SOLUTION BRIEF

Secure the Hybrid Workforce with Fortinet Unified SASE

Executive Summary

Work from anywhere (WFA) has significantly expanded the attack surface, encompassing home offices and mobile workers. This additional complexity makes securing networks, applications, and resources much more difficult. Secure access service edge (SASE) removes the complexity and offers IT teams a better way to protect their WFA users.

SASE solutions provide secure access and high-performance connectivity in branches of any size and remote locations. However, many SASE solutions only solve part of the problem. Fortinet Unified SASE addresses all WFA security challenges with a comprehensive, single-vendor SASE solution. It can deliver all components needed and removes complexity by integrating software-defined wide area networking (SD-WAN) with cloud-delivered security service edge (SSE) to extend the convergence of networking and security from the network edge to remote users. It also offers unified management, a unified agent, and end-to-end digital experience monitoring (DEM).

84% of companies have a hybrid workforce and need to secure WFA employees' access to the network, often from multiple locations—on-site, at home, or anywhere they can get a Wi-Fi connection.[1]

Hybrid Workforce Challenges

Securing the hybrid workforce presents unique challenges as the rapid expansion of new network edges and the increase in WFA employees have created vulnerabilities that cybercriminals now readily exploit. Security policies must be consistently applied and enforced, and an optimal work experience for all users must be provided.

Fortinet Unified SASE provides consistent security and user experience, whether users are accessing the web, corporate applications, or Software-as-a-Service (SaaS) applications. The solution includes a high-performance and scalable cloud network with 140+ locations globally, enabling broad coverage, scalability, and proven security controls.

Simple, Seamless, and Scalable Cloud-Delivered Security and Networking

Fortinet Unified SASE offers a full set of security and networking capabilities that go beyond the basic SASE elements offered by other vendors. Our solution includes:

Endpoint protection, zero-trust network access (ZTNA), and DEM

A single agent, FortiClient, is used for endpoint protection, ZTNA, and DEM.

FortiClient provides security for endpoints, whether local or remote. It delivers endpoint visibility via telemetry and ensures that all Fortinet Security Fabric components have a unified view of endpoints to provide tracking, awareness, compliance enforcement, and reporting.

Fortinet Universal ZTNA features flexible zero-trust application access control, regardless of the user or application's location. ZTNA allows IT teams to authenticate, secure, and monitor per-user and per-session access to business-critical applications. It supports continuous near-real-time device posture verification and blocks noncompliant devices and sessions in near real time.

DEM functionality simplifies troubleshooting and monitors end-to-end user experience. DEM shows a comprehensive view of the end-user experience and translates it into measurable business outcomes while reducing mean time to resolution. Fortinet delivers end-to-end DEM encompassing endpoint devices, on-premises networking, users, and applications. Last-mile monitoring ensures the fastest connection from each cloud location. First mile monitoring easily pinpoints issues down to the user's local network and endpoint device.

Firewall-as-a-Service (FWaaS) and secure web gateway (SWG)

FWaaS enables high-performance SSL inspection and AI-powered advanced threat detection techniques for cloud traffic, applications, and services. The Fortinet FWaaS solution establishes and maintains secure connections for remote users while analyzing traffic without impacting user experience.

SWG adds protections against advanced web threats with broad capabilities for securing web traffic, including encrypted traffic. Its web filtering, antivirus, file filtering, data loss prevention, and other security controls work together to enable a defense-in-depth strategy for managed and unmanaged devices.

Cloud access security broker (CASB) and data loss prevention (DLP)

The **FortiGuard CASB Service** provides comprehensive visibility, control, and security to SaaS applications. Malicious applications are blocked with inline CASB.

The **FortiGuard Data Loss Prevention Service** protects sensitive data against breaches, insider threats, and data exfiltration across the entire hybrid environment.

SD-WAN

Cloud-delivered SD-WAN capabilities, including application steering and dynamic routing, help identify the shortest path to corporate applications. It then makes corrections as the integrity of those connections changes, delivering and maintaining a superior user experience for remote workers.

