Protecting the ATM Network with Fortinet

Security Fabric Provides Optimal Protection for Dispersed ATMs
Executive Summary

Protecting a network of geographically dispersed automated teller machines (ATMs) is a key challenge of modern banking. An effective security infrastructure entails enterprise-class next-generation firewalls (NGFWs) at the network edge. It also includes a host-level NGFW at each ATM and an endpoint protection solution on each machine. The network needs sandboxing functionality to isolate threats and management software that streamlines security administration across widely dispersed machines. Security teams are often inclined to seek each of these solutions from different vendors. However, running an assortment of disparate point products reduces the efficiency and effectiveness of securing an ATM network’s attack surface.

What banks need is a set of solutions, as embodied in the Fortinet Security Fabric, that integrate tightly. They should share threat intelligence in real time and enable remote management of all elements of the security infrastructure.

Key Benefits of the Security Fabric

The Fortinet Security Fabric consists of best-of-breed security products in each of the areas crucial for protecting an ATM network. These solutions include Fortinet products and third-party security software. Integrated by design, the solutions share information about any threats they detect and their response to those threats. This information sharing happens automatically, in real time. No human intervention is required to ensure that security solutions across an ATM network respond in concert to perceived problems.

Automated threat-information sharing enables a more effective, coordinated response to multivector attacks targeting multiple facets of a bank’s attack surface. When one security solution recognizes a known threat, the entire Security Fabric is prepared to defend against that threat.
To protect against advanced, unknown, and zero-day threats, the Security Fabric incorporates real-time threat intelligence from FortiGuard Labs. The team of expert security researchers at FortiGuard Labs continuously examine third-party software applications, looking for exploitable vulnerabilities. Automated sharing of this information across the Security Fabric enables solutions to respond quickly when a previously unknown threat emerges.

The Fortinet Security Fabric also includes solutions that provide best-of-breed security administration and management. Utilizing these tools streamlines management by enabling remote, centralized administration of the entire security infrastructure for a network of ATMs.

Core Components of a Fortinet Security Fabric for ATM Networks

The Fortinet Security Fabric delivers broad visibility and protection to every security device on a bank’s corporate network. It also reduces the total cost of ownership (TCO) of security management. The Security Fabric approach is vital for securing a network of dispersed ATMs.

Fortinet solutions provide both best-of-breed functionality and tight Security Fabric integration in each of these crucial security areas:

FortiGate NGFWs

With purpose-built security processors and integration of threat intelligence from FortiGuard Labs, FortiGate NGFWs offer top-rated protection for any network. For example, in 2018, FortiGate NGFWs received their fifth consecutive “Recommended” rating from NSS Labs.¹ Gartner has included Fortinet in the “Leaders” quadrant of its Magic Quadrant for Enterprise Network Firewalls for two consecutive years.²

To meet the unique, diverse needs of an ATM network, Fortinet NGFWs come in a range of models. They are available as appliances, virtual machines (VMs), or cloud-based solutions. High-end FortiGate NGFWs provide business-grade perimeter protection to help prevent malware from entering the bank’s corporate network.

Meanwhile, midrange or entry-level FortiGate NGFWs are well-positioned to serve as hostlevel firewalls on individual ATMs. Host-level NGFWs can turn each ATM into its own network segment, preventing threats from moving laterally between machines. This is especially important if a thief uses a skimming device to hijack an ATM’s phone or internet jack.

Further, zero-touch deployment of updates and patches makes FortiGate NGFWs an efficient option for managing security on widely spread-out ATMs. Security organizations no longer need to send staff to branch locations to configure and install—or conduct maintenance on—firewalls. When the FortiGate appliance plugs into the network, it automatically connects to the FortiDeploy service and receives remote configuration instructions.

Secure SD-WAN

Built into its FortiGate NGFWs, Fortinet enables organizations to activate software-defined wide-area networking (SD-WAN) solutions. To activate Fortinet Secure SD-WAN, banks simply need to turn it on. The infrastructure exists in the form of already-deployed FortiGate NGFWs. Fortinet Secure SD-WAN has garnered significant praise for its performance, low TCO, and powerful security. For example, it achieved a “Recommended” score in NSS Labs’ first-ever SD-WAN testing.³ Moreover, the TCO of SD-WAN protection was nearly 90% lower in FortiGate NGFWs than in the next-closest competitor.⁴

Very small branches, retail “pop-up” stores, or temporary bank locations may not have traditional data links available for SD-WAN applications. This is solved with FortiExtender WAN client. FortiExtender enables banks to deploy ATMs over a secure SD-WAN network connection anywhere 3G/4G LTE mobile coverage is available.
Fortinet Security Fabric for ATM Networks

FortiClient Endpoint Protection

Endpoint protection is crucial on a network of isolated ATMs. Indeed, endpoints are popular targets for cyberattackers. A recent study, for example, found that 30% of data breaches involve the installation of malware on an endpoint. Endpoints that control machines holding significant quantities of cash are far more desirable targets than the typical corporate desktop computer. Thus, it is imperative for banks to utilize an endpoint protection solution on each ATM system in their network.

Fortinet FortiClient next-generation endpoint protection software provides best-of-breed malware detection and threat mitigation. Specifically, because it fully integrates with the Fortinet Security Fabric, FortiClient incorporates physically isolated ATMs into a bank’s security environment. FortiClient receives real-time updates on any threat activity detected on the network. It also receives external intelligence from FortiGuard Labs and other third-party threat intelligence services. As a result, FortiClient-protected ATMs can proactively combat advanced threats versus the reactive risk approach taken by stand-alone endpoint solutions.

The integration of FortiClient with Fortinet security management tools enables a bank’s IT staff to perform remote vulnerability patching. This is critical to protecting each ATM against known threats. It also minimizes staff time dedicated to endpoint protection, despite the widely dispersed nature of most ATM networks. Moreover, FortiClient virtual patching enables centralized IT staff to push out updates extremely quickly in the event of zero-day threats.

FortiClient has received significant recognition. This includes a “Recommended” rating in NSS Labs’ 2018 Advanced Endpoint Protection report. In the tests NSS Labs conducted, FortