SASE, powered by Fortinet

Scalable, cloud-delivered security and networking for a hybrid workforce

A hybrid workforce has become the new reality for most organizations. This has created new challenges by expanding the attack surface while making it more challenging to secure remote users. The growing number of new network edges and remote users, often implemented as discrete projects, leave gaps in security that cybercriminals are all too anxious to exploit. At the same time, organizations with large numbers of remote offices and a hybrid workforce often struggle to ensure that security policies are being applied and enforced consistently for users both on and off the network while delivering superior user experience to everyone.

Highlights

FortiOS

Fortinet's unified operating system, FortiOS, is the culmination of over 20 years of industry leading innovation. It powers our unique security-driven approach to seamlessly converge networking and security from the cloud.

FortiGuard AI-powered security services

AI-powered security services, applied across application, content, web traffic, devices and users, provide automated and consistent protection against the latest attacks while ensuring rapid, real-time detection and response.

Cloud-based management

Simple, cloud-based management provides centralized visibility and control across distributed users and applications—all backed by industry-leading SLAs.

Key business outcomes

Consistent security posture everywhere
Overcome security gaps and minimize your attack surface with consistent security posture powered by the same FortiOS.

Superior user experience
With intelligent application steering and dynamic routing, our SD-WAN capabilities deliver a superior user experience.

Operational efficiency
Simplify operations with cloud-delivered management combined with enhanced security and networking analytics.

Shift to an OPEX business model
Efficient user-based license model allows organizations to shift from upfront capital investments.

Key use cases

Secure Internet access
For remote users or branch locations no longer protected by the corporate perimeter, direct Internet access expands the attack surface and related risks. SASE offers comprehensive secure web gateway (SWG) and firewall as a service (FWaaS) capabilities for both managed and unmanaged devices by supporting an agent and agentless approach.

Secure private access
Traditional VPNs cannot address the challenges faced by today's hybrid workforce. Because they do not inspect connections, they inadvertently expand the attack surface and increase the risk of lateral threat movement. SASE secure private access offers the industry's most flexible secure connectivity to corporate applications. Organizations can enforce granular access to applications with universal ZTNA, enabling explicit per-application access and enabling the critical shift from implicit to explicit trust. SASE secure private access also offers organizations the benefits of seamless integration with SD-WAN networks and access to corporate applications by automatically finding the shortest path—powered by the intelligent steering and dynamic routing capabilities available in SASE.

Secure SaaS access
With the rapid increase in SaaS adoption, many organizations struggle with shadow IT challenges and stopping data exfiltration. SASE secure SaaS access, with next-generation dual-mode CASB, using both in-line and API-based support, provides comprehensive visibility by identifying key SaaS applications and reporting risky applications. CASB also offers granular control of applications to secure sensitive data and detect and remediate malware in applications across both managed and unmanaged devices.

Security as a service

Secure Web Gateway (SWG)

Protects against the most advanced web threats with a broad set of capabilities for securing all web traffic, including encrypted. SWG enables a defense-in-depth strategy with web filtering, anti-virus, file filtering, DLP (data loss prevention) and more.

Firewall as a Service (FWaaS)

Leveraging the independently certified and acclaimed capabilities of FortiOS, our FWaaS technology enables high-performance SSL inspection and advanced threat detection techniques from the cloud. It also establishes and maintains secure connections and analyzes in-bound and out-bound traffic without impacting user experience.

Universal ZTNA

Applying ZTNA everywhere for all users and devices, regardless of location, shifts implicit access to explicit control. Granular controls, applied per application, combine user authentication, continuous identity and context validation and monitoring.

Next-generation dual-mode CASB

With both inline and API-based support, next-gen CASB identifies key SaaS applications and reports shadow IT applications, provides secure access to sanctioned SaaS applications, restricts access to SaaS apps to trusted endpoints and enables ZTNA posture checks for application access.

Networking as a service

Software-Defined WAN (SD-WAN)

Fortinet's cloud-delivered SD-WAN capabilities include application steering and dynamic routing to help identify the shortest path to corporate applications.

Application visibility + control

FortiSASE includes over 5,000 application signatures, first packet identification, deep packet inspection, custom application signatures, SSL decryption and TLS1.3 with mandated ciphers to ensure and maintain visibility and control over applications.

Expanding SASE to secure all users, edges + devices

Fortinet SASE is becoming the industry's most comprehensive SASE offering–securing users, access, edges, and devices anywhere while delivering the highest ROI, consistent security posture and improved user experience. Powered by Fortinet's unique security and networking convergence approach, it offers organizations a simple networking journey towards SASE.

