SOLUTION BRIEF

Unified SASE: Comprehensive, Single-Vendor SASE for Securing the Hybrid Workforce

A Cloud-Centric and Scalable Security and Networking Solution to Protect Users, Devices, and Edges

Executive Summary

With the rise of the hybrid workforce, organizations have had to secure their employees who access the network and applications from on-site and off-site. This work-from-anywhere (WFA) shift has significantly expanded the attack surface, encompassing home offices and mobile workers, thereby increasing the complexity of network, application, and resource security.

Organizations dealing with numerous remote offices and WFA employees often encounter difficulties in consistently applying and enforcing security policies and ensuring an optimal work experience for users, regardless of their network location.

Securing this hybrid workforce environment presents a unique challenge as the changes have occurred organically rather than through a carefully planned strategy. The rapid proliferation of new network edges and the inclusion of WFA employees, often implemented as independent projects, have created vulnerabilities that cybercriminals eagerly exploit. On top of this, the trend has also led to organizations experiencing poor user, device, and application visibility, resulting in more threats and security gaps.

A secure access service edge (SASE) architecture helps address these exploits by providing secure access and high-performance connectivity to users in branches large and small or in any remote location. However, many SASE solutions only solve part of the problem. They either fail to provide consistent enterprise-grade cybersecurity to their hybrid workforce or cannot seamlessly integrate with the range of physical and virtual network and security tools deployed at the network edge. The result is an inability to deliver consistent cybersecurity and optimal user experiences.

Unified SASE, built on the Fortinet single-vendor approach, delivers a comprehensive SASE solution by integrating software-defined wide area network (SD-WAN) with a cloud-delivered security service edge (SSE) to extend the convergence of networking and security from the network edge to remote users, together with a unified management, unified agent, and digital experience monitoring (DEM).

