



Lumen® SASE with Fortinet

A fully integrated network and security converged solution deployed at the edge, enabling a single, seamless, secure access experience

A Wakeup Call to Distributed Businesses

Enterprise networks increasingly rely on cloud-based applications to run their businesses and support remote and mobile users. The enterprise network has grown beyond the conventional network edge, challenging IT to secure and manage an ever-expanding attack surface. VPN solutions alone are not enough to protect users working remotely. For organizations to remain secure, all endpoints must be secured and managed with the same security and networking policies as their on-premises infrastructure, regardless of where they're located.

“**Failure to modernize infrastructure and invest in operations automation and intelligent security practices will severely impede the success of organizations.**”

—SASE: Addressing the Fundamentals, IDC, 2022.

Today's distributed workforce requires anywhere application access for users and their many devices. The need for diverse services, such as remote work environments, application adoption, hybrid cloud, and others, presents increased demands on IT:

- Limited IT and security resources and expertise
- The extended attack surface associated with hybrid work
- A complex and fragmented ecosystem of users, endpoints, and datasets
- The unrelenting pace of technological change in enterprises (e.g. IoT, edge computing, multiple clouds)

Lumen SASE with Fortinet

Over time, many organizations built a patchwork of solutions with multiple vendors to secure different services, applications, and protections. These were often complex, inflexible, and limited due to lack of integration or scope of capabilities. Considering current infrastructures, the expanding threat landscape, and a widely distributed workforce, businesses today require a simplified, optimized, secure way to protect businesses at the edge.

Secure Access Service Edge (SASE) is a security-driven networking solution for the enterprise, combining tightly integrated technologies designed to deliver seamless, secure access to every worker and company device, wherever they are located. It begins with an industry-leading next-generation firewall (NGFW), supported and enhanced by FortiGuard Labs threat intelligence services. NGFW with SD-WAN capabilities deliver high-performance security and connectivity at scale, enabling maximum flexibility and security for any configuration or environment.

SASE is fast and easy to deploy, and intuitive to learn, because everything is designed to work seamlessly with everything else through centralized management and full integration and orchestration.

From next-generation firewalls and multifaceted threat protection, to software-defined wide area networking and cyber protection support, SASE cloud-based services deliver a host of compelling, integrated solutions.

Core Components

Next-Generation Firewalls (NGFW): Provide full visibility and threat protection for any edge at scale, weaving security deep into the hybrid IT architecture for security-driven networks. NGFWs combine deep inspection and advanced techniques to maintain secure connections and end-to-end security protection for users, devices, applications, and data.

SD-WAN: A flexible, fast and scalable, software-defined approach to managing and securing the WAN. The integrated, security-driven networking approach consolidates SD-WAN, NGFW and advanced routing, enhancing work-from-anywhere from any edge.

Zero Trust Network Access (ZTNA): Allows organizations to shift from implicit to explicit trust by creating application-specific level access, while providing IT control and visibility into who and what is connected to the network. ZTNA includes several technologies working together—multi-factor authentication (MFA), network access control (NAC), access policy enforcement, and integration with dynamic network segmentation.

FortiClient: Delivers protection, compliance, and secure access in a single, modular lightweight client that runs on an endpoint, such as a laptop or mobile device. It enables secure, remote connectivity and the application of consistent access policies across devices, while also providing information, visibility and control to each connected device.

FortiManager: Provides centralized management from a single console, for complete visibility of devices on the network, security policy management, and accelerated deployment and provisioning at scale.

