WHITE PAPER

A Future-Ready Security Platform for AI, Cloud, and Hybrid Work

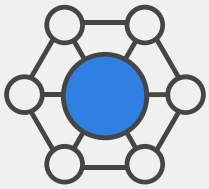
Flexible, High-Performance Fortinet Unified SASE Addresses Modern Networking Challenges and Threats

Executive Summary

Hybrid work, cloud-first strategies, and rapid generative AI (GenAI) adoption are fundamentally changing how users access applications and data. Meanwhile, new AI-driven risks are being introduced. They include unsanctioned AI usage, sensitive data leakage into public models, and AI-assisted cyberattacks.

Simultaneously, security and networking teams face mounting pressure to reduce risk, control costs, and do more with limited resources. Traditional VPNs, cloud-only security services, and fragmented SD-WAN deployments cannot keep up. This results in security gaps, inconsistent policy enforcement, performance bottlenecks, operational complexity, and limited visibility into AI-driven activity.

Fortinet Unified SASE addresses these challenges by converging networking, security, and AI-driven protection into a single, high-performance platform. Built on a single operating system, one policy engine, and one management plane, Unified SASE delivers consistent zero-trust enforcement, optimized application performance, GenAI application visibility and control, and end-to-end intelligence across users, devices, and locations, on-net and off-net.



Gartner Market Forecast

Gartner® estimates the market for SASE will grow at a compound annual growth rate of 26.0% over five years, reaching $28.5 billion by 2028.[1]

By integrating secure SD-WAN, security service edge (SSE), zero-trust access, GenAI security controls, and AI-powered security services (including FortiAI-Assist), organizations can simplify operations, govern AI usage, enforce compliance at scale, improve user experience, and reduce total cost of ownership. The final result is a future-ready foundation that aligns security, networking, AI governance, and business priorities for modern enterprise environments.

The Limits of VPNs and Cloud-Only SSEs

Hybrid work, SaaS adoption, and GenAI-driven workflows have exposed fundamental limitations in traditional network and security architectures. VPN-centric access models were designed for a small number of remote users accessing applications hosted in a central data center. Once connected, users often gain broad network access, increasing lateral movement risk and expanding the blast radius in the event of a breach. VPNs struggle to inspect increasing volumes of encrypted traffic and AI-generated content.

Also, cloud-only SSE architectures attempt to modernize security but often rely on centralized inspection points, forcing traffic hair-pinning, increasing latency, and creating inconsistent enforcement for on-net and off-net users. Critically, many lack granular controls for emerging GenAI applications, leaving organizations without visibility into which AI tools are being used, what data is being shared, and whether sensitive information is exposed to public models.

When combined with standalone SD-WAN, enterprises must manage multiple tools, consoles, and policies across separate data silos, while also attempting to bolt on AI governance tools. This dramatically increases operational complexity.

The result is higher costs, reduced visibility, unmanaged AI risk, and growing operational fatigue across security and networking teams. Organizations need a unified approach that delivers consistent zero-trust enforcement, high performance, AI governance, and simplified operations across users, devices, branch offices, campuses, and edge environments.

Unified SASE in Practice: Unified, Flexible, Intelligent

Fortinet Unified SASE delivers high-performance security and networking for users regardless of location. Employees, contractors, and partners experience the same protection, access controls, and application performance whether they are on the corporate network, working from home, or roaming. Automatic on-net and off-net detection ensures seamless policy enforcement without manual VPN switching or security gaps.

Universal zero trust

Zero-trust access is applied universally across all environments. Access decisions are continuously verified based on user identity, device identity, and device posture, with checks occurring every 60 seconds. Granular controls leverage dozens of posture attributes to determine access to each application, while a single unified agent supports secure access, endpoint protection, vulnerability scanning, and web filtering. This delivers a truly unified and intelligent security experience.