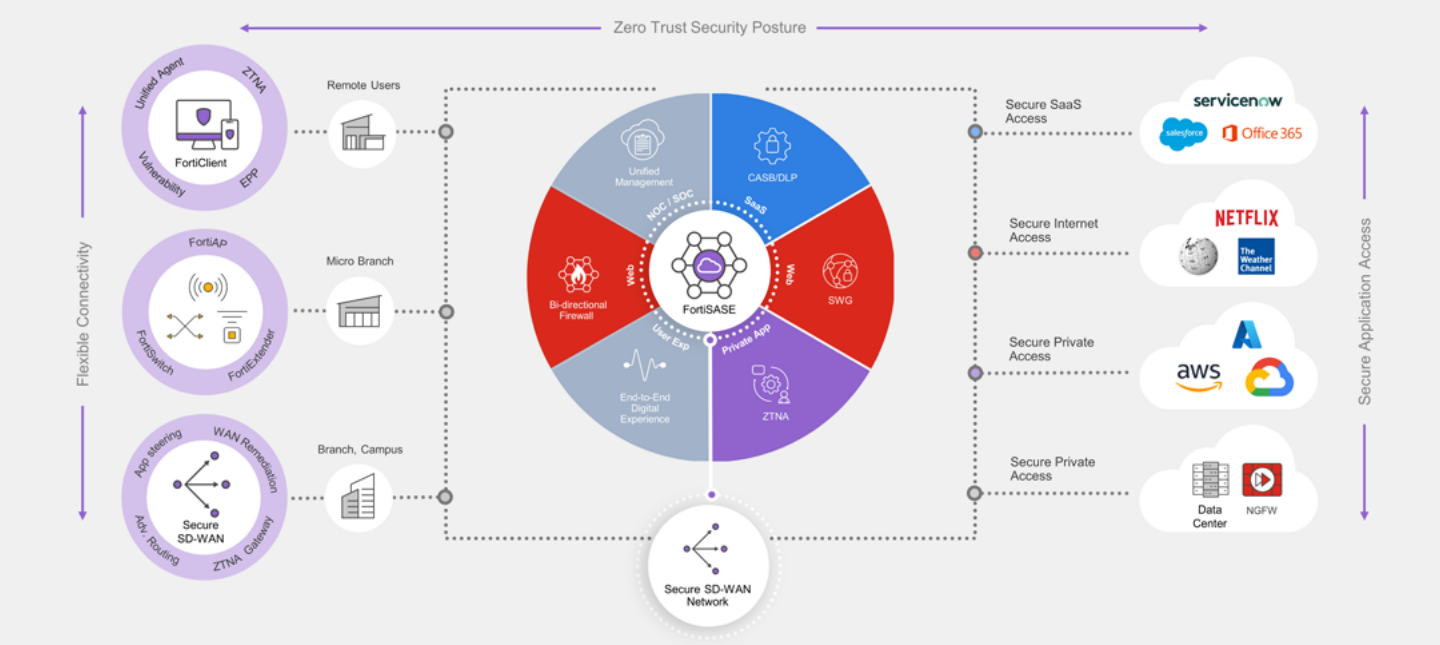

Figure 1: Unified SASE with AI-powered security services

Unified SASE has been specifically engineered to converge networking and security into an integrated and adaptive solution to ensure optimal and secure connectivity for the hybrid workforce. Unified SASE is a comprehensive cloud-centric SASE solution that safeguards WFA users with the same underlying OS, AI-powered services, unified agent, management, and experience monitoring as our on-premises solution. And it secures all users, devices, and edges, including microbranches, for the best flexibility for organizations with disparate architectures and requirements.

Fortinet Unified SASE includes a high-performance and scalable cloud network with 100+ locations globally, enabling broad coverage and scalability for all our customers, regional and global. Unified SASE provides the utmost security, whether users access the web, corporate applications, or Software-as-a-Service (SaaS) applications.

Unified SASE, driven by FortiOS and FortiGuard AI-Powered Security Services, provides simple and scalable networking and security convergence for consistent protection and superior user experience for the hybrid workforce.

The Unique Fortinet Strategy

Our unique secure networking strategy, driven by a single operating system called FortiOS and enhanced with FortiGuard AI-Powered Security Services, enables Fortinet to weave security and networking functionality into a single, integrated system to deliver consistent security and user experience to any user anywhere.

Unified SASE enables organizations to secure access to the web, cloud, and applications with enterprise-grade cybersecurity and superior user experience built in.

Simple, Seamless, and Scalable Cloud-Delivered Security

An intuitive cloud-based user interface provides unified network and security visibility and is easy to configure. You can instantly see endpoints, users, point-of-presence graphical information, and threat analytics.

As a single-vendor SASE solution, Unified SASE is managed by Fortinet FortiManager, providing unmatched visibility, management, and consistent security policies across on-premises and remote users. Its SSE component, FortiSASE, offers easier user onboarding and the industry's most flexible tiered user-based licensing model. This allows organizations to transition from CapEx to OpEx business models to keep the costs of today's highly dynamic networks and infrastructures predictable.

FortiSASE is also Service Organization Controls (SOC 2) certified. It provides independent validation that its solution security controls operate per the American Institute of Certified Public Accountants applicable Trust Services Principles and Criteria. This SOC 2, Type II standard certification demonstrates Fortinet's commitment to ensuring our customers meet diverse compliance requirements.

Additionally, FortiSASE offers a comprehensive set of enterprise-class security capabilities already fully integrated into the solution, including SWG, zero-trust network access (ZTNA), next-generation dual-mode CASB, FWaaS, and advanced threat protection capabilities.

Unified SASE supports five critical use cases:

1. Secure internet access

For WFA users operating outside the corporate perimeter, direct internet access expands their attack surface and risk. Unified SASE offers comprehensive SWG and FWaaS capabilities to secure managed and unmanaged devices by supporting agent and agentless approaches.

2. Secure private access

With the hybrid workforce, traditional VPNs struggle to scale. And because they do not include integrated inspection or advanced protections, compromised VPN tunnels can open access to every application, expanding the attack surface and increasing the risk of lateral threat movement. Unified SASE Secure Private Access (SPA) offers the industry's most flexible and secure connectivity to corporate applications.

Using a Universal ZTNA approach, organizations can implement granular application access to enable explicit, per-application access to help shift security strategies from an implicit trust model to a more secure explicit trust strategy. Unified SASE SPA also integrates seamlessly with SD-WAN networks to automatically find the shortest path to corporate applications powered by the intelligent steering and dynamic routing capabilities available in Unified SASE.

3. Secure SaaS access

Given the rapid increase in SaaS adoption, organizations continue to struggle with shadow IT challenges and stopping data exfiltration. Unified SASE SPA with 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. Next-generation CASB also offers granular control of the applications to secure sensitive data and detect and remediate malware in applications across both managed and unmanaged devices.

