WHITE PAPER

Fortinet Financial Services Cybersecurity Solutions

Protecting Institutions Against Advanced Threats While Optimizing Cost and Efficiency

Executive Summary

Financial services institutions are faced with near-constant attacks and intrusion attempts. Cybersecurity teams at those companies need visibility in order to achieve the cost savings, operational efficiency, and compliance reporting that they need to maintain competitiveness. Fortinet cybersecurity solutions for financial services cover a number of use cases with comprehensive protection. The performance of FortiGate high-end firewalls meets the specialized needs of electronic trading infrastructures, and the Fortinet Security Fabric covers the entire organization with a multilayered defense visible on a single pane of glass, with centralized policy controls. Additionally, Fortinet supports connectivity at branch locations with secure networking solutions that are scalable and high performing.

The financial services sector is a high-value target for cyberattacks—the world's most-attacked industry, according to one report.[1] Facing constant intrusion attempts and other attacks, financial services organizations often find it difficult to move from a reactive cybersecurity stance to a proactive one. Achieving this goal is complicated by a continually expanding attack surface[2] brought about by new technologies launched through digital innovation initiatives.[3] Adding to this complexity is the need for compliance with a growing number of regulations regarding the use of financial and personal data.[4]

> **"The cost to a financial institution facing a cyberattack specifically targeting their online banking services costs an average of $1.8 million."[5]**

Protecting extremely sensitive data is a top priority, for both business and compliance reasons. But security cannot come at the expense of network performance, as consumers and businesses increasingly demand real-time access to every offering, from online and mobile banking to high-frequency trading. At the same time, institutions must control costs and optimize operational efficiency to remain competitive in an industry with many players.

Key Financial Services Cybersecurity Challenges

Cost reduction

Financial services organizations are under constant pressure to contain and reduce costs across their IT environment. Cybersecurity budgets require strategic financial and human resource allocation. Given that money and staff time are finite, risk tolerance must be balanced against risk posture, and trade-offs must be made. Adding to these challenges are cybersecurity staff shortages,[6] which make it difficult and expensive to fill certain roles—if they can be filled at all.

Visibility

The attack surface continues to grow in scope and is increasingly difficult to protect. The proliferation of Internet-of-Things (IoT) devices, the adoption of multiple clouds for business services, and the use of mobile devices by customers and employees rapidly expand the attack surface. As a result, financial services firms deploy more and more point security products to cover the gaps created by the expanding attack surface. The resulting security silos obfuscate visibility—increasing operational inefficiencies and ratcheting up risk.

Operational efficiency

Lack of integration across the different security elements and architectural fragmentation increase operational inefficiencies. Without integration, many security workflows must be managed manually, which causes delays and increases the likelihood of mistakes. In addition to delaying threat detection, prevention, and response, architectural silos create redundancies, increased operational costs, and potential holes in an organization's cybersecurity posture.

Flexibility

As financial services organizations increasingly embrace cloud applications and infrastructure, the security architecture must be sufficiently agile to enable fast, secure, and compliant public, private, and hybrid cloud-based services while protecting traditional on-premises services at the same time.

Compliance reporting

The financial services sector is among the most highly regulated industries in the world, with personal and corporate financial data residing across the network—from the campus, to the data center, to the edge, to the cloud. Organizations must be able to demonstrate compliance with multiple regulations and standards without redeploying staff from strategic initiatives to manually prepare audit reports.

> **"Financial services firms reported 819 cyber incidents to the Financial Conduct Authority (FCA) in 2018, up from just 69 incidents in 2017, an increase of more than 1,000%."[7]**

Use Cases

Cybersecurity for electronic trading infrastructures

Electronic trading is a specialty in financial services that requires extremely high deterministic performance in its digital systems. This includes the firewalls that protect traffic between electronic trading platforms and the rest of the financial institution, including systems that provide real-time information to customers. If misleading information is transmitted to the banking side of the business in the first seconds after a transaction—or that information is delayed—customer satisfaction suffers. Often, these problems can be traced to "jitter," in which small packets of data pass through the firewall in nonsequential order.

