SOLUTION BRIEF

Meeting Financial Services Challenges with Infrastructure and Security Automation from Fortinet

Executive Summary

Large global financial services institutions are facing mounting challenges from several directions at once. The rising demand for more digital products; fiercer, more frequent cyberattacks; and tighter banking regulations are all converging on a competitive, dynamic landscape where legacy institutions and fintech disruptors are vying for market share.

Fortinet automation solutions help financial services providers meet these challenges and position themselves for growth by establishing an automation framework across all applications and infrastructure. This enables faster, more accurate scaling of resources while maintaining consistent security standards.

The financial sector continues to be victimized by financially motivated organized crime—typically via phishing, use of stolen credentials, or ransomware. As a result, successful system intrusions in the financial services industry have doubled from 14% in 2016 to 30% in 2022.[4]

The Evolving Challenges of the Financial Services Industry

Customers want more digital experiences. Customers are demanding—perhaps even taking for granted—that their financial services providers deliver a seamless digital experience. This includes banking and financial management on mobile applications; more responsive, effective customer support that is both more digitized and more human; and more data-driven offerings that help them better analyze their financial status and plan for the future.

Indeed, most financial services providers are well on their way to meeting these demands. Eighty-four percent have already implemented mobile banking and 72% have implemented cloud-based customer collaboration platforms, according to a recent study.[1]

Cyberattacks are increasing. Financial services providers are also defending themselves from an onslaught of data breaches, ransomware, malware, phishing, and social engineering attacks that are growing in sophistication, frequency, and intensity. IBM estimates the average cost of a financial sector data breach is $5.85 million—with an average of 233 days needed to find and contain each intrusion.[2] And the challenges of fending off these threats are increasing as the attack surface expands in breadth and complexity.

New regulations are adding to the challenge. Financial services providers are addressing all of these customer demands and security threats while meeting new, more stringent regulations for data privacy and security within an expansive computing environment. And as regulatory expectations increase, operating costs spent on compliance have increased by over 60% for retail and corporate banks.[3]

Financial Services Providers Pursue Cloud and Automation on Their Terms

While the vast majority of financial services companies (83%) are already deploying cloud technology as part of their primary computing infrastructures,[5] for many the ideal state is having all the advantages of public cloud within a private cloud infrastructure they own. Private cloud infrastructure gives financial services providers the flexibility, availability, and speed of service delivery of public cloud infrastructure, while affording more control for security and regulatory compliance. Put simply, they want to be their own AWS, Azure, or Google Cloud.

Emerging technologies like containers and microservices have built on the foundation of the cloud to bring automation to servers and storage. Now, forward-looking, financial-services providers are looking to extend automation into the network to bring the same efficiency, standardization, and speed to the routers and switches, firewalls, and load balancers of private cloud infrastructure.

The Benefits of Building an Automation Framework with Fortinet

Fortinet automation solutions for financial-services providers make network and security automation accessible. Companies leveraging automation platforms to deploy infrastructure using an Infrastructure-as-Code (IaC) model realize significant benefits through a streamlined and automated provisioning model. Where once separate IT teams worked in silos based on the infrastructure layer—with different teams for applications, servers, routers and switches, and firewalls—they can now all "talk to each other," doing their work within a unified automation framework that integrates the entire deployment cycle and maintains security posture at scale. Financial-services customers using Fortinet automation are deploying applications in minutes instead of days.

Key Use Cases for Fortinet Automation

Provision/reprovision: Fortinet automation allows teams to rapidly provision infrastructure and applications, while reprovisioning allows them to delete existing configurations and quickly rebuild from what is stored in the database—a reset button for an entire infrastructure that might be compromised by malware, disaster, or other unforeseen events. Reprovisioning through Fortinet automation also enables greater licensing flexibility, for example, by making it easier to reallocate firewall licenses to other projects.

- Some Fortinet customers are using the platform to bring new devices onto the network. They leverage the API and automation framework together with FortiManager (the central manager of security devices), so that new devices are simply plugged in and all the pre-provisions, templates, and security policy is pushed down live. This makes it possible to build out a complex network built on SD-WAN and VPNs all in an automated fashion.