4. Branch transformation

With Fortinet Secure SD-WAN, organizations can improve connectivity, operations, and application access by enhancing and securing the WAN on-premises. This transformation results in a significantly better user experience for all.

5. VPN to ZTNA transition

ZTNA eliminates points of vulnerability by restricting network access. Also, the transition from VPN to ZTNA and adopting extensive identity verification leads to only appropriate users being granted access to the data and systems relevant to their role in the organization.

Delivering Comprehensive Security Capabilities at Scale

Unified SASE offers full security capabilities to secure traffic destined for the internet, private data centers, and SaaS applications.

Unified management and DEM

Unified SASE offers high visibility across both on-premises and remote users. With FortiManager, organizations can leverage a unified policy engine and management system that spans all edges and users, regardless of their location.

Unified SASE innovates by adding DEM functionality. DEM empowers organizations with unified visibility into users' experiences as they interact with applications and devices. DEM encompasses endpoint devices, on-premises networking, users, and applications. It allows organizations to obtain a comprehensive view of the end-user experience and translate it into measurable business outcomes.

Unified SASE equips organizations with the necessary tools to overcome the challenges associated with hybrid work, including visibility, protection, and optimization of the end-user experience.

Unified agent and Universal ZTNA

A single agent, FortiClient, is used for fabric integration, secure access, and endpoint protection. The Fortinet unified agent provides endpoint visibility via telemetry and ensures that all Fortinet Security Fabric components have a unified view of endpoints to provide tracking and awareness, compliance enforcement, and reporting. FortiClient delivers security and protection for endpoints, whether local or remote.

Fortinet Universal ZTNA features the industry's most flexible zero-trust application access control, regardless of the user or application is location. ZTNA allows IT teams to authenticate, secure, and monitor per-user and per-session access to business-critical applications. Universal ZTNA functionality can be applied everywhere for all users and devices, regardless of location. This shifts security from an implicit access approach to a more secure explicit access strategy, per application, based on continuous identity and context validation.

FWaaS and SWG

Leveraging the independently certified capabilities of FortiOS is the core of the Fortinet industry-leading security fabric strategy. It enables high-performance SSL inspection and advanced threat detection techniques for cloud traffic, applications, and services. Without impacting user experience, the Fortinet bi-directional FWaaS solution establishes and maintains secure connections for remote users while analyzing inbound and outbound traffic.

The SWG also protects against the most advanced web threats with broad capabilities for securing web traffic, including encrypted traffic. Its web filtering, antivirus, file filtering, data leak prevention, and more work together to enable a defense-in-depth strategy for managed and unmanaged devices.

CASB and data leak prevention

Unified SASE enables secure SaaS access with support for inline and out-of-band CASB capabilities. These capabilities are powered by the FortiGuard CASB Service to provide comprehensive visibility, control, and security to SaaS applications.

As a part of its cloud-delivered security services, Unified SASE also includes the FortiGuard Data Loss Prevention Service to protect sensitive data across the entire hybrid environment. This service includes a wider range of data identifiers, file types, and SaaS applications, as well as advanced data-matching techniques to prevent inadvertent data leaks. By continuously enhancing DLP, Fortinet provides organizations with deep insights into cloud applications and tools to effectively counter new threats.

Secure SD-WAN

Fortinet Secure SD-WAN transforms networking and security powered by one OS. Fortinet is the first vendor to organically deliver SD-WAN, NGFW, advanced routing, and ZTNA application gateway in one WAN edge. As Fortinet Secure SD-WAN is the only vendor with purpose-built ASICs across all platforms, it allows for massive scaling and performance.

Secure SD-WAN intelligently and dynamically steers 8,000+ applications, including industrial application signatures. With forward error correction and packet duplication, the Fortinet solution remediates WAN impediments automatically. Furthermore, the tight integration across the LAN, WLAN, WWAN, and ZTNA enables organizations to seamlessly transition to SD-Branch and SASE.

Also combined with FortiSASE, Secure SD-WAN offers an integrated, simpler, more automated, and more easily consumable service, also called Secure Private Access, as mentioned previously. FortiSASE SPA enables broader and seamless access to every private application at private data centers or public cloud environments by automatically finding the shortest path to each application, including VoIP and other unified communications applications, enabling superior user experience without requiring infrastructure upgrades. It allows organizations to enable secure access to private applications for WFA users leveraging existing SD-WAN or NGFW investments.

