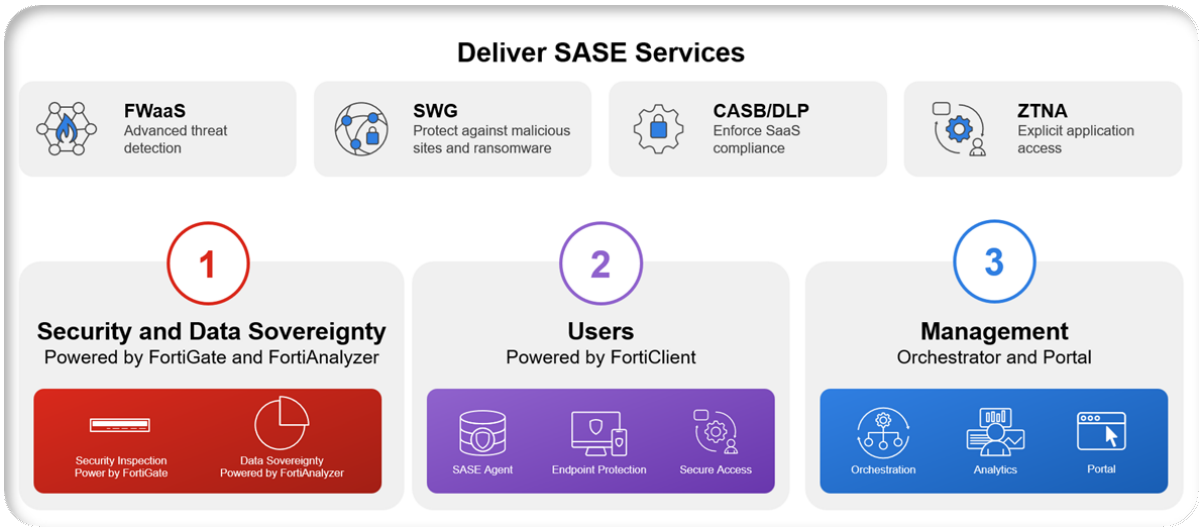
FortiSASE Sovereign



Highlights

- Turnkey private SASE—ready to deploy
- Fast rollout, zero complexity
- Full control of data, infrastructure, and policy
- Built-in sovereignty and compliance
- Complete, single-vendor SASE stack
- Simple, flexible purchasing

Seamlessly Deliver Your Own SASE Service with Full Data Compliance

Data sovereignty ensures that digital data is governed by the laws of the country or region where it is collected, processed, or stored. As a result, organizations must comply with local regulations on data residency, privacy, and security—keeping sensitive information within legally defined jurisdictions.

This scenario is especially critical for highly regulated industries, including finance, healthcare, and government, as well for as multinational organizations managing complex global compliance requirements.

Fortinet elevates SASE innovation with FortiSASE Sovereign—an industry-first turnkey solution that enables service providers, large enterprises, and governments to build their own private SASE cloud. Designed for highly regulated environments, it lets organizations deliver customized SASE services to customers or employees while maintaining full control over data, infrastructure, and operations.

With FortiSASE Sovereign, organizations can ensure compliance, strengthen security, and improve operational efficiency—all while maintaining full autonomy over architecture and feature sets. This flexibility enables them to create tailored, differentiated service offerings that precisely meet diverse regulatory and business needs.

Key business outcomes

Rapid time-to-value

Turnkey private SASE cloud solution with prepackaged components enables seamless deployment, reducing complexity and accelerating implementation.

Operational autonomy and agility

Full customer control over service features and architecture enables tailored security and networking to meet unique business needs. A hybrid design that separates data control (customer premises) from orchestration (Fortinet network) lowers costs and accelerates go-to-market strategies.

Enterprise-grade sase security and scalability

A full suite of best-of-breed SASE features combined with multi-tenant management delivers comprehensive protection and efficient operations across distributed environments.

