WHITE PAPER

Protecting Financial Services in the Hybrid Workforce Era

FortiSASE Delivers Security, Simplicity, and Performance for Remote Work

Executive Overview

Today's banking and financial services sector embraces new digital capabilities to remain relevant in an increasingly competitive landscape. Organizations leverage applications, networks, and devices to boost operational efficiency, increase customer satisfaction, and launch new products and services. But as companies rely on new digital tools, their attack surface expands. Each remote employee login, cloud application, or service integration is a new potential vulnerability.

To maintain resilience against a combination of sophisticated threats and a rapidly transforming hybrid infrastructure, financial services institutions need advanced protection from the data center to the endpoint to the edge. As a critical extension of the Fortinet Security Fabric platform, Fortinet's FortiSASE secure access service edge solution can consistently apply enterprise-grade protection and superior user experience across all the extended parts of a modern financial services organization.

Finance firms lose approximately $5.9 million per data breach, 28% higher than the global average.[1]

Trends and Challenges in Securing Financial Services

Financial institutions are desirable targets for cybercriminals. These organizations are typically responsible for managing customer money and often retain volumes of personally identifiable information (PII) and other sensitive data. As such, financial institutions also face increasing legislative pressure to protect customer data. Failure to comply with these regulations and maintain strict security standards may lead to steep penalties and losing the ability to process credit card payments.

Beyond this baseline of common risks, several technology trends have been adversely impacting cybersecurity within the financial services sector in recent months.

- **The rise of the hybrid workforce:** A recent survey showed that U.S. senior executives expect fully remote and hybrid work to grow through 2028.[2]
- **Software-as-a-Service (SaaS) adoption:** SaaS continues to dominate the software market. It also accounts for more than 45% of public cloud services revenue.[3]
- **Zero-trust framework adoption:** More than half of respondents from a global survey reported that they considered adopting a zero-trust strategy a top or high priority for their organization.[4]
- **Overall lack of process modernization:** Many financial organizations must evaluate and update their software and internal processes for greater efficiency. Despite the widespread adoption of SaaS and an anticipated embrace of zero trust, there is a critical need for transformational process modernization, such as SaaS with some component of zero trust. One of the most significant vulnerabilities for financial institutions is the proper management of their software.[5]
- **Security inefficiency:** Security and risk management leaders are currently hampered by operational inefficiencies due to poor integration across their security stack.[6]

The combined effect of these trends is causing some unique operational challenges for the financial institutions' IT and security teams.

Poor user experience: As working from anywhere has become the new normal in most industries, employee experience and productivity are negatively impacted by backhauling application traffic to on-premises data centers for centralized security controls.

Struggling to maintain regulatory compliance: The financial services industry faces increasingly strict and complex regulatory requirements. This includes aggressive new SEC rules for greater accountability and transparency, which require businesses to manage their cybersecurity risks.[7] Over the past year, 83% of banking leaders say their cybersecurity concerns have increased, while 70% say their concerns about compliance have increased.[8] At the same time, rapid digitalization, SaaS adoption, and hybrid work have increased the security risks associated with shadow IT. Last year, 41% of employees acquired, modified, or created technology outside IT's visibility.[9]

Complex business-to-business connectivity: Managing multiple business-partner VPNs has become difficult for large financial organizations to manage and maintain concerning patches and updates.

Lack of redundancy: In the event of a power outage or other on-prem system failures, financial services organizations need to back up their physical network firewalls to ensure that all parts of the business (such as distributed ATM networks) remain protected at all times.

Solution: SASE

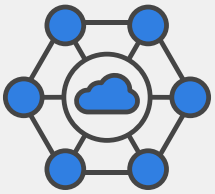
A SASE architecture can address these challenges by extending secure access and high-performance connectivity to work-from-anywhere users. SASE combines cloud-delivered networking (SD-WAN) and security capabilities, including Firewall-as-a-Service (FWaaS), secure web gateway (SWG), zero-trust network access (ZTNA), and cloud access security broker (CASB). This offers hybrid financial services organizations secure network edge connectivity, an optimized application experience, and security for branch locations and remote users.

However, many SASE solutions available today have severe limitations, especially when serving the sensitive needs of banking and financial institutions.

- **SASE comprises security products from different vendors, creating complexity and security gaps.** Lack of native integration between the different components can inhibit visibility, intelligence sharing, and automation, thereby slowing threat detection and response capabilities.
- **Multivendor SASE can also be difficult to deploy and manage.** This creates unnecessary burdens for under-resourced security teams while increasing risks to the organization.
- **Many SASE solutions rely on shared compute in cloud instances.** This can expose risks to stored data and cause compliance problems for financial services organizations.

A single-vendor SASE solution can address these concerns. Single-vendor SASE refers to delivering networking and security capabilities in a unified solution from one vendor. It converges networking and security both in the cloud and on-premises, which reduces complexity while helping to improve efficiency and lower costs by simplifying the number of disparate vendors and products that IT teams have to manage.

