time as things got more complex.

You may have added a firewall at one point, a VPN at another, a tool for cloud security, a separate SD-WAN platform, a system for zero-trust network access, a DEM dashboard, products focused on such things as endpoint protection and security analytics and identity management. All are important, but each has its own console and dashboard, its own policy engine, its own software update schedule, individualized integration requirements, administrator training, and much more.



WARNING

The costs add up, and it's far more than just the price of the software. The complexity and fragmented visibility means humans going down duplicate paths needlessly, learning new interfaces, maintaining multiple systems, and correlating all the data. It's complex, it's expensive, it slows troubleshooting, and it makes it all the more likely that something important will be overlooked. You need visibility from end to end, from the user all the way to the applications, but you don't get that when you're tapping into multiple vendors.

All of that improves tremendously with unified SASE. No more jumping among multiple consoles because there's just one shared operational picture. Correlating information across platforms is a huge advantage. AI services also appreciate a unified platform, with better performance and smoother access to the information and connections they need to function well.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

It's worth noting that simple product aggregation isn't enough. Unified SASE works well because all of the pieces and parts are fully integrated, not just gathered under one roof but thriving as a happy family. It's not just a consolidation of related products, but a simplification of operations. And a unified SASE platform integrates AI into everything to make its work more efficient and effective, as the next section describes in more detail.

Sending AI in to Assist

One more reminder that, as with so many other parts of the enterprise, the future involving unified SASE is much brighter when it taps into the capabilities of AI. Not just AI tools that are bolted on, but AI capabilities that are built right into the platform.

Native AI capabilities in unified SASE are a godsend for troubleshooting. There are multiple intertwined factors that go into what the user experiences as either a "fast" experience or a "slow" application that causes them grief (for more on this, see Chapter 4).

The remedy to the slowness could be a simple fix that requires a few minutes, but figuring out what that fix is might take quite a bit longer because it involves weighing whether there's an overloaded endpoint or a routing issue or a problem with the cloud provider or any number of other potential glitches. With AI on the team, humans don't have to assemble the puzzle because AI has already put the pieces together by the time a problem is apparent.

The convenience of having a superfast helper is just the beginning of the beauty of the integrated AI. It speaks to you in your native language as well.


TIP

Got a problem? You used to have to hunt across multiple consoles in search of the potential source. Natural-language interfaces in unified SASE means the human administrator can just ask a conversational question. For example, "Why are the employees in St. Louis experiencing poor performance this morning when using Microsoft Teams?" That's what you really want to know, right? So, just ask!

Before you can take a breath or two, the AI assistant is already replying with an explanation. It seems that one of the regional

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

internet providers was having a latency issue, the assistant tells you. SD-WAN shifted traffic to a different path. Within three minutes, the user experience was back to normal, and there were not any security issues detected.

Although the environment has become increasingly complex in recent years, the problem-solving has gotten faster and easier. In fact, the problem-solving has been increasingly automated, and you can have a natural-language conversation with the machine that got it done without anyone asking.

It's not just a problem-solving miracle, either. AI assistance is there to help human administrators make better decisions about the network and security environment.

In a similarly straightforward way, for example, you can find out pertinent details that will inform your plan to roll out a new SaaS application to employees across the country (or all over the world). You can ask all the right questions, such as who has enough bandwidth and who doesn't, are there any new security policies needed, might this new app affect the way other business services perform, can existing zero trust policies be reused?

Beyond that, AI learns all the time. It's always building context, which means that each investigation or configuration or remediation informs the next one. Its understanding of the environment gets richer all the time.



REMEMBER

That helps the AI capabilities continue to improve. It also preserves institutional knowledge and helps new engineers and analysts succeed as if they've been around for years. You never know the value of a human's acquired knowledge until that human retires or gets a new job. AI keeps the wisdom in-house and on-tap for the future.

With that in mind, you can see how unified SASE powered by AI doesn't just improve networking and security. It helps make people better.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Creating simplicity and flexibility
- Protecting and tapping into AI
- Ensuring consistency
- Improving the digital experience
- Building a foundation for the future

Chapter 6
Ten Smart Moves for AI-Ready Unified SASE

You want a good reason to make a move into unified secure access service edge (SASE)? How about ten good reasons? This chapter explores some of the most compelling ways unified SASE will boost your enterprise's operations, from added simplicity to greater efficiency to flexible futures to the power of artificial intelligence (AI).

Making It Simpler

No one has ever tried to make a serious case that complexity is a good thing. It often seems inevitable, but is never desirable. Information technology (IT) environments have tended to get more complex all the time, with every new platform and tool and security need. And yet no one ever tried to sell complexity as a great new security feature.

Unified SASE is one of those seemingly rare opportunities to move in the other direction, the direction of simplicity. Consolidating networking and security into a unified platform brings shared visibility, shared policies, and shared intelligence. There's one management console, one unified examination of telemetry from

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

all over. That reduces the chances of anything bad falling through the cracks, whether users are on-premises or remote.

Trusting No One

What zero trust really means is verifying everyone, and it's a fundamental concept that is essential for tight IT security. The key in the world of unified SASE is that zero trust must apply not only to every person, but also everything else.