Simple consumption models

Simple purchasing options enable organizations to align security investments with performance and budgetary requirements

Highlights

Turnkey SASE Solution with Seamless Deployment

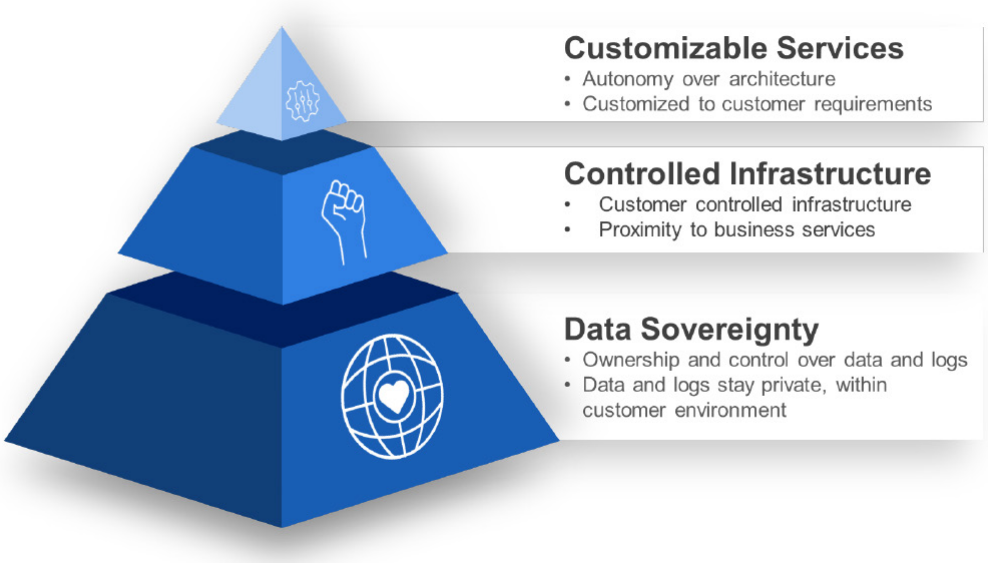
FortiSASE Sovereign delivers a fully operational, out-of-the-box platform with a complete SASE stack—including SWG, FWaaS, ZTNA, and CASB. Purpose-built for rapid rollout, it combines flexible packaging with a streamlined architecture that keeps data and core security functions on-premises, while leveraging Fortinet-hosted orchestration and management. The result is faster deployment, reduced complexity, and predictable performance—without compromising control.

Full Autonomy and Control

FortiSASE Sovereign provides complete operational control over deployment locations, SASE features, and security infrastructure, enabling organizations to manage their environments with confidence and maintain full visibility. It supports customizable security and network policies that align with local regulations and unique business needs, enhancing compliance and efficiency. Service providers can create tailored offerings for different market segments, delivering maximum flexibility to meet diverse customer requirements while maintaining security and control.

Data Sovereignty and Compliance

FortiSASE Sovereign ensures compliance with regional data residency and sovereignty laws by keeping sensitive data within designated jurisdictions. It provides organizations with full control over their data and logs, ensuring they remain private within their own environment. It gives organizations all the tools they need to build a fully compliant SASE solution.



Key use cases

Custom SASE offerings

Service providers can create tailored SASE packages for different sectors, ensuring data sovereignty, security, and service options.

Localized data control

FortiSASE Sovereign enables global organizations to keep security processing and sensitive customer data within designated jurisdictions.

Regulatory compliance

Governments ensure that all security processing and data remain within national boundaries to comply with regional regulations.

A solution built for data sovereignty

FortiSASE Sovereign ensures compliance with stringent data residency and sovereignty laws by keeping sensitive data within designated jurisdictions. Service providers and organizations retain full control over their data storage and logs, preserving privacy within their own environments. This level of control is essential for regulated industries that must meet strict compliance requirements while maintaining operational efficiency.