Flexible Connectivity

- **Unified agent:** FortiClient is a single agent for security fabric integration, SASE, and endpoint protection. The Fortinet unified agent provides endpoint visibility through telemetry and ensures that all Fortinet Security Fabric components have a unified view of endpoints to provide tracking and awareness, compliance enforcement, and reporting. Automatic ZTNA tunnels provide secure remote connectivity. FortiClient provides security and protection for endpoints, whether local or remote.
- **Agentless connectivity:** Agentless security is available for BYOD devices or devices where an agent cannot be downloaded (like Chromebooks) using Proxy Auto-Configuration files.
- **Microbranches:** Fortinet Unified SASE includes expanded integrations within the Fortinet WLAN portfolio to further support organizations securing microbranches and related devices. FortiAP wireless access points intelligently offload traffic from microbranches to a SASE point of presence (POP) for comprehensive security inspection at scale for all devices. This integration also means the Fortinet WLAN portfolio can be managed by the same simple, cloud-based management console customers already use for SASE. This complements Fortinet's existing support for users at the location and presents organizations with a new approach to cloud-based security by extending enterprise-grade protections, such as sandboxing, intrusion prevention systems, and URL filtering, to microbranches without additional appliances or services.

  Unified SASE also supports managing and integrating a FortiExtender configured as a LAN extension. A FortiExtender with the LAN extension configuration allows an edge deployment. An edge deployment is a branch office with a LAN behind a FortiExtender with secure internet access over a backhaul connection to Unified SASE. By relying on FortiExtender instead of FortiClient to handle secure connectivity to Unified SASE, this solution essentially extends the single-user, single-device FortiClient endpoint case to a multi-user, multi-device LAN environment.
- **Secure edge:** To optimize user experience, Unified SASE lets you choose to perform security with your local FortiGate or connect branch offices to Unified SASE for security inspection in the cloud via FortiGate NGFW and Fortinet Secure SD-WAN. It allows you to manage traffic during seasonal peaks or when the company is growing rapidly. It also permits offloading guest traffic to Unified SASE for secure internet access and performs local security for employees.

The Fortinet Difference

Rather than providing an isolated, cloud-only approach, Unified SASE offers services built into the Fortinet Security Fabric. By extending and using the power of FortiOS, the Fortinet Security Fabric provides broad visibility, granular control, and consistent, proactive protection everywhere.

- **Consistent cybersecurity for users, whether on- or off-network:** Unified SASE offers comprehensive cloud-delivered security with natively integrated ZTNA to provide consistent protection for WFA users.
- **Unified agent:** One unified agent supports multiple use cases. The FortiClient agent can be used for ZTNA, traffic redirection to SASE, and endpoint protection without requiring multiple agents for each use case.
- **Unified management and visibility:** Unified SASE offers high visibility across both on-premises and remote users, ensuring the security of the modern hybrid workforce. With FortiManager, organizations can leverage a unified policy engine and management system that spans all edges and users, regardless of their location.

  Also, FortiAnalyzer, in conjunction with Unified SASE, provides centralized logging and response capabilities for networking and security across the entire organization. This enables organizations to understand their network and security events, facilitating effective incident response and mitigation.
- **Superior user experience:** Applications are intelligently and dynamically steered over appropriate links, ensuring business productivity and quality of experience. WFA users can leverage the superior user experience to access corporate applications with SD-WAN SPA securely.

These technologies, powered by a single FortiOS operating system, provide an integrated, cloud-centric SASE solution that protects users, applications, and endpoint devices while seamlessly interoperating with the rest of the distributed network. This effortless end-to-end approach to converging networking and security enables the sort of adaptive strategy organizations require in today's rapidly evolving digital environment.

Also, with the expansion of the single-vendor SASE approach, Unified SASE has become the industry's most comprehensive and integrated SASE offering. It safeguards users, access, edges, and devices anywhere while delivering the highest ROI, consistent security posture, and improved user experience. Driven by a security and networking convergence approach, Unified SASE enables a simple, secure networking journey toward SASE for today's hybrid workforce.

February 5, 2024 4:13 PM

2271319-C-0-EN