SASE's new innovations enhance the cutting-edge AI-powered solution specifically designed for the hybrid workforce, the power of cloud delivery, unified management and logging, with comprehensive features, such as universal ZTNA, SD-WAN integration, OT/IoT security, LAN/WLAN/5G security, digital experience monitoring and a flexible licensing model. The new Fortinet SASE solution ensures the utmost security for all edges, devices and users, whether they are accessing the web, corporate or SaaS applications.

The Fortinet advantage

Rather than providing an isolated, cloud-only approach, SASE functions as an extension of the Fortinet Security Fabric, extending and leveraging the power of FortiOS—the operating system that unifies the entire portfolio of Fortinet security solutions. The following benefits include:

Consistent security + superior user experience
Comprehensive cloud-delivered security and networking combined with universal ZTNA for users anywhere.

One unified agent
Our unified agent supports multiple use cases. FortiClient can be used for ZTNA, traffic redirection to SASE, CASB, and endpoint protection without the multiple agents for each use case other solutions require.

Features list

	Features	Description
Secure SD-WAN	Application identification + control	Granular application policies, application SLA-based path selection, dynamic bandwidth measurement of SD-WAN paths, active/active and active/standby forwarding, overlay support for encrypted transport, application session-based steering and probe-based SLA measurements. More than 8,000 applications are controlled, including industrial control signatures.
	Advanced routing	Supported routing options include application-aware routing, static routing, internal gateway (iBGP, OSPF v2/v3, RIP v2), external gateway (eBGP), VRF, route redistribution, route leaking, BGP confederation, router reflectors, summarization and route aggregation and route asymmetry.
	Network + security convergence	The industry's only purpose-built and ASIC-powered SD-WAN that enables thin edge and WAN edge to secure all applications, users and data in branch offices. Integrating with SASE enables consistent robust security for users everywhere.
	Secure private access	Securely connect remote users to private applications by establishing IPSec tunnels from SASE PoP to multiple SD-WAN hubs.
Cloud-delivered security	API-CASB	Directly connected to leading SaaS providers to access usage and data stored in the cloud. This enables administrators the ability to scan provisioned cloud resource configurations for potential threats, as well as SaaS application data for threats, proprietary information or sensitive customer records. This ensures that all users of the organization's SaaS applications are monitored and protected no matter where they are or what device they are on.
	In-line CASB	Protects data in motion and data at rest for cloud applications, creates shadow IT report, performs risk assessment and expands visibility into risk trends and events.
	FWaaS	Powered by FortiOS, the SASE FWaaS is a cloud-based service that provides hyperscale, next-generation firewall (NGFW) capabilities, including web filtering, advanced threat protection (ATP), intrusion prevention system (IPS) and domain name system (DNS) security.
	SWG	FortiSASE SWG relies on FortiOS explicit web proxy, captive portal and authentication features to secure customers' web traffic.
	ZTNA	ZTNA is a capability within zero trust access (ZTA) that controls access to applications. It extends the principles of ZTA to verify users and devices before every application session. ZTNA confirms that they meet the organization's policy to access that application.

