

# FortiSASE: Securing Corporate Application Access for the Hybrid Workforce

## Executive Summary

The recent rapid transition to a hybrid workforce created new headaches for IT teams by expanding—and even inverting—the organization’s attack surface. With more users and devices accessing critical resources from outside the traditional network than ever, security and IT teams have had to scramble to secure them. Beyond providing reliable access, one critical struggle has been ensuring that security policies are being applied and enforced consistently whether users are on or off the corporate network.

One of the latest and most effective tools designed to address this challenge is the Secure Access Service Edge (SASE) architecture. The FortiSASE architecture quickly extends secure access and high-performance connectivity to users regardless of their geographic location or application type. And because FortiSASE is tied into the Fortinet Security Fabric strategy, it empowers organizations to provide consistent, secure access to the web, cloud, enterprise network, and business-critical applications deployed anywhere—all while delivering enterprise-grade security and optimal user experience. What’s more, FortiSASE’s secure private-access strategy also helps organizations shift from a CapEx to an OpEx business model, enabling them to also address many of the costs associated with this transition.

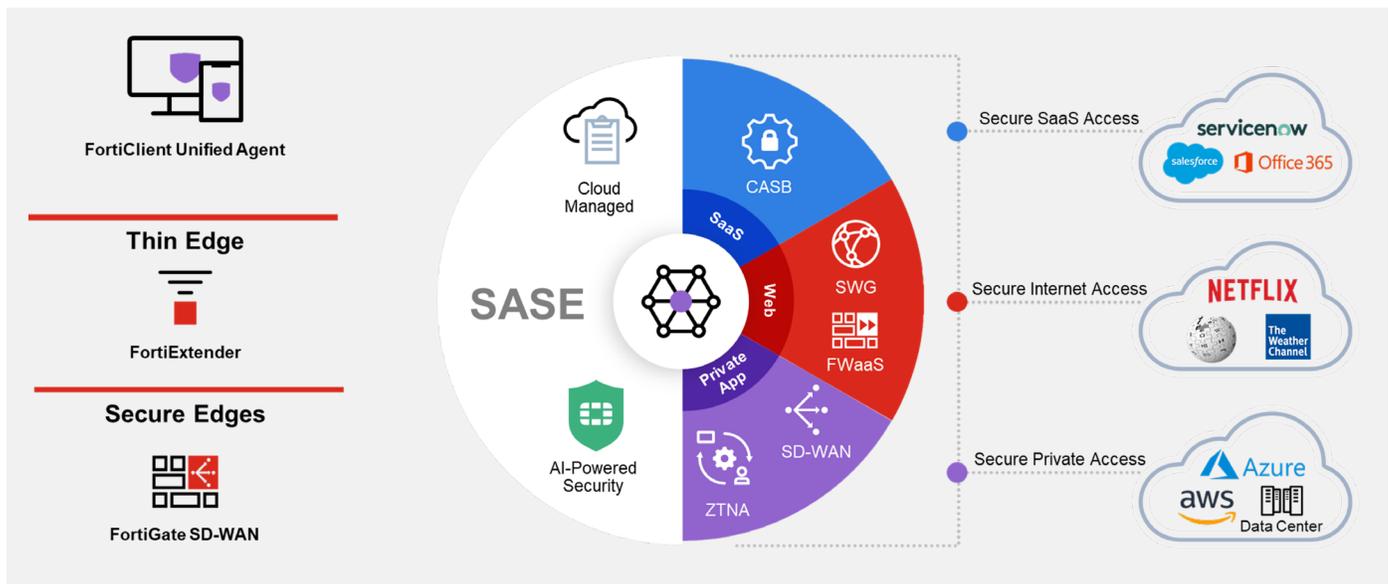


Figure 1: Consistent security at every edge, powered by FortiOS

## FortiSASE: Seamless cloud-delivered security and superior user experience for corporate apps

FortiSASE offers simple, cloud-based management with a self-service design, easy user onboarding, and a flexible, tiered, and user-based licensing model.

