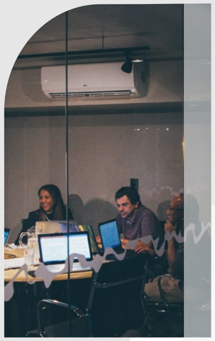


A new security landscape for financial services

Exploring adaptive security from Fortinet and AWS

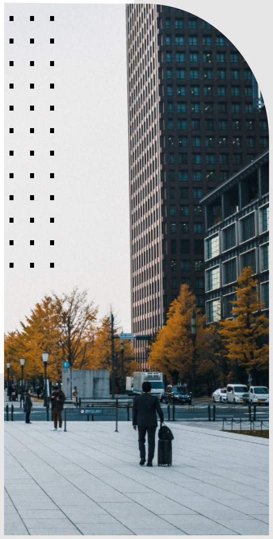


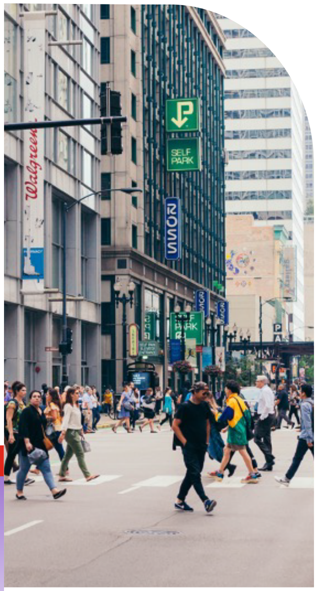
Table of Contents

Introduction: The future state of cloud, networking, and compute

With digital transformation now an accepted practice and with more financial services firms moving data and applications to the cloud, the threat landscape continues to grow. The rise of ransomware attacks, email-borne threats, and other bad acts puts assets and data on-premises, on the cloud, on devices, and at the edge at greater risk.

In the past, centralized point solutions and hub-and-spoke architectures dominated the financial services security scene. Today, the effects of the pandemic have created a different security landscape. Remote working, distributed work, virtual offices, increased migration from on-premises data to the cloud, and cloud-first applications require a change. Software-defined wide area networks (SD-WAN) security, "zero trust" architectures, next-generation firewalls, and secure access service edge (SASE) have come together to create new security ecosystems for financial services. The convergence of these technologies is the way forward for cybersecurity.

Why are these ecosystems the future state? The answer to that question is flexibility. From SD-WAN to SASE, new technologies require a security fabric that can adapt to an everchanging financial services cloud, data center, and edge landscape. In this eBook, we explore how Amazon Web Services (AWS) and Fortinet work together to provide that fabric.



Cybersecurity challenges and trends that affect financial services

As evidenced by the new Cybersecurity Executive Order, improving cybersecurity and being able to handle persistent threats, ransomware attacks, and other malicious activity are an important focus area.[1] Ransomware is more adaptive and scalable than it was just a few years ago, and has a large threat surface area. While putting protective measures in place, financial services organizations also need to navigate industry regulations, which evolve over time.

The good news is that innovative security solutions are answering these challenges. To address one of the most notable landscape changes—the move from traditional hub and spoke, router-based network architectures to SD-WAN—and the integration with security to create secure SD-WANs available. An SD-WAN is a virtual WAN architecture that can select the optimal access transport services—including MPLS, LTE, and broadband internet services—and secure SD-WANs are built to protect them.

To ensure legitimate access to the computing resources that have shifted to the cloud, there is **Zero Trust architecture.** It uses least-privilege and need-to-know access to ensure only the right users are getting into financial services applications at the right level. For full, consistent, and precise control of applications, centralized management, and security automation across the hybrid environments prevalent in financial services organizations, forward-looking firms are increasingly turning to **adaptive cloud security.**

The latest trend in cybersecurity is **Secure Access Service Edge (SASE).** Many in the tech world, including Gartner (who coined the term in 2019), believe it is the future of converged security and networking. It is a network architecture that combines SD-WAN and Zero Trust with security functions such as secure web gateways, and cloud access security broker. SASE is the ultimate manifestation of the need for integrated networking and Zero Trust-based security across LAN, WAN, data center and cloud edges.

[1] The White House, Executive Order on Improving the Nation's Cybersecurity. 21 May 2021.