Network and security automation: Fortinet automation mitigates security vulnerabilities by making it possible to automate repetitive, yet critical tasks related to security, decreasing human error, and enforcing standards without compromising speed to market.

- Some Fortinet customers are using the platform for policy automation. Fortinet is integrated with their ticketing systems to navigate an approval process and the collection of new information related to applications that are being provisioned, changed, or moved. Teams execute the workflow of approvals; once approved, changes are automatically pushed to FortiManager. Users avoid performing these steps manually and potentially making mistakes, or wasting time watching screens load. They simply review and push changes out.

Financial Benefits

- **Reduced total cost of ownership (TCO):** Fortinet automation is not a replacement of IT staff. It is a force multiplier, reducing TCO by executing common, repeatable tasks so that infrastructure teams can better respond to the volume and rate of change. Fortinet automation shifts time spent implementing to time spent planning, verifying, and monitoring, increasing the quality and accuracy of the work.
- **Risk mitigation:** Decreased human errors, automated adherence to security standards, automated security responses, compliance, and auditing all contribute to lower risk.
- **Faster time to market:** Automating routine infrastructure and security configurations leads to significant reductions in time-to-market for new products and services.
- **Increased productivity:** Infrastructure teams are able to bring more services online, faster.

Technical Benefits

- **Robust and comprehensive API:** The same API is used across physical, virtual, and cloud appliances, allowing for the automation of most configuration tasks.
- **Augmented employee performance:** Infrastructure team members perform technical configurations faster and more accurately.
- **API language consistency:** One single API is used across all deployed Fortinet firewalls, regardless of version and model.

- **Streamlined process:**
  The "assembly line" approach means a streamlined process with all teams working within the same automation framework for simpler, faster delivery of services.

Operational Benefits

- **Decreased human error:** Automation brings consistency to the mundane tasks that are most prone to human error.
- **Offloaded repetitive tasks:** Team members can recapture time by avoiding the many repetitive tasks of deploying new services.
- **Maintaining standards:** The consistency of automation enforces standardization across all tasks.
- **Strengthened security posture and decreased threat landscape:** By reducing human error from the deployment process, use of automation significantly reduces exposure to cyberattacks.

Transitional Benefits

- **Policy optimization:** Fortinet automation helps to standardize and optimize security policies, enabling a smooth, stable transition when deploying new digital tools and services.
- **Automated conversion services:** Migrating complex, outdated device configurations to modern solutions is challenging and time consuming, and the process can introduce errors. Fortinet automation enables a smooth, supported migration experience while automatically eliminating errors and redundant information.
- **Modernization of security adoption:** Accurately apply next-generation threat protection services to a security policy intelligently, pre- or post-deployment.
- **Low-touch provisioning:** The rapid, low-touch provisioning of network devices in a large-scale environment gives IT teams the speed required to respond rapidly to service demands.

What Makes Fortinet Automation Different?

While there are several network and security automation platforms available to financial services providers, Fortinet confidently offers distinct value that sets it apart from competitors.

Robust and comprehensive API

With Fortinet's automation solutions, the same API is used across appliances in physical, virtual, and cloud infrastructure, no matter what type of container, firewall, or hardware device. The entire Fortinet suite also uses the same API language (JSON) for simple, powerful, and scalable use cases and performance.

Commitment to automation and the API

Fortinet is invested in and committed to the continued success of its automation platform and its future roadmap. If there's a network or security task that can be feasibly automated, but isn't yet through Fortinet, it likely will be in the near future.

[1] "2021 Financial Services Digital Transformation Survey," BDO, January 2021.

[2] "How can a zero trust policy improve your industry?," Security Intelligence, January 14, 2022.

[3] "Regulatory productivity: Is there an answer to the rising cost of compliance?," Deloitte, May 23, 2022.

[4] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.

[5] "Google Cloud study: Cloud adoption increasing in financial services, but regulatory hurdles remain," Google, August 12, 2021.

FORTINET

www.fortinet.com

July 8, 2022 9:45 PM
1646658-0-0-EN