SOLUTION BRIEF

FortiSASE: Secure SaaS Access with Comprehensive Visibility and Control

Executive Summary

The hybrid workforce has become a reality for most businesses, yet it creates new headaches by expanding the organization's attack surface. This presents a challenge for cybersecurity and IT teams as they work to secure these remote users. One struggle is ensuring that security policies are being applied and enforced consistently for users that are both on and off the corporate network. Secure access service edge (SASE) architecture helps extend secure access and high-performance connectivity to users regardless of their geographic location.

FortiSASE offers a full set of networking and security capabilities, including secure web gateway (SWG), universal zero-trust network access (ZTNA), next-generation dual-mode cloud access security broker (CASB), Firewall-as-a-Service (FWaaS), and Secure SD-WAN.

Powered by FortiOS, FortiGuard AI-powered security services, and a unified agent, FortiSASE drives operational efficiency and delivers consistent security everywhere. FortiSASE enables three key use cases:

1. Secure internet access: Securing all user traffic to and from the internet
2. Secure private access: Secure and reliable access to privately hosted applications
3. Secure SaaS access: Comprehensive visibility and control for SaaS applications

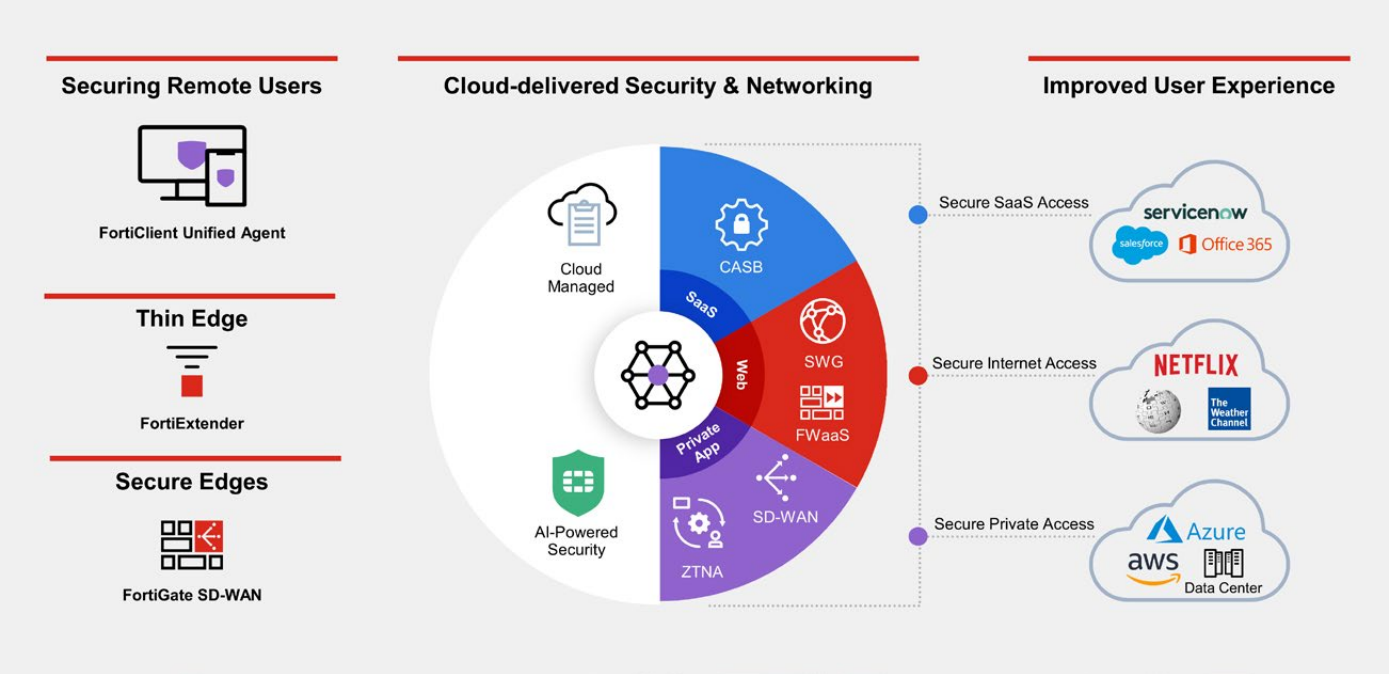

Figure 1: Consistent security at every edge, powered by FortiOS

FortiSASE: Simple, Seamless, and Scalable Cloud-Delivered Security

FortiSASE empowers organizations to enable secure access to the web, cloud, and applications anywhere while delivering enterprise-grade security and superior user experience. The FortiSASE solution enables secure SaaS access with support for inline and API-based CASB capabilities. These capabilities are powered by the FortiGuard CASB Service to provide comprehensive visibility, control, and security to SaaS applications.