Designed as a turnkey solution, Fortinet Sovereign SASE simplifies deployment with pre-integrated components for rapid setup, configuration, and multitenancy management. Service providers can create flexible service offerings with scalable threat performance options based on user count. Its hybrid architecture enables on-premises data control while leveraging cloud-based orchestration for fast, cost-effective deployment.

With full autonomy and control, service providers can independently manage their infrastructures, deployment locations, and security policies for each customer to align with local regulations and unique business needs. This operational independence ensures optimized security, performance, and compliance without relying on third-party management. Customizable policies enable providers to offer tailored services that address diverse customer requirements across market segments.

The Fortinet Advantage

Fortinet is the only vendor offering a turnkey, easily deployable SASE solution that provides full autonomy and control over services and architecture, ensuring unparalleled flexibility, security, and compliance. Fortinet's key advantages include:

- Turnkey private SASE with prepackaged components for seamless deployment
- Full customer control of service features and architecture
- Flexible purchasing options tailored to diverse security and performance needs
- Comprehensive set of best-of-breed SASE features and multitenant management

Features



FIREWALL	
Next-generation firewalls	Powered by FortiOS, FortiGate Next-Generation Firewalls (NGFWs) deliver hyperscale NGFW capabilities, including web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and Domain Name System (DNS) security.
FortiGate-as-a-service	(Optional) FortiGate-as-a-Service (FGaaS) is the industry's first Hardware-as-a-Service option that combines the power of our proprietary ASIC technology with the flexibility and scalability of cloud services. This service can be used with Sovereign SASE to leverage Fortinet resources for security inspection.
SSE CAPABILITIES	
Secure web gateway	Fortinet Sovereign SASE secure web gateway (SWG) uses the FortiOS explicit web proxy, captive portal, and authentication features to secure customers' web traffic.



Universal ZTNA	Zero-trust network access (ZTNA) is a capability within zero-trust access (ZTA) that controls access to applications. It extends ZTA principles to verify users and devices before each application session. ZTNA confirms that users and devices meet the organization's policy for accessing that application. The ZTNA EMS server is located in Fortinet's points of presence (POPs).
Inline CASB	Inline CASB protects data in motion and at rest for cloud applications, creates shadow IT reports, performs risk assessment, and expands visibility into risk trends and events.



Data leak prevention	Data leak prevention (DLP) allows businesses to identify sensitive information across multiple cloud-based systems, prevent accidental data sharing, and monitor and protect data. It offers predefined reports for standards including SOX, GDPR, PCI, HIPAA, NIST, and ISO27001 to provide organizations with visibility into policy violations so they can be tracked and remediated.
AI-POWERED SERVICES	
Fortiguard AI-powered security services	Fortinet Sovereign SASE provides botnet protection by default, and all security services, such as AV, IPS, web filtering, and DLP, are enabled through FortiGuard AI/ML-powered security. All signature updates and definitions are delivered in near real time. Fortinet has a massive customer base of 900,000+ customers. FortiGuard Labs leverages intelligence from this install base, which allows us to propagate any new zero-day threat signatures to all customers in real time.



SPA	
Secure private access	Secure private access (SPA) securely connects remote users to private applications by establishing IPsec tunnels from your private SASE POP to multiple SD-WAN hubs.









ADVANCED THREAT DETECTION	
Antivirus	Fortinet Sovereign SASE antivirus (AV) delivers automated updates that protect against the latest polymorphic attacks, viruses, spyware, and other content-level threats. Based on the patented content pattern recognition language (CPRL), the antivirus engine is designed to prevent known and previously unknown virus variants providing 1.8 million new AV definitions every week.
Antispam	FortiGuard antispam provides a comprehensive, multilayered approach to detecting and filtering spam processed by organizations. Dual-pass detection technology can dramatically reduce spam volume at the perimeter, giving you unmatched control over email attacks and infections.
Application control	Fortinet Sovereign SASE can recognize network traffic from well-known applications as well as custom applications. Application control uses IPS protocol decoders to analyze network traffic and detect application traffic, even when traffic uses non-standard ports or protocols. Quickly create policies to allow, deny, or restrict access to applications or entire application categories.
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 including DNS over TLS (DoT), DNS over HTTPS (DoH), DNS flood protection, DNS tunneling, DNS infiltration, C2 server identification, and DGAs (Domain Generation Algorithms).
Intrusion prevention	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, using deep packet inspection of network traffic. The service is augmented by our in-house research team.
Sandboxing	Sandboxing utilizes AI and ML to identify and isolate advanced threats in real time. It inspects files, websites, URLs, and network traffic for malicious activity, including zero-day threats, and analyzes suspicious files in a secure virtual environment.
SSL inspection/decryption	Using deep inspection, Fortinet Sovereign SASE impersonates the recipient of the originating SSL session, then decrypts and inspects the content to detect and block threats. It then re-encrypts the content and forwards it to the real recipient. Deep inspection not only protects you from attacks that use HTTPS but also protects you from other commonly used SSL-encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.
Web filtering	Web filtering uses 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, it provides complete protection against web-borne threats, with AI-driven detection, analysis, and enforcement for real-time protection against known and unknown threats.



CONNECTIVITY	
Unified agent	A single unified agent supports multiple use cases. The FortiClient agent can be used for ZTNA, traffic redirection to SASE, and endpoint protection, without requiring separate agents for each use case. Support is available for a wide range of OS, including Windows, macOS, Linux, Android, and iOS.
Endpoint protection	The FortiClient offers security, compliance, and authorized access controls in a single client. FortiClient provides 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 device data to the rest of your system. This approach provides you with endpoint security information, visibility, and the ability to control who and what can access each device.
Authentication	Support for SAML-based authentication and seamless integration with third-party identity providers such as Microsoft Entra ID and Okta is available, along with support for native FortiTrust ID. Support is also available for local, LDAP, and RADIUS.
MONITORING AND MANAGEMENT	
Single console	With the Sovereign SASE console, administrators gain a centralized management platform with a single dashboard for all-in-one configuration and visibility across all use cases (web, private, and SaaS security). Through a single pane of glass, they 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. The Sovereign SASE console is hosted in Fortinet POPs.
Global server load balancing (GSLB)	FortiAppSec Cloud GSLB Service is a DNS-based service designed to guarantee business continuity by keeping applications online and available, even in the face of localized application issues. Using custom health checks, the GSLB service monitors application endpoints or cloud services. It aims to optimize the availability, user experience, and security of enterprise applications.
Orchestrator	The Fortinet Sovereign SASE orchestrator is key to the solution. It is hosted in Fortinet POPs and provides configuration synchronization, health checks and resource management, security posture checks, external IP synchronization with GSLB, and communication via the FortiGate Cloud tunnel.
MSSP portal	The portal provides centralized, multitenant management and configuration, enabling managed security service providers (MSSPs) to efficiently deploy and manage SASE services across their client bases. From a single pane of glass, MSSPs can configure security policies, network settings, and user access, ensuring consistent, unified security across multiple client environments.
Reporting and analytics	You can generate data reports from logs using the Reports feature. You can configure FortiSASE to regularly run reports at scheduled intervals, send them as email attachments to select recipients, and manually run reports when desired. Logging and monitoring are also useful for understanding what is happening on your network and for informing you about network activities, such as virus detections, visits to invalid websites, intrusions, failed login attempts, and more.