Testing at two top global banks[8] confirms that **FortiGate high-end firewalls** provide the lowest latency in the industry, with near zero jitter. At the same time, they deliver highly scalable protection for traffic moving between electronic trading infrastructures and corporate systems. Built-in intrusion prevention system (IPS), intent-based segmentation with zero trust access, and mobile security features eliminate the need for separate point products for these functions. Single-pane-of-glass visibility improves operational efficiency, and application programming interface (API)-enabled automation helps organizations tailor policies and workflows to the unique needs of electronic trading.

These cybersecurity features help organizations achieve business requirements such as:

- Meeting federal regulations on traffic inspection between partners without compromising performance metrics
- Improving security effectiveness by segmenting critical customer and business data
- Improving visibility to facilitate automation and simplify management

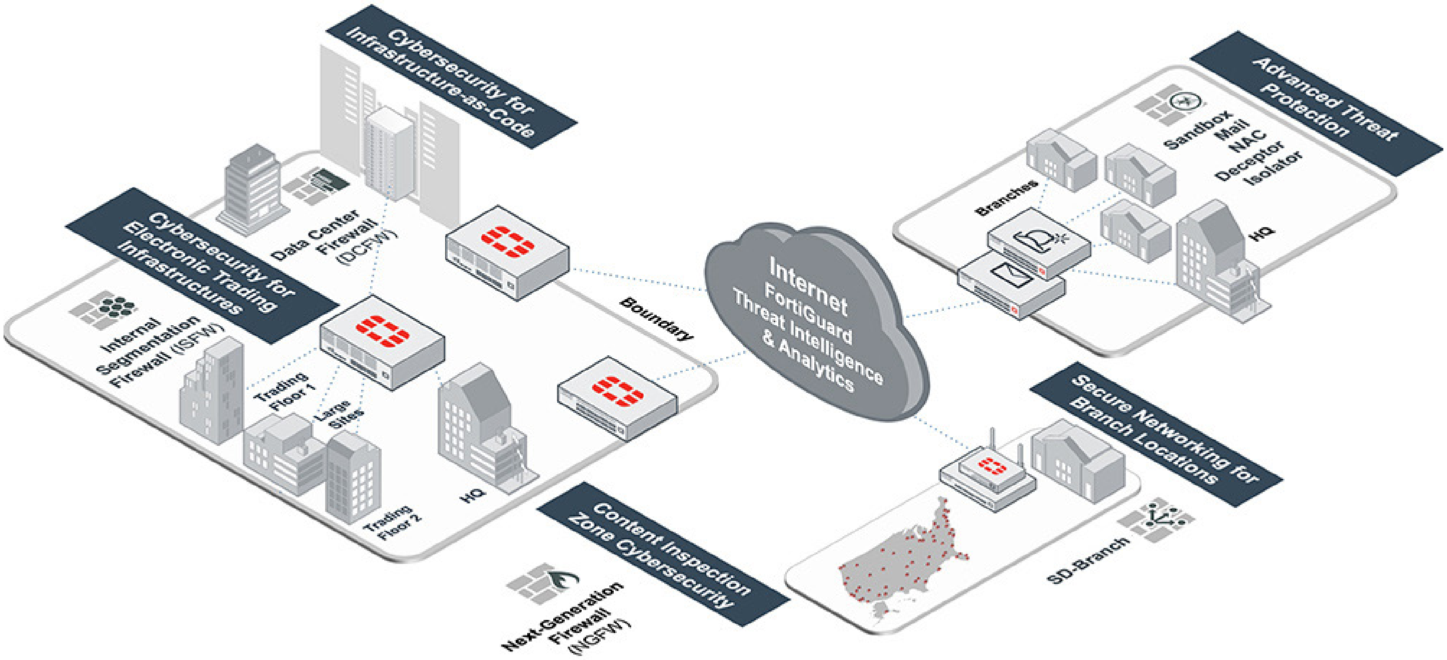
Cybersecurity for Infrastructure-as-Code