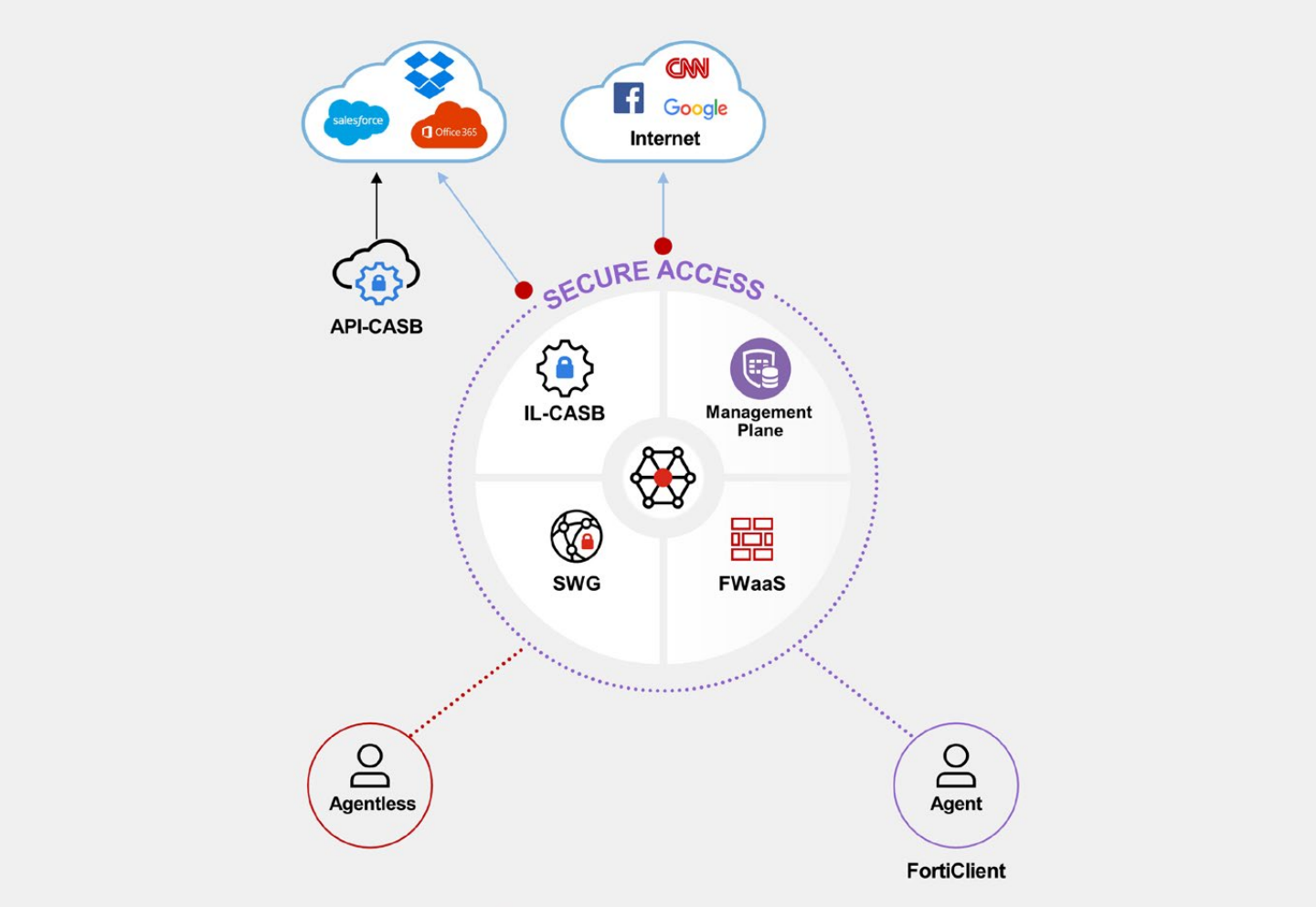

Figure 2: Secure SaaS access for managed and unmanaged devices

Why Organizations Choose FortiSASE

Cybercriminals will continue to find clever ways to infiltrate an enterprise's ever-expanding attack surface. That's why organizations need a solution capable of following, enabling, and protecting users no matter where they—or the applications they use—are located. FortiSASE provides more than an encrypted tunnel to address today's advanced threats. It includes a portfolio of enterprise-grade security solutions designed to inspect traffic and detect and respond to known and unknown threats.

FortiSASE also integrates endpoint and network security, providing seamless visibility and control across and between all endpoints, enforcing conditional access policies, and delivering an automated threat response. It provides end-to-end visibility for both hosts and endpoint devices to help organizations harden endpoints and enhance their security posture. Specifically, the Fortinet endpoint security agent, FortiClient, simplifies endpoint management by centralizing key security tasks, identifying vulnerabilities, and correlating events to improve incident reporting.