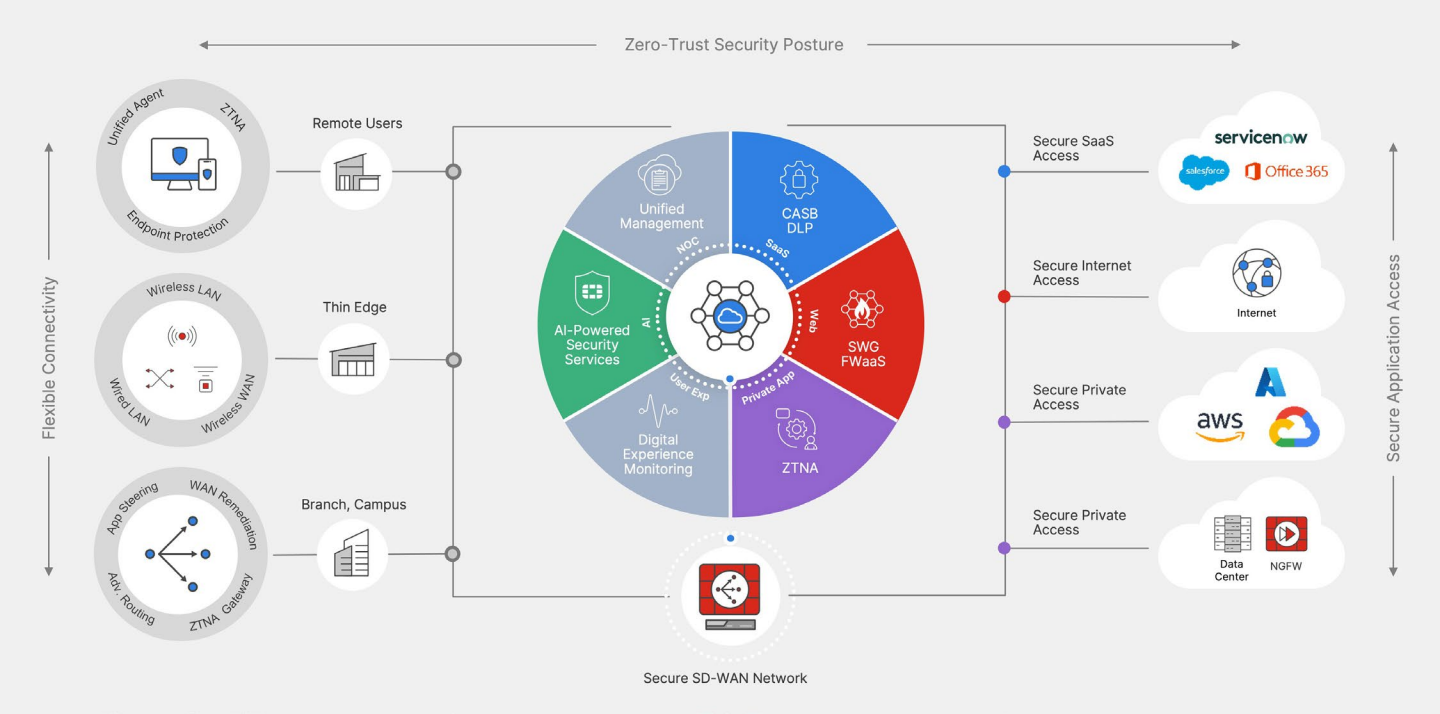


Figure 1: Fortinet Unified SASE with AI-powered security services

Key Use Cases

Secure internet access (SIA)

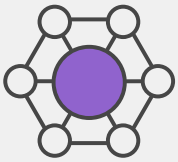
The comprehensive FWaaS and SWG capabilities secure managed and unmanaged devices by supporting agent and agentless approaches. Natively integrated FortiGuard AI-Powered Security Services protect content and users from ransomware and other sophisticated attacks.

Secure private access (SPA)

Zero-trust connectivity to corporate applications with unique SD-WAN integration provides low-latency access. ZTNA eliminates points of vulnerability by restricting network access. With Fortinet Universal ZTNA, you can implement granular application access to enable explicit, per-application access and help shift security strategies from an implicit trust model to a more secure explicit trust strategy. Fortinet Universal ZTNA provides continuous near-real-time device posture verification and blocks noncompliant devices and sessions.