The explosion in SaaS deployments has caused inefficiencies and complexities that can no longer be ignored, even as enterprise cloud adoption rolls on.[10]



Single-vendor SASE solutions are expected to grow twice as fast as multivendor approaches.[11]

Single-vendor SASE can also improve the user experience if the solution has a single agent. To implement ZTNA, some vendors require a different endpoint agent for their SASE product vs. their hardware firewall to help enforce ZTNA. Having multiple agents means users must learn multiple interfaces, and IT must manage each solution separately. Dealing with a patchwork of different products with a varying look, feel, and deployments increases complexity, cost, and risk. But if there's only one agent, it's easier for users and IT teams.

Taking the benefits of a single-vendor approach even further, a unified SASE solution enforces consistent policies and controls across on-premises and cloud environments to dynamically address the needs of hybrid workforces. This approach facilitates complete integration of SASE functions while helping further reducing the managerial burden on resource-constrained IT teams. While the market has identified single-vendor SASE as a standard, Fortinet's solution goes above and beyond by leveraging Unified SASE, which has hybrid use cases.

Why Fortinet

FortiSASE offers simple, cloud-based management with a self-service design, easy user onboarding, and a flexible, tiered, and user-based licensing model. License bundles include Fortinet ZTNA with the endpoint agent, so ZTNA capabilities are available whenever the customer wants to enable them.

Universal ZTNA

Leverage ZTNA in the office, at home, or when traveling to apply application-level segmentation.

Single-Vendor SASE

Leverage Fortinet SASE solutions to participate in SD-WAN and add internet security for traveling and remote workers.

Wireless Mesh

Send Fortinet access points to strategic users for their home office to extend the wireless network with zero-touch provisioning.

Branch Office at Home

Deploy FortiGates, switches, and APs with zero-touch provisioning to add Secure SD-WAN to increase resiliency for the home executive.

Secure SD-WAN

The Secure SD-WAN platform supports cloud-first, security-sensitive global enterprises and protects the hybrid workforce.

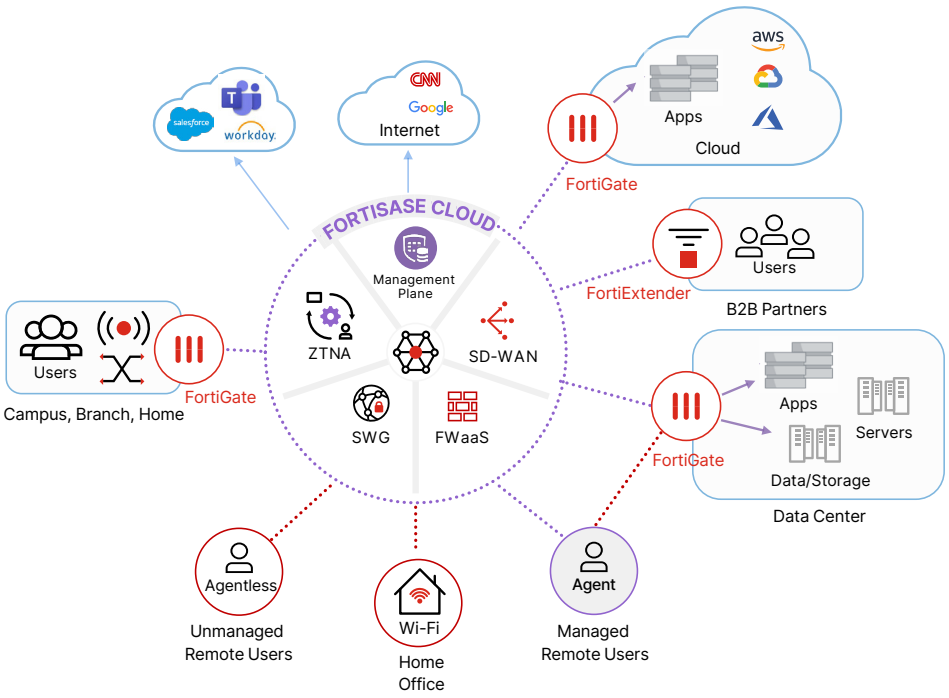


Figure 1: Financial services single-vendor SASE with ZTNA

FortiSASE 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. FortiSASE also seamlessly integrates with our FortiEDR endpoint security solution, automatically identifying and stopping breaches in real time.

Consistent cybersecurity for users, whether on- or off-network: FortiSASE provides comprehensive cloud-delivered security with natively integrated ZTNA to provide consistent protection for WFA users.

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.

Unified management and visibility: FortiSASE offers high visibility across both on-premises and remote users, ensuring the security of the modern hybrid workforce. With FortiManager, organizations can leverage a unified policy engine and management system that spans all edges and users, regardless of their location. Also, FortiAnalyzer, in conjunction with FortiSASE, provides centralized logging and response capabilities for networking and security across the entire organization. This enables organizations to understand their network and security events, facilitating effective incident response and mitigation.

A single, unified operating system: FortiOS provides an integrated, cloud-based SASE solution that protects users, applications, and endpoint devices while seamlessly interoperating with the rest of the distributed network.