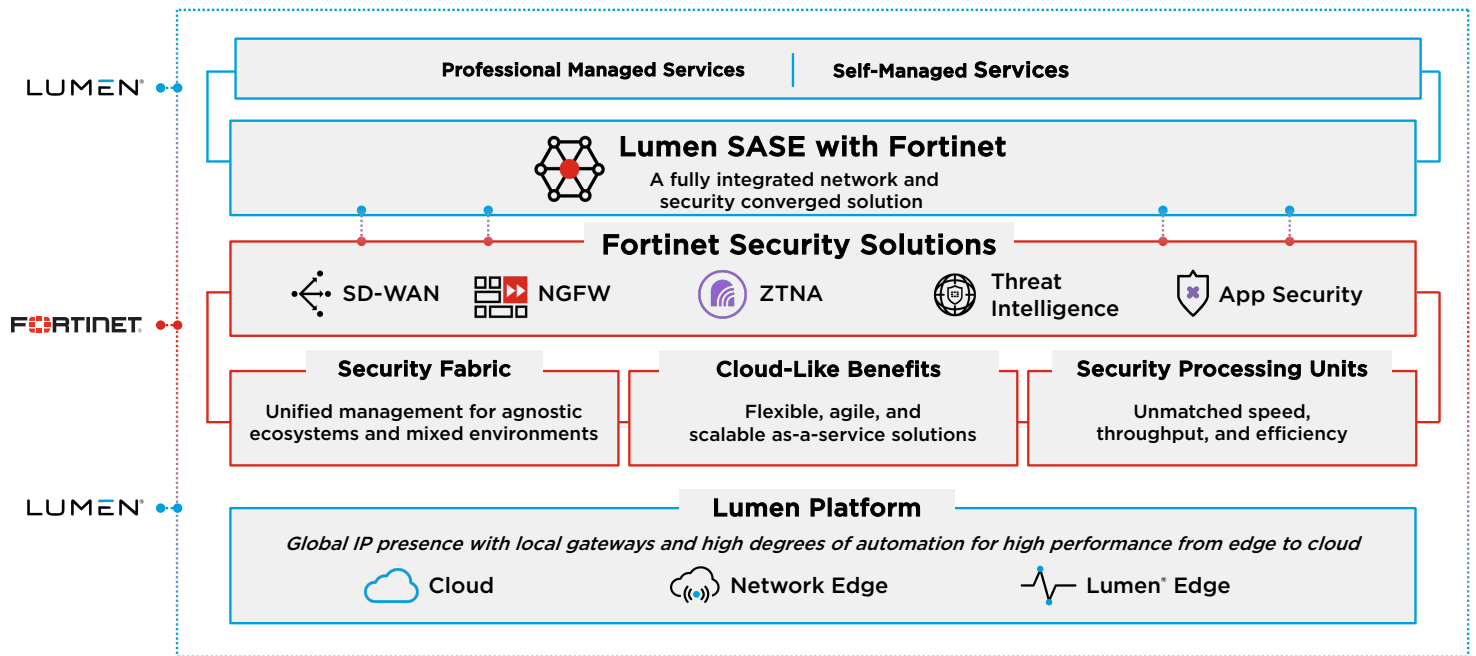
FortiAnalyzer: Is a reporting, analytics, and automation platform with complete visibility of the entire attack landscape, for advanced threat detection and rapid response against cyber risks.

Fortinet's Threat Intelligence from FortiGuard Labs: Uses artificial intelligence and machine learning to analyze over 100 billion security events and to provide one billion security updates every day in real time.

Managed service options: Ranging from self-managed to professionally managed services by Lumen.

A tightly integrated, converged experience

Lumen SASE with Fortinet represents the convergence of networking and security. Integrated with Lumen's highly connected world-wide backbone, are advanced, native security solutions: SD-WAN, NGFW, and ZTNA, designed to provide comprehensive cybersecurity protection for all users, devices, and applications, across all network edges. This advanced security is part of the Fortinet Security Fabric, which unifies management in a single pane of glass and performs at speeds for maximum throughput and efficiency. This convergence creates a scalable, flexible, optimized network and user experience. All of which can be fully and seamlessly managed.



Product Offerings

| Common Deployments | Small Retail/ Home Office | Branch/ SMB | Big Retail/ SMB | Medium Branch | Large Branch/ Campus |
|---|-------------------------------|-------------------------------|--------------------------------------|---|--|
| Appliances | 40F | 60F | 100F | 200F | 1800F |
| IPsec VPN Throughput¹ | 4.4 Gbps | 6.5 Gbps | 6.5 Gbps | 11.5 Gbps | 55 Gbps |
| Max IPsec Tunnels | 200 | 200 | 200 | 2,000 | 100,000 |
| Threat Protection² | 600 Mbps | 700 Mbps | 900 Mbps | 1 Gbps | 9.1 Gbps |
| Application Control Throughput³ | 990 Mbps | 1.8 Gbps | 1.8 Gbps | 2.2 Gbps | 17 Gbps |
| SSL Inspection Throughput | 310 Mbps | 630 Mbps | 715 Mbps | 1 Gbps | 23 Gbps |
| Unrestricted Bandwidth | ✓ | ✓ | ✓ | ✓ | ✓ |
| Zero Trust Network Access (ZTNA) | ✓ | ✓ | ✓ | ✓ | ✓ |
| SD-WAN | ✓ | ✓ | ✓ | ✓ | ✓ |
| Connectivity | | | | | |
| Interfaces | 5 x GE RJ45 | 10 x GE RJ45 | 8 x GE RJ45 2 x Shared Port Pairs | 18 x GE RJ45 8 x GE SFP 2 x 10 GE SFP+ 4 x Shared Port Pairs | 2 x GE RJ45 MGMT Ports 2 x 10 GE SFP+ / GE SFP HA Slots 16 x GE RJ45 Ports 8 x GE SFP Slots 12 x 25 SFP28 / 10 GE SFP+ / GE SFP Slots 4 x 40 GE QSFP+ Slots |
| Hardware Variants | WiFi, 3G4G | WiFi, Storage | WiFi, Bypass, POE, Storage | Storage | AC or DC, with or without Storage |
| 5G/LTE Connectivity | | | Supports FortiExtender | | Supports FortiExtender |
| Extensibility | Supports FortiAP, FortiSwitch | Supports FortiAP, FortiSwitch | Supports FortiAP, FortiSwitch | Supports FortiAP, FortiSwitch | |
| Form Factor | Desktop | Desktop | Desktop | 1RU | 2RU |
| Power Supply | Single AC PS | Single AC PS | Single AC PS, dual inputs | Dual AC PS | Dual PS (AC or DC) |

¹ The IPsec VPN performance test uses AES256-SHA256

² SSL Inspection performance values use an average of HTTPS sessions of different cipher suites ³ IPS, Application

³ Control, NGFW, and Threat Protection are measured with logging enabled

Benefits: Improve, Advance, Simplify, and Secure

- **Enhance performance**
Minimize latency and maximize efficiencies from edge computing and the convergence of networking and security. Plus, enable a consistent security and user experience across all edges.
- **Advance security**
High performance, always-on threat protection. Secure all applications, users, and data virtually anywhere with a next-generation firewall that combines SD-WAN and security capabilities in a unified solution.
- **Simplify operations**
With centralized management, deployment, and automation, companies can save time and respond quickly to connectivity and security issues with orchestration, analytics, and end-to-end visibility.
- **Secure work-from-anywhere**
Provide tightly integrated, zero-touch networking and security solutions to each device and application with full IT control and visibility.

The Lumen-Fortinet Advantage

Lumen, operating one of the most highly peered IP backbones in the world, offers high density edge points of presence in major metros across the globe. This provides more onramps to cloud-based services, web, and SaaS applications employees need to access from anywhere. Fortinet is the only SASE vendor to provide consistent security posture with enterprise-grade protection across every edge and User, powered by 20+ years of organic innovations with FortiOS and FortiGuard AI-powered security services. Fortinet's global leadership and innovation is among the [most validated](#) in the industry by Gartner, IDC, Forrester, and Frost & Sullivan; and through our collaboration with global alliances.

GLOBAL LEADERSHIP AND COLLABORATION



Together, Lumen and Fortinet deliver a fully integrated network and security solution – from the core, to the cloud to the edge – supporting the dynamic, high performance, and secure access needs of modern hybrid organizations.