Today’s workforce is mobile and dynamic. To remain competitive, organizations must ensure that these workers have access to corporate applications and data from anywhere. FortiSASE’s Secure Private Access (SPA) capability provides secure and reliable access to your corporate applications. Connectivity can be securely enabled using existing Fortinet ZTNA, SD-WAN, and NGFW deployments.

For example, FortiSASE SPA enables security teams to selectively enable both apps and users at a granular level with tighter ZTNA posture access without impacting any other connectivity. And when paired with an SD-WAN network, FortiSASE automatically finds the shortest path to each application by dynamically connecting directly to the SD-WAN spoke hosting the application—ensuring the highest level of performance. Administrators can also configure granular rules from the FortiSASE portal to grant application access to specific users, groups, or device posture tags.

In addition to its seamless integration with FortiGate NGFW devices, FortiSASE also supports Fortinet’s Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), and Cloud Access Security Broker (CASB) functionalities—all enhanced with continuous threat intelligence updates from FortiGuard Labs. Powered by the FortiOS operating system, FortiSASE FWaaS has all the same features, security, and reliability customers depend on from FortiGate Next-Generation Firewalls (NGFWs). When working together as a unified Security Fabric meshed platform, these threat protection capabilities enable secure internet and SaaS application access from any user, device, or location to applications or resources deployed anywhere.

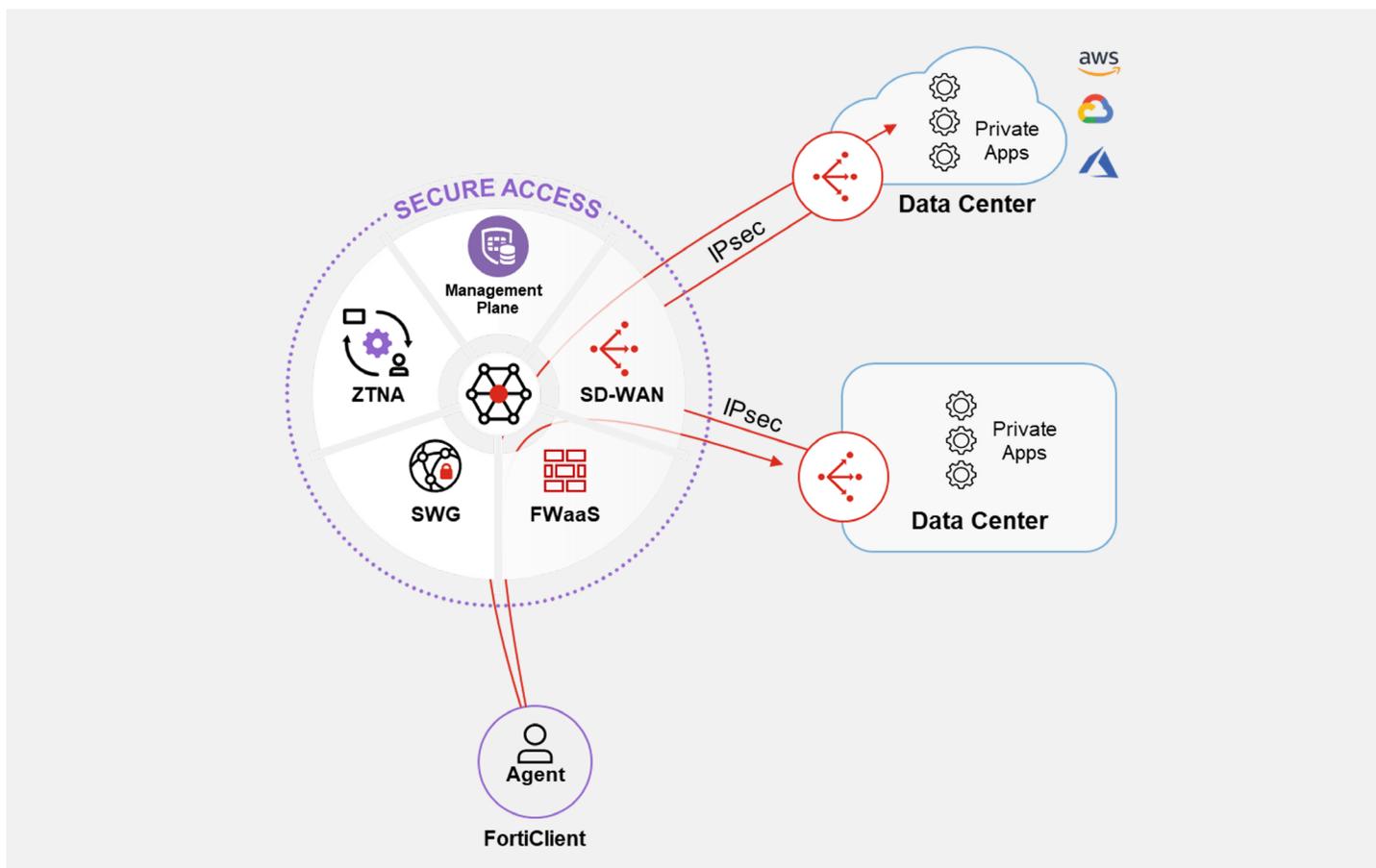


Figure 2: Secure private access for the hybrid workforce

### Why organizations choose FortiSASE for SPA

With more remote users than ever needing access to applications deployed in your private data centers, the risk of compromise and lateral threat movement has grown exponentially. FortiSASE SPA enables broad and seamless access to every private application, such as payroll apps, deployed in private data centers or public cloud environments. It starts by automatically finding the shortest path to each application, including VoIP and other Unified Communications applications, enabling a superior user experience without requiring infrastructure upgrades. This also helps ensure secure access to private applications for remote users leveraging your existing SD-WAN/NGFW investments.

FortiSASE regularly increases its SD-WAN hub connectivity coverage and simplifies hub configurations through its SASE interface to cater to larger enterprises deploying Secure SD-WAN architectures globally.



FortiSASE also integrates endpoint and network security, providing seamless visibility and control across and between all endpoints. The integration can enforce conditional access policies and deliver automated threat responses. It also provides end-to-end visibility for 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 critical security tasks, identifying vulnerabilities, and correlating events to improve incident reporting.

The FortiSASE Secure Private Access solution enables:

- **Simplicity:** With Fortinet’s best-in-class security deployed everywhere, FortiSASE provides a consistent experience for on-premises and remote security to reduce security gaps, simplify operations, and significantly reduce overhead resources associated with setup and configuration.
- **Consistent Security:** IT teams can overcome security gaps and minimize attack surfaces through a consistent security posture enforced across physical offices, virtual and cloud environments, and remote users. Simplifying network and security policy management through a unified networking approach and single agent ensures that strong security can be deployed and enforced everywhere.
- **Superior User Experience:** FortiSASE SPA offers Secure SD-WAN hub connectivity to support hybrid networks with seamless on-premises integration. Fortinet’s Secure SD-WAN application-driven approach provides broad application steering with accurate identification, advanced WAN remediation, and accelerated cloud on-ramp for optimized network and application performance.

### FortiSASE Secure Private Access Features

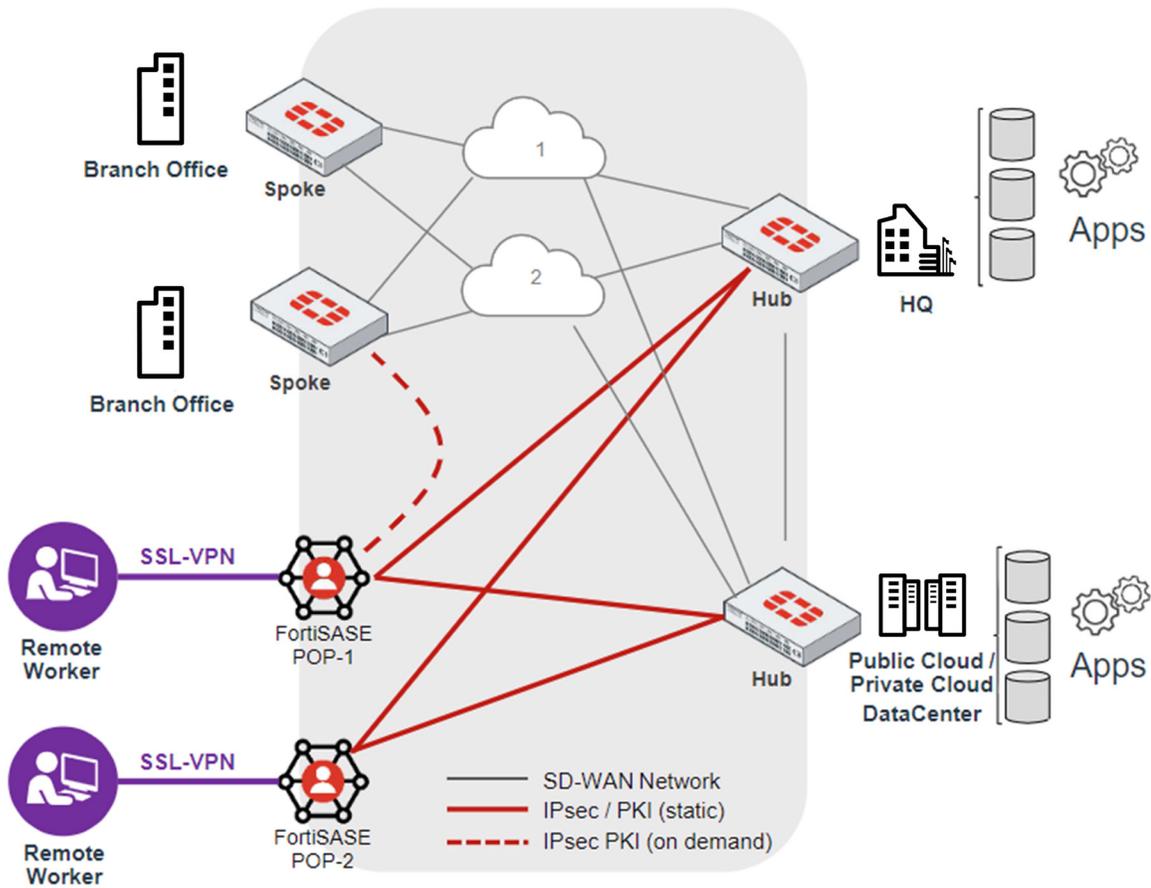


Figure 3: Comprehensive security for safe access to corporate apps

## Key FortiSASE benefits:

<p><b>Universal ZTNA</b></p>	<p>ZTNA is a capability within Fortinet's Zero Trust Access (ZTA) solution that controls access to applications. It extends the principles of ZTA to verify users and devices before every application session. ZTNA also confirms that they meet the organization's policy to access that application.</p>
<p><b>SD-WAN (application-aware traffic control)</b></p>	<p>SD-WAN application traffic controls provide 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.</p>
<p><b>Flexible deployment</b></p>	<p>Flexible deployment models are available for both SD-WAN and SASE.  <b>SD-WAN:</b> Deployment options include hub-to-spoke (partial mesh), spoke-to-spoke (full mesh), and multi-WAN transport support.  <b>SASE:</b> Easy configuration of SASE POPs and SD-WAN hubs from the SASE management console.</p>
<p><b>SD-WAN routing</b></p>	<p>Advanced routing options include 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.</p>
<p><b>Network and security convergence</b></p>	<p>The industry's only organically developed, purpose-built, and ASIC-powered SD-WAN enables thin edge (SD-WAN, routing) and WAN Edge (SD-WAN, routing, NGFW) to secure all applications, users, and data in the branch offices. And its integration with FortiSASE enables consistent robust security for users everywhere.</p>

## Achieve better business outcomes with FortiSASE

FortiSASE meets the growing need of today's organizations 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, Fortinet's goal is to help you consolidate security under one vendor through a single client and operating system, to reduce complexity, increase security effectiveness, provide consistent policy orchestration and enforcement, and ensure a reliable user experience across today's expanding networks. Because of its unique approach, FortiSASE enables hybrid workforce security and cloud-delivered security for WFA strategies for any organization worldwide.