FortiSASE secures SaaS access and enables:

- **Cloud application visibility:** Discover cloud applications usage across all sanctioned and unsanctioned (shadow IT) cloud applications to help enforce policy-based controls
- **Data security:** Protect data in motion and at rest within cloud applications. Control productivity, privacy, compliance, and security of corporate and non-corporate tenants
- **Assess risk:** Evaluate application usage spikes to determine risk and ensure corporate data is handled safely

FortiSASE Secure SaaS Access Features

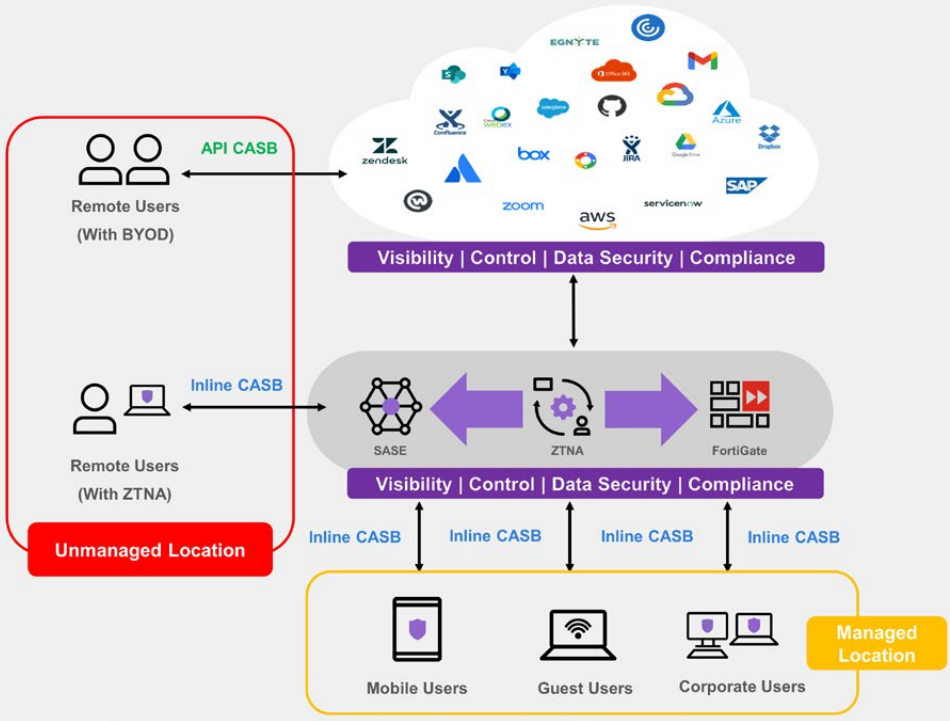

Figure 3: Comprehensive security services for secure SaaS access

API-CASB

The cloud-native CASB service provides visibility, compliance, data security, and threat protection for cloud applications. Using direct API access, it enables deep inspection and policy management for data stored in SaaS and Infrastructure-as-a-Service (IaaS) applications. It also provides advanced tools that provide detailed user analytics and centralized management to ensure policies are enforced and your organization's data isn't getting into the wrong hands. It supports:

- Agentless deployment
- Integration with applications using API connector
- Visibility for bring-your-own-device (BYOD) and unmanaged locations/devices
- Data at rest scanned with the CASB engine

Inline CASB

Inline CASB recognizes network traffic generated by many applications. Application control with inline CASB using IPS protocol decoders can analyze network traffic to detect application traffic, even if the traffic uses nonstandard ports or protocols. Application control with inline CASB supports traffic detection using the HTTP protocol (versions 1.0, 1.1, and 2.0). By providing access control to SaaS applications, you can leverage application control and SSL deep inspection to act as an inline CASB. Traffic between users and the cloud service is inspected by inline CASB to enforce security policies as they access cloud-based resources. Deeper control of SaaS application behavior can also be enabled by HTTP header insertion capabilities along with web filtering. It supports:

- Control over managed and unmanaged locations
- Posture assessment, visibility, and protection for cloud applications based on agent
- Data in motion scanned with the CASB engine

Managed Location	When managed users are at the office and trying to access SaaS applications, the user request is traversed through the gateway, where the gateway applies the right cloud security policy for accessing the application using the inline CASB. Guest users are also given access to the cloud application with the help of explicit proxy settings using the inline CASB.
Unmanaged Location	When users are working from any location other than a managed location—like home, airport, hotels, or anywhere—both the inline and API CASB can be leveraged to secure SaaS applications.
Managed User	Organizations with agent-based deployment (FortiClient) can leverage inline CASB to secure SaaS access.
Unmanaged User	Organizations with a BYOD policy or where there is a need to secure guest user access can leverage API CASB to secure SaaS access.

Achieve Better Business Outcomes with FortiSASE

FortiSASE meets the need for consistent networking and security from any location—ultimately delivering enhanced user experiences and better business outcomes. Wherever your organization is on its digital acceleration journey, the Fortinet goal is to help unify security under one vendor, with one client and one operating system to reduce complexity, increase security effectiveness, and ensure a reliable user experience across today's expanding networks.

FortiSASE enables hybrid and cloud-delivered cybersecurity for the remote workforce for any organization worldwide.

March 23, 2023 3:30 PM
1990950-0-0-EN