High performance: FortiSASE helps security teams manage risks at speed, scale, and performance. Fortinet's custom ASIC technology provides the lowest latency of any SASE vendor.

Use Cases and Benefits

FortiSASE supports use cases relevant to today's financial services organizations. Above and beyond single-vendor SASE, Fortinet's approach enables a unified SASE solution that uniquely converges networking and security to support today's hybrid workforces. It provides high ROI through consolidation and improved digital user experience, offering a robust network of over 100 global SASE locations for broad coverage and scalability.

Improved user experience: With FortiSASE, users enjoy outstanding application performance while organizations get the same level of security that they have with their on-prem security infrastructure. For example, FortiSASE allows organizations to offload volumetric traffic. This means streaming video apps like Zoom or WebEx don't have to be backhauled to data centers. Secured traffic can go directly through the internet to improve the overall end-user experience.

Compliance: Because FortiSASE runs on physical hardware as opposed to a virtualized server, Fortinet provides the ability to have dedicated SASE instances with no shared compute. This uniquely benefits financial services organizations because there is no shared memory space to cause problems from a compliance standpoint. FortiSASE is portable and can be deployed in Google Cloud Platform and Amazon Web Services environments. The solution is largely made available through Fortinet's own data centers or hosted in partner data centers across the globe.

Flexible deployment: Organizations can be prescriptive about what they protect with FortiSASE on an application-by-application basis. You have complete autonomy and flexibility in terms of how the deployment goes. For example, you can start by just putting one or two applications into SASE while the rest of your traffic goes through existing data center-based security.

Cyber-risk management is nothing new to financial services companies, but the importance of a robust, comprehensive strategy has never been more critical and will only increase as institutions expand their technological footprint.[12]

Cloud-based redundancy: Cloud-based FortiSASE improves the resiliency of financial services organizations by providing failover security in the event of on-premises security outages.

Simplified life-cycle management: FortiSASE offers flexibility for spinning up new environments and workloads, greatly simplifying the time and labor of life-cycle management for operations teams.

Seamless B2B connectivity: With Fortinet, B2B connectivity becomes a managed service via a thin branch device. This approach eliminates management on the customer side, bypassing the need to upgrade or patch a VPN concentrator in the data center. It also offloads troubleshooting on the remote side. As a result, many of today's pressing financial services compliance issues are simplified.

Legacy proxy replacement: FortiSASE supports hosted proxy security, enabling organizations to eliminate the cost and complexity of legacy proxy infrastructure.

Guest networks: Fortinet can accommodate guest networks by leveraging existing infrastructure or APs. FortiSASE secure internet access (SIA) allows organizations to offload the burden of supporting guest network access to a cloud-based solution, keeping on-premises financial services networks separate and secure from customers, partners, and other visitors.

Remote call centers: Many insurance companies and other financial institutions rely on customer call centers staffed by on-premises employees. FortiSASE enables these call centers to be staffed by remote workers. Organizations can replace or augment their VPNs thanks to the built-in FortiSASE ZTNA capabilities, which provide proper identity access management compared to a VPN's all-or-nothing approach. With Fortinet, this shift doesn't have to happen all at once. Organizations can use VPN and ZTNA in tandem and strategically transition application access on their own schedule.

Summary

As new digital tools and hybrid work structures introduce new risks to financial institutions, security teams need to ensure the resiliency of operations, compliance with regulations, and the effectiveness of their cybersecurity infrastructure across an expanding attack surface. As an extension of the Fortinet Security Fabric, FortiSASE addresses the challenges of today's banking and financial organizations, from optimizing the user experience to ensuring operational redundancy to protecting sensitive data and PII in compliance with strict industry standards and regulations.

[1] "Cost of a data breach 2023: Financial industry impacts," Security Intelligence, August 30, 2023.

[2] "Survey: Remote Work Isn't Going Away — and Executives Know It," Harvard Business Review, August 28, 2023.

[3] "Worldwide Public Cloud Services Revenues Surpass $500 Billion in 2022, Growing 22.9% Year Over Year, According to IDC Tracker," IDC, July 6, 2023.

[4] "Is adopting a zero trust model a priority for your organization?," Statista, December 7, 2023.

[5] "Cybersecurity In Finance: Protecting Client Data And Mitigating Risks," Forbes, September 11, 2023.

[6] "Most organizations want security vendor consolidation," Security Intelligence, September 21, 2023.

[7] "Balancing risk and compliance: implications of the SEC's new cybersecurity regulations," CSO, August 22, 2023.

[8] "2023 Risk Survey," Bank Director, March 2023.

[9] "Shadow IT is increasing and so are the associated security risks," CSO, June 6, 2023.

[10] "CIOs take aim at SaaS sprawl," CIO, March 15, 2024.

[11] "More Enterprises Opt for Single-Vendor SASE Solutions," Network Computing, August 7, 2023.

[12] "The cyber clock is ticking: De-risking emerging technologies in financial services," McKinsey & Company, March 11, 2024.

May 16, 2024 2:27 PM

2638618-0-0-EN