Address security in this new landscape

Adaptive security and a security fabric are key to protecting your customers' and investors' valuable and confidential financial data from threats like ransomware and hacks while remaining compliant with regulations. AWS and Fortinet can deliver both. AWS infrastructure for financial services organizations is built to help manage compliance with SOC, GDPR, PCI-DSS, CCPA, and others—while remaining agile. AWS global data centers make it possible to follow data sovereignty laws.

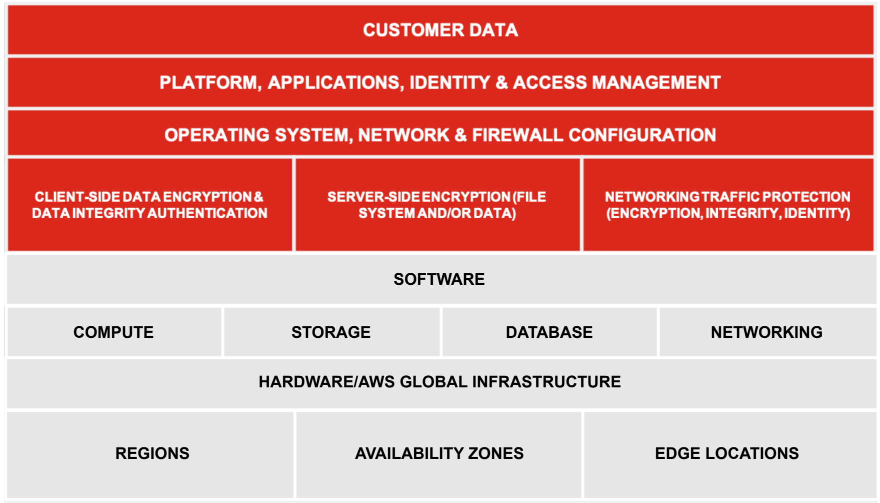
However, there's a balance between the security that AWS supplies and the control your financial services firm has over its workloads. The AWS Shared Responsibility Model[2] describes the roles. AWS is responsible for protecting the infrastructure that runs all the services offered on AWS. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS services. Your responsibilities depend on the AWS services your financial services organization selects. AWS also offers security services that you can use as part of your SOC.

But if you don't have the bandwidth or the desire to manage it all yourself, there are other options available from Fortinet that can help. Fortinet is an established leader in securing financial services, with deep expertise in integrating best-in-class security and SD-WAN products that readily integrate with AWS.

The Fortinet Security Fabric for AWS brings end-to-end security with market-leading prevention, detection, and mitigation technologies, augmented with AI-driven threat intelligence to combat today's most advanced threats.

For example, Fortinet solutions enabled Yedpay, an e-commerce payment platform, to keep pace with continually evolving cyberattacks. Fortinet provided security across Yedpay's current offerings while preparing to expand its services and grow its business. Let's take a closer look at how AWS and Fortinet approach cybersecurity for financial services.

Security IN the cloud



CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

Security OF the cloud

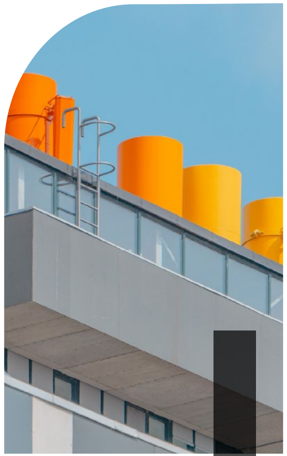
[2] AWS Cloud Services, Shared Responsibility Model.

Centralize data and asset visibility and automate security

In a 2021 Fortinet cloud survey, 78% of respondents said that they want a single pane of glass view of their assets.[3] Fortinet understands how important visibility is to customers. Fortinet's adaptive security solutions for financial services hinge on providing better visibility across AWS, data centers, and networks. Fortinet Security Fabric is integrated at an OS level, providing cross-platform, domain visibility and control spanning LAN, WAN, data centers, and cloud edges. FortiGuard Labs provides real-time visibility into threats, offering a successful, industry-leading zero-day detection operation.

In addition, the Fortinet Security Fabric for AWS enables organizations to centrally manage both cloud and on-premises security functionality, which helps eliminate human errors and mundane tasks, such as configuration management, while reducing the burden on limited IT resources. The Security Fabric delivers centralized security management using a consistent operational model. Your financial services organization also gains in-depth visibility into AWS application deployments and the ability to apply intent-based policies. By using dynamic address groups and logical naming of cloud-based resources, the Security Fabric allows your financial services firm to scale out security policies across its cloud infrastructure.