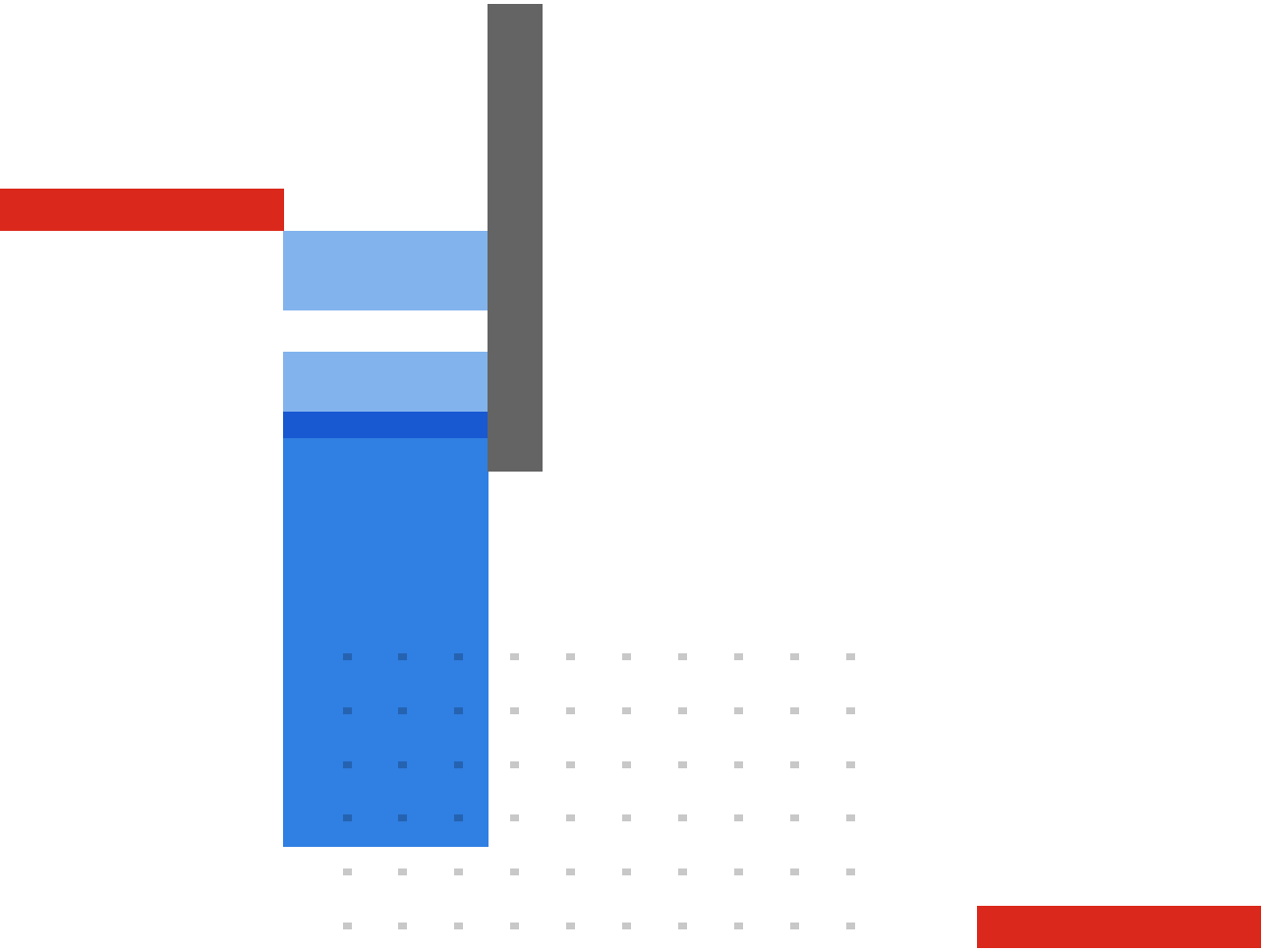




See the FortiSASE Sovereign Ordering Guide for full details on components and SKUs for purchase
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-sovereign-sase.pdf

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Copyright © 2026 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 SVP Legal and above, 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.

June 9, 2026

FSS-DAT-R02-20260609