Features list

	Features	Description
Advanced threat detection	Antivirus (AV)	FortiSASE Antivirus delivers automated updates that protect against the latest polymorphic attacks, viruses, spyware and other content-level threats. Based on patented content pattern recognition language (CPRL), the antivirus engine is designed to prevent known and previously unknown virus variants, providing 1.8M new AV definitions every week.
	Antispam	FortiGuard antispam provides a comprehensive and multi-layered approach to detect and filter spam processed by organizations. Dual-pass detection technology can dramatically reduce spam volume at the perimeter, giving you unmatched control of email attacks and infections.
	Application control	SASE can recognize network traffic generated by well-known applications, as well as custom applications. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. Quickly create policies to allow, deny or restrict access to applications or entire categories of applications.
	Data leak prevention	DLP allows businesses to identify sensitive information across multiple cloud-based systems, prevent the accidental sharing of data and monitor and protect data. Offers predefined reports for standards, including SOX, GDPR, PCI, HIPAA, NIST and ISO27001 to provide organizations visibility into policy violations so they can be tracked and remediated.
	DNS filtering	DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains (NRDs) and parked domains. It protects against sophisticated DNS-based threats, such as DNS over TLS (DoT), DNS over HTTPS (DoH), DNS flood protection, DNS tunneling, DNS infiltration, C2 server identification and domain generation algorithms (DGAs).
	Intrusion prevention (IPS)	The AI/ML-powered IPS service provides near real-time intelligence with thousands of intrusion prevention rules to detect and block known and suspicious threats before they reach your devices.
	Next generation AI-powered sandbox	AI/machine learning technology identifies and isolates advanced threats in real time. Files, websites, URLs and network traffic are inspected for malicious activity, including zero-day threats. Sandboxing technology is used to analyze suspicious files in a secure virtual environment.
	SSL inspection/ decryption	Using deep inspection, FortiSASE impersonates the recipient of the originating SSL session then decrypts and inspects the content to find and block threats. The content gets re-encrypted and sent to the real recipient. Deep inspection not only protects you from attacks that use HTTPS, but it also protects you from other commonly used SSL-encrypted protocols like SMTPS, POP3S, IMAPS and FTPS.
	Web filtering	Web filtering leverages a database of hundreds of millions of URLs classified into 90+ categories to enhance granular web controls and reporting. TLS 1.3 support extends analysis to encrypted traffic. It also blocks unknown malicious URLs almost immediately. Cloud-enabled technology provides complete protection to web threats, AI-driven detection, analysis and enforcement for real-time protection against known and unknown threats.
	Outbreak alerts	Receive communication and comprehensive details on the latest cybersecurity attacks, including the timeline, impacted technology and where applicable patches/mitigation recommendations can be found.

	Features	Description
Connectivity	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.
	Agentless connectivity	Agentless security is available for BYOD devices or devices where an agent cannot be downloaded (e.g., Chromebooks) with the use of PAC files.
	Endpoint protection	Fortinet's FortiClient offers security, compliance and authorized access controls in a single client. FortiClient gives you endpoint protection software that runs directly on an endpoint, such as a smartphone or tablet. FortiClient then connects to the Fortinet security fabric and feeds the devices to the rest of your system. This provides you with endpoint security information, visibility and the ability to control who and what accesses each device. SASE supports management and integration of a FortiExtender configured as a LAN extension. By relying on FortiExtender instead of FortiClient to handle secure connectivity to FortiSASE, this solution essentially extends the single-user, single-device FortiClient endpoint case to a multiuser, multidevice LAN environment.
	Thin edge	Secure WLAN/LAN products integrate with the Fortinet single-vendor SASE solution. This enables secure micro-branches where LAN solutions are deployed to send traffic to a FortiSASE solution and ensure comprehensive security of all devices at the site with a single management console.
	Secure edge	SASE lets you choose to perform security with your local FortiGate or connect branch offices to FortiSASE for security inspection in the cloud through FortiGate NGFW and Fortinet secure SD-WAN.
	API connectivity	SASE integrates seamlessly with FortiAnalyzer (analytics), FortiMonitor (DEM), FortiSIEM (threat detection). Open REST APIs are available to be leveraged and used for inbound integrations.
	Authentication	Support for native FortiTrust ID and SAML-based authentication is available, as well as seamless integration with 3rd party identity providers, such as Microsoft Entra ID and Okta.
	Dedicated IPS support	With an additional license, FortiSASE can support dedicated public IPs for customers, enabling IP reputation and geo-location services with source IP anchoring.
AI-powered services	Fortiguard security services	SASE provides botnet-protection by default and all the security services like AV, IPS, web filtering and DLP are enabled by the FortiGuard AI/ML powered security. Signature updates and definitions are updated in near real time.

	Features	Description
Monitoring + management	Single console	With the SASE Console, administrators gain a centralized management platform for a single dashboard for all-in-one configuration and visibility for all use cases (web, private and SaaS security). Through a single pane of glass, administrators can efficiently deploy and manage security services, monitor network performance and analyze security events. Actionable insights and customizable reports enable informed decision-making and continuous optimization of security and networking strategies.
	Reporting + analytics	You can generate data reports from logs by using the Reports feature. You can configure FortiSASE to regularly run reports at scheduled intervals and manually run reports when desired. Logging and monitoring are also useful components to help you understand what is happening on your network and to inform you about network activities, such as a virus detection, visit to an invalid website, intrusion, failed login attempt and others.

Our managed connectivity, communications and security solutions are innovative. Your business outcomes are imperative.

To learn more about Windstream Enterprise, visit windstreamenterprise.com

WINDSTREAM ENTERPRISE