TIP

Zero trust must cover every user, all devices, every application, the whole roster of application programming interfaces (APIs), and all AI agents. Authenticate every connection, evaluate every request — and by the way, do all this automatically.

Keeping Tabs on AI

The question is no longer where in the enterprise you find AI operations — it's more like what area has *not* been touched by AI? It's all over, and the only way to keep it secure is to know all about where it is and what it is doing.

Unified SASE protects generative AI usage and keeps watch over prompts. Expect full visibility and usage governance so you know who's using what tool and tapping into what information. Responsible AI includes solid access controls and data protection policies, and it shines a light on shadow AI and the use of risky, unauthorized AI tools.

Asking AI for Help

Expect to tap into AI-assisted operations as you adopt and use unified SASE. Among other things, the platform should have tools that speed up troubleshooting and tuning, make remediation-policy recommendations, discover shadow AI, handle risk scoring, and complete autonomous remediation when appropriate.

The platform should ease the work of administrators and make it possible to easily get answers to questions such as why an app is running so slow, what policy should be used, and whether a

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

security alert is actually important. AI is a member of the team, capable of explaining, recommending, and doing.

Watching the Experience

IT analysts follow all kinds of metrics to see how things are operating and what things are out of kilter. Users don't care — all they want to know is if the thing they want to do is working properly. They are the customer, and that is what their experience is all about, getting things done and being productive.



REMEMBER

That's why digital experience monitoring (DEM) is so important, and why it's such a good idea to join networking and security operations through unified SASE. Together, these disciplines can make things work well for users, so that their digital experience is a satisfier. What's even better than a DEM add-on? DEM that's built right into unified SASE without the need for more hardware or software.

Enforcing Consistently

Rules are rules, no matter where the users are. Unified SASE allows you to apply security policies consistently everywhere and for everything — across branches, remote users, the cloud, private apps, and whatever other place or person or platform you're thinking about.



TIP

Consistent policy enforcement makes administration simpler whether users are remote or on-premises, closes security gaps, and cuts down on confusion. Attackers don't care where users are working, and the security architecture should not, either.

Reining in Vendor Sprawl

Some people think of vendor sprawl as an expense. And it's true, every time you add an IT product or service, you get another invoice to pay. But even more critical, vendor sprawl leads to complexity, with more policies, more training, more integration needed, and more opportunities for trouble.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Unified SASE, by its very existence as a unified product encompassing many of the things you used to buy different products for, reduces vendor sprawl. It improves visibility, simplifies management, and lowers costs.

Fighting AI with AI

Your employees are getting better with AI all the time. Unfortunately, so are your adversaries. You must plan for thwarting AI-powered threats by strengthening detection, prevention, and response workflows, using your own AI.


TIP

Unified SASE is well-equipped with AI functionality, because the best way to fight AI-savvy bad guys is with good AI that strengthens behavioral analytics, automated responses, threat intelligence and detection, and incident investigation.

Creating New Flexibilities

Flexibility is the key to business success in the future. Unified SASE helps keep your networking and security architecture nimble. It enables you to keep it simple while facilitating flexibility for such things as hybrid work, bring-your-own-device programs, thin-edge devices such as access points, and evolving cloud environments.

An adaptable architecture is welcoming to AI agents, who are valuable new team members. It responds well to changing business priorities. It deals with cloud migration and various work evolutions without complaint. What you need is an architecture that can adapt without requiring a total redesign every few years.

Getting Ready to Scale

Unified SASE powered by AI capabilities is a fantastic choice for today. It's an even better choice for tomorrow. If there's one thing the past few years have taught us, it's that change is happening faster all the time, and we need to be ready for anything.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Of course, most enterprises maintain growth as a key goal, which means operations must be prepared to scale. Your architecture must be ready to grow with whatever change comes its way — building capacity, adding new capabilities, exploring new directions with AI, meeting user needs for faster and simpler experiences. It should scale and innovate without ever sacrificing resilience or control.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

FORTINET

AI Changes Everything. Including SASE.

As AI transforms how people work and how data moves, yesterday's approach to networking and security isn't enough.

Fortinet Unified SASE provides the secure, intelligent foundation organizations need to connect users, applications, and data in the AI era.

One platform. Unified networking and security. Built for what's next.

Explore Unified SASE

www.fortinet.com/unified-sase

Understand intelligent unified SASE architecture

This book explores how AI is transforming the landscape and why unified SASE is ideal for an increasingly AI-driven operation. It spells out the fundamentals of SASE and all of the helpful components that align effectively. It discusses the challenges of securing AI in your operations, the dangers posed by malicious actors who also are very keen on the benefits of AI, and the promises of using AI to help secure your environment and thwart the bad guys.

Inside...

- Employing AI for a stronger defense
- Inviting nonhumans to the network
- Addressing threats powered by AI
- Automating the work of SASE
- Understand the user's digital experience

FORTINET

Steve Kaelble is the author of many books in the For Dummies series, and his writing has also been published in magazines, newspapers, and corporate annual reports. When not immersed in the For Dummies world or writing articles, he engages in healthcare communications.

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

ISBN: 978-1-394-46603-0
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.