Companies leveraging automation platforms to deploy infrastructure using an Infrastructure-as-Code (IaC) model realize significant benefits through a streamlined and automated provisioning model. Often used in support of DevOps cycles, IaC means that changes to an organization's infrastructure can be made quickly and easily.[9] This greatly improves operational efficiency, but it also exposes organizations to potential undiscovered vulnerabilities.[10]

The best way to provide a secure IaC infrastructure is to take a Security-as-Code approach, intentionally building security into the underlying structure of DevOps applications. **FortiGate internal segmentation firewalls** (ISFWs) leverage intent-based segmentation to intelligently segment infrastructure according to business intent, apply adaptive process control, and provide automated threat protection across the IaC environment. **FortiManager** and **FortiAnalyzer** provide centralized network and security management, log correlation, and analytics to enable high performance and robust security from a single console. Fortinet's open ecosystem enables seamless and deep integration with third-party automation platforms via Fabric Connectors and a robust representational state transfer application programming interface (REST API).

A Fortinet Security-as-Code solution protects the IaC infrastructure by:

- Providing protection for critical, time-sensitive network traffic without sacrificing performance
- Segmenting network traffic according to business intent, bolstering compliance and guarding against breaches


Cybersecurity for Infrastructure-as-Code
Data Center Firewall (DCFW)
Cybersecurity for Electronic Trading Infrastructures
Internal Segmentation Firewall (ISFW)
Trading Floor 1
Large Sites
Trading Floor 2
HQ
Boundary
Internet FortiGuard Threat Intelligence & Analytics
Advanced Threat Protection
Sandbox
Mail
NAC
Deceptor
Isolator
Branches
HQ
Secure Networking for Branch Locations
SD-Branch
Content Inspection Zone Cybersecurity
Next-Generation Firewall (NGFW)

Financial services cybersecurity solutions from Fortinet cover the entire attack surface—from the electronic trading floor to branch locations—with a broad, integrated, and automated approach to security.

Content inspection zone cybersecurity

No longer is an organization's infrastructure neatly contained within its in-house data-center infrastructure. One recent survey found that 85% of companies operate in multiple public and private clouds.[11] Software-defined wide-area network (SD-WAN) technologies are now routinely moving organizations' network traffic over the public internet,[12] and IoT devices are proliferating at the edge.[13]

As a result, a perimeter-based approach to cybersecurity is no longer adequate for financial services institutions. It is more effective to think in terms of a content inspection zone—a virtual perimeter that spans corporate data centers, multiple clouds, IoT devices, and network traffic moving on the public internet.

FortiGate next-generation firewalls (NGFWs) utilize purpose-built security processors and comprehensive threat intelligence from FortiGuard Labs to deliver top-rated, high-performance inspection of clear-texted and encrypted traffic. Single-pane-of-glass visibility and control across on-premises and cloud-based environments drives operational efficiency and enhanced security. And the **Fortinet Security Fabric** enables end-to-end integration of a variety of Fortinet and third-party security tools using Fabric Connectors and an open API. Robust threat intelligence powered by artificial intelligence (AI) underlies the entire security architecture, enabling detection and response to attacks in real time.

An end-to-end, integrated security architecture powered by Fortinet brings many benefits:

- *Operational efficiency* with the elimination of manual security processes
- *Cost avoidance* through consolidation of cybersecurity and elimination of redundant licenses
- *Simplified compliance reporting,* avoiding an all-hands-on-deck approach to audit preparation
- *Enhanced security* with automated response workflows and real-time threat intelligence

Secure networking for branch locations

As network traffic increases—especially to and from distant cloud data centers—financial services institutions face increasing costs to maintain acceptable levels of network performance between branch offices and headquarters. Purchasing additional multiprotocol label switching (MPLS) bandwidth is an expensive and time-consuming undertaking, and is not scalable to future network demands.[14] At the same time, remote branches—and edge devices within them[15]—are a target for cyber criminals, who see them as easier to penetrate.