To reduce risk and complexity, Fortinet security solutions integrate with AWS and use automation to provide centralized management, cloud-native visibility, and broad protection across the attack surfaces. Fortinet Fabric Management Center integrates with your NOC and SOC to look at network and security performance, automating key features to reduce the risk of misconfigurations, which account for 40% of breaches. With the ability to analyze security data faster, organizations can make better business and security decisions around that data.



[3] Fortinet, Cloud Security Report, 2021.

Bolster security with AI/ML

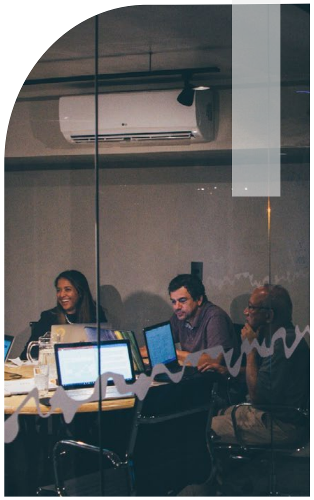
Solutions with artificial intelligence and machine learning (AI/ML) can help secure your financial services organization's cloud data and workloads more effectively and efficiently—with much less effort and time. Cloud security requires analyzing large amounts of data quickly, which can be impossible in a human-centered IT environment. When AI/ML is in the security mix, the human eye is replaced with automation and visualization so that analyzing the volumes of data generated by monitoring and other measurement tools is quicker and more efficient.

AI/ML built into cloud, network, and compute security should be applied to more than automating analytics. It should be an integral part of a mature prevention, detection, and response edge-to-edge security strategy. Applying AI at the right point of technology on the right surface also helps move detection as far left of the detonation of malware as possible. Utilizing AI in security services enables coordinated and consistent real-time defense from the latest attacks. And that is why AI powers the Fortinet Security Fabric for AWS, for example, to enhance the accuracy of detection, to accelerate the mitigation of threats at speed, and to scale.

But it doesn't stop there. Using millions of global network sensors, FortiGuard Labs monitors the worldwide attack surface and employs AI to mine that data for new threats. To help your financial services firm meet compliance standards and protect-mission critical hosted applications, Fortinet FortiWeb Web Application Firewalls on AWS provide advanced features and AI-based machine learning detection engines that defend web applications from known and zero-day threats. FortiGuard Security Services also offer AI-enabled security capabilities for content, web, device, and users. These continuously assess risks and automatically adjust protection across the Fortinet Security Fabric.

Tackle the DevSecOps angle

Developing with agility is crucial for all modern companies in almost every industry, and financial services is no exception. Unfortunately, hackers are increasingly attacking major organizations through development (dev) environments. As more application teams adopt continuous integration/continuous delivery (CI/CD) workflows, it's increasingly important that organizations have integrated and automated security in place to protect these workflows, which is where DevSecOps comes in.



In the DevSecOps philosophy, the entire approach of development is structured around security. It starts with a transformation of organizational culture, getting developer and security teams aligned on the same end goal. Moving to a posture of more automation, monitoring, and oversight, not just detective controls, is key.

The implementation of a DevSecOps model is easier with the right tools. With the Fortinet Security Fabric for AWS you can achieve full visibility and control across your dynamic multi-cloud environments without compromising security. You can use secure SD-WAN to create more efficient paths for the testing and communication essential to the DevSecOps process. As you expand and adjust your development team, you can incorporate Zero-Trust Network Access control with Fortinet FortiNAC.

Summary

Fortinet's partnership with AWS is a better-together combination that ensures the protection of your AWS workloads with security solutions that constantly evolve based on threat intelligence. In addition, the Fortinet Security Fabric integrates SD-WAN to ensure optimized networking and security across the LAN, WAN, data center and cloud edges.

The integration with key AWS services enables the Fortinet Security Fabric to simplify security management, ensure full visibility across cloud, hybrid, and edge environments, and provide broad protection across your workloads and applications. Some of these services include Amazon GuardDuty, AWS Outposts, AWS Transit Gateway, AWS Gateway Load Balancer, Amazon Elastic Cloud Compute (Amazon EC2), and Amazon CloudFront, and AWS Outposts.

Find Fortinet solutions in AWS Marketplace.

FORTINET® | aws

Copyright © 2021 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 General Counsel, 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. 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.