AI-native security and operational intelligence

Unified SASE provides comprehensive visibility and control over AI application usage across the organization. It enables discovery of GenAI tools, enforcement of granular policies governing data sharing with public AI models, and the prevention of sensitive data exfiltration. Integrated DLP, CASB, and inline inspection capabilities extend to AI-driven workflows, while advanced threat detection helps identify AI-assisted attacks, such as automated phishing and content manipulation.

GenAI security and assistance

By embedding GenAI protection directly into SSE and secure SD-WAN enforcement points, organizations eliminate separate AI security silos and ensure consistent inspection wherever users connect.

Complementing these controls, FortiAI-Assist integrates GenAI into the Unified SASE management experience to accelerate operations. This includes translating natural language into policies, summarizing alerts with contextual risk insights, automating troubleshooting across network and security domains, and speeding root cause analysis through correlated telemetry. Ultimately, operational overhead is reduced, and security teams can scale efficiently.

Secure Access for Users, Devices, and Edges

According to Gartner, "By 2027, 50% of CIOs and chief information security officers [CISOs] will push for consistent secure access for all types of entities, including users and devices at branch office, campus and edge locations."[2]

Performance-first architecture

East-west traffic across branches, campuses, and IoT or OT environments is segmented and inspected using hardware-accelerated enforcement. This granular segmentation limits lateral movement and enables instant threat containment, significantly reducing organizational risk.

Application availability and performance are protected through an autonomous, application-aware SD-WAN architecture with built-in self-healing. The platform continuously monitors for congestion, brownouts, and link failures, dynamically steering traffic across broadband, 5G, and MPLS links to maintain predictable performance.

Each site operates without a single point of failure, continuing to forward and inspect traffic locally even during disruptions, providing a flexible and resilient network experience.

Sovereignty and compliance without compromise

Unified SASE also enables organizations to meet data sovereignty and regulatory requirements without compromising user experience. Location-aware policies ensure traffic is inspected locally or within specific regions when required, while still providing seamless access as users move between locations. Sovereign deployment options, including FortiSASE Sovereign and flexible service models, including managed services, support compliance across global environments, reflecting the solution's intelligent and adaptive design.

Simplified platform economics

By consolidating networking and security into a single platform, Unified SASE significantly reduces complexity and cost. Secure SD-WAN, SSE, zero trust, wireless, LTE and 5G connectivity, and AI-powered security services all operate on the same OS, policy engine, and management plane. This consolidation eliminates overlapping tools, reduces operational overhead, simplifies licensing, and delivers a predictable cost model with industry-leading total cost of ownership, illustrating the platform's truly unified and simplified approach.

End-to-End Intelligence and Visibility

Unified SASE provides end-to-end visibility that accelerates troubleshooting and reduces mean time to resolution. Telemetry from endpoints, networks, and security services is correlated within a unified data lake and enriched with built-in digital experience monitoring.

Teams gain full visibility from the endpoint to the application, enabling rapid identification of whether issues originate in the network, security controls, endpoints, or cloud services. Integrated analytics, FortiAI-Assist, and optional SOC services further streamline operations and strengthen security outcomes, making Fortinet Unified SASE the most flexible, intelligent, and unified solution for modern enterprise hybrid security.

The Future of Secure Access Starts with Unified SASE

Fortinet Unified SASE represents the next evolution of secure access with purpose-built for AI adoption, cloud scale, and hybrid work realities. By converging networking, security, AI governance, and GenAI-powered operations into a flexible, high-performance platform, organizations can enforce zero-trust access everywhere, govern GenAI safely, improve user experience, simplify operations, and future-proof their infrastructure for what developments and threats come next.

[1] Charanpal Bhogal, Charlie Winckless, Neil MacDonald, Andrew Lerner, John Watts, Shailendra Upadhyay, Christian Canales, Marissa Schmidt, Jonathan Forest, Gartner Forecast Analysis: Secure Access Service Edge, Worldwide, Gartner, February 5, 2025. https://www.gartner.com/en/documents/6152891

[2] Ibid.

March 10, 2026 5:57 PM / MKTG-2980-0-0-EN