FortiGate Secure SD-WAN enables network traffic to travel securely over multiple connections between branches and headquarters—including the public internet. It eliminates the requirement for all traffic to be routed through the data center for inspection, preventing bottlenecks that result in latency. And it builds scalability into the network infrastructure connecting branch offices with headquarters, thus eliminating future bandwidth investments.

At remote locations, **Fortinet SD-Branch** enables financial services organizations to combine networking and security capabilities for branch offices—all administered from a single FortiGate NGFW. The solution includes **FortiSwitch** switches, **FortiAP** wireless access points, and the **FortiExtender** LTE WAN extender to ensure secure and high-performance networking at the branch. And the **FortiNAC** network access control (NAC) solution enables full visibility and control over all IoT devices found at the network edge.

FortiGate Secure SD-WAN and Fortinet SD-Branch enhance security and network performance in the branch network by:

- *Enabling security-driven networking,* making it harder for adversaries to penetrate the network from a branch location
- *Driving operational efficiency* by combining networking and security into a single product, centrally controlled through a single device

Advanced threat protection

Attacks from adversaries are increasing in volume,[18] velocity,[19] and sophistication,[20] and financial services firms are among the top targets.[21] Security teams that still rely on manual response to incoming threats are overwhelmed with the number of alerts and cannot stop advanced threats that move at machine speed. At the same time, insider threats—malicious and accidental—pose increasing risk in the financial services sector as the value of financial services data increases for threat actors.[22]

To combat these threats, it is best to take a two-pronged approach, targeting both malware and the attackers that create it. The foundation of an *attack-based defense* is robust, real-time threat intelligence. All Fortinet Security Fabric tools leverage comprehensive, AI-powered threat intelligence from **FortiGuard Labs,** based on one of the world's largest intelligence networks. AI and machine learning (ML) help identify unknown or zero-day threats, which are increasingly common due to adversaries' use of advanced techniques like polymorphism.[23]

FortiSandbox provides another layer of defense against zero-day threats. It enables unknown files to be examined in a safe location before being allowed onto the network.

Intrusions Experienced in Financial Services[16]

(in the past 12 months)

- Malware, 49%
- Spyware, 37%
- Insider threats, 35%
- DDoS, 31%
- Mobile, 29%
- Phishing, 24%
- Ransomware, 16%
- SQL injection, 13%
- Zero-day attacks, 12%
- Man-in-the-middle attacks, 11%

Impact of Intrusions in Financial Services[17]

(in the past 12 months)

- 40% suffered an operational outage that affected productivity
- 40% experienced a breach that damaged brand reputation
- 34% suffered an operational outage that impacted revenue
- 32% had an operational outage that affected worker productivity
- 32% lost critical business data

"Progressive companies are offering compelling, personalized customer experiences while building financial services cybersecurity operations that are data-driven, flexible, and scalable."[24]

And since 60% of malware is now encrypted,[25] the secure sockets layer/transport layer security (SSL/TLS) inspection capabilities in **FortiGate NGFWs** allow for inspections to include encrypted traffic—without impacting performance.

An *attacker-based defense* provides an arsenal of tools to identify and neutralize those who would infiltrate the network—whether they are outside or inside the company, and whether their intent is malicious or benign. **FortiDeceptor** is designed to lure attackers into identifying themselves before they cause damage. And **FortiInsight** protects against insider threats by continually monitoring users and endpoints for noncompliant, suspicious, or anomalous behavior that suggests compromise.