Secure SaaS access

Next-generation dual-mode CASB, using both inline and out-of-band support, provides comprehensive visibility by identifying key SaaS applications and reporting risky applications to overcome shadow IT challenges. CASB and DLP offer granular control of the applications to secure sensitive data and detect and remediate malware in applications across both managed and unmanaged devices.



"The SASE market is not just growing; it's transforming how enterprises approach their network and security architecture. As businesses adapt to the new normal of hybrid work and distributed applications, integrating networking and security into a cohesive, cloud-native solution becomes paramount."[2]

Secure access from thin edge locations

Fortinet Unified SASE secures access to the internet and corporate applications from the thin edge with cloud-delivered AI-powered security to protect from malware, ransomware, and zero-day cyberthreats without any endpoint agents.

FortiAP wireless access points intelligently offload traffic from thin edge locations to a SASE point-of-presence for comprehensive security inspection at scale for all devices. This integration also means you can manage the Fortinet WLAN portfolio from the same management console being used for SASE. Our solution also offers cloud-delivered management of FortiAP devices with zero-touch provisioning, removing the need for local on-site administrative staff and reducing management costs.

Secure SD-WAN for branch and campus locations

Fortinet Unified SASE includes the industry's only organically developed software complemented by an ASIC-accelerated platform to deliver the most comprehensive secure SD-WAN solution for branch and campus. It provides real-time application optimization for a consistent and resilient application experience, along with advanced next-generation firewall protection. Transitioning from MPLS to broadband via SD-WAN reduces cost and enhances application performance. This shift optimizes user experience and provides security for direct internet access.

The Fortinet Advantage

Rather than providing an isolated, cloud-only approach, Fortinet Unified SASE is integrated with the Fortinet Security Fabric platform. Using one operating system, FortiOS, across security controls, the Fortinet Security Fabric provides broad visibility, granular control, and consistent, proactive protection everywhere. Additional benefits achieved with Fortinet Unified SASE include:

Reduced complexity and full visibility

Unified management equips you with the necessary tools to overcome the challenges associated with hybrid work, including visibility, protection, and optimization of the end-user experience. Fortinet Unified SASE provides a single console to manage all SSE capabilities, including FWaaS, SWG, ZTNA, CASB, DLP, and DEM.

Superior user experience

Productivity and quality of experience for remote workers are ensured with cloud-delivered SD-WAN capabilities such as intelligent application steering and dynamic routing.

Agentless connectivity

Agentless security is available for BYOD devices or devices where an agent cannot be downloaded, such as Chromebooks, with the use of proxy auto-configuration files and thin edge devices.

Thin edge security

Our thin edge SASE solution provides comprehensive, agentless protection and simplified management for thin edges delivered via FortiAPs and FortiExtenders. This enables secure access for OT/IoT devices and simplified access in home office and small office locations using Wi-Fi. This unique capability lets you extend enterprise-grade protection to thin edge locations without additional appliances, agents, or services.

Conclusion

Fortinet Unified SASE, powered by a single operating system, is an integrated, cloud-delivered solution that protects users, applications, and endpoint devices while seamlessly interoperating with the rest of the distributed network. Our unique solution provides unified network and security visibility and is easy to configure via its intuitive cloud-hosted user interface. A single management console for all SSE capabilities and DEM simplifies operations, improving ROI and facilitating the transition to hybrid-work security.

Our commitment to reducing complexity and offering flexible solutions is demonstrated by our diverse use case offerings, which range from traditional remote access to microbranch deployments and SD-WAN integrations. This adaptability extends zero trust, where continuous verification ensures robust security postures across all connections, even where software agents cannot be deployed.

Learn more about solving today's WFA challenges with Fortinet Unified SASE.

[1] E Shawn Farshchi, "How To Balance Employee Trust, Empowerment And Compliance In A Remote-Work World," Forbes, January 31, 2023.

[2] "Single-vendor SASE to Dominate Market Growth as Enterprises Favor One-Stop Solutions," Del Oro Group, January 24, 2024.

FORTINET

www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 22, 2024 2:49 PM

2271319-D-0-EN