This two-pronged approach helps organizations deal with the advanced threat landscape by:

- *Creating a multilayer defense* to detect zero-day threats
- *Catching attackers in the act,* matching their technological sophistication to identify them and thwart their campaigns

> **"Customers are more comfortable sharing data with companies they actually trust; when firms fail to deliver on security, their brand reputation, customer trust and even revenue are negatively impacted."[26]**

Fortinet Differentiators

High performance

FortiGate offers the industry's *lowest latency and jitter rates* for electronic trading infrastructures—when microseconds matter. And ensuring SSL/TLS encryption inspection does not impact network performance.

Visibility and operational efficiency

The Fortinet Security Fabric includes a long list of third-party APIs—as well as an open API architecture. This enables financial services firms to integrate disparate security elements distributed across an ever-expanding attack surface into a single-pane-of-glass view.

Secure branches

A comprehensive ***software-defined branch infrastructure*** that provides optimal security and improves network performance, from the switching infrastructure to the data center.

Conclusion

For financial services institutions, it is arguably more important than ever to safeguard corporate data, applications, and workflows from increasingly advanced threats. The Fortinet Security Fabric provides a unified platform that enables them to build a comprehensive, integrated protection network for the entire institution while maintaining high network performance.

[1] "IBM X-Force Threat Intelligence Index 2019," IBM, accessed November 6, 2019.

[2] "Protecting the Expanding Attack Surface," Fortinet, accessed November 6, 2019.

[3] "Industry leaders struggle to balance digital innovation and security," Help Net Security, April 4, 2018.

[4] "Federal Regulations for Financial Institutions and Other Industries," CSI, accessed November 6, 2019.

[5] "The Impact of Cybersecurity Incidents on Financial Institutions," Identity Theft Resource Center and Generali Global Assistance, accessed November 6, 2019.

[6] Jon Oltsik, "Is the cybersecurity skills shortage getting worse?" CSO, May 10, 2019.

[7] Warwick Ashford, "Financial services top cyber attack target," Computer Weekly, July 31, 2019.

[8] "Deterministic Communications for Secure High-speed Performance," Fortinet, September 23, 2019.

[9] Christopher Null, "Infrastructure as code: The engine at the heart of DevOps," TechBeacon, accessed November 6, 2018.

[10] Justin Boyer, "Security as Code: Why a Mental Shift is Necessary for Secure DevOps," Simple Programmer, March 7, 2018.

[11] "Assembling your cloud orchestra: A field guide to multicloud management," IBM, October 2018.

[12] Andy Patrizio, "Enterprises are moving SD-WAN beyond pilot stages to deployment," Network World, May 7, 2018.

[13] "25% Of Cyberattacks Will Target IoT in 2020," Retail TouchPoints, accessed November 6, 2019.

[14] Nirav Shah, "Reducing WAN OpEx with High SD-WAN Performance," CSO, April 9, 2019.

[15] Howard Altman, "The top five cyber threats for banks—and how to meet them," BAI Banking Strategies, June 26, 2019.

[16] Based on a series of survey studies with different personas conducted by Fortinet. Research report forthcoming.

[17] Ibid.

[18] "Security Teams Overwhelmed by Rising Volume of Attacks," Dark Reading, May 31, 2017.

[19] Dave Barton, "Automation: Moving Security from Human to Machine Speed, and All its Implications," Security Magazine, May 28, 2019.

[20] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[21] Warwick Ashford, "Financial services top cyber attack target," Computer Weekly, July 31, 2019.

[22] Tucker Bailey, et al., "Insider threat: The human element of cyberrisk," McKinsey, September 2018.

[23] Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," Smarter MSP, June 13, 2018.

[24] "Challenges and Opportunities to Close the Cybersecurity Gap in the Financial Services Industry," SecurityIntelligence, April 18, 2019.

[25] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[26] "Industry leaders struggle to balance digital innovation and security," Help Net Security, April 4, 2018.

FORTINET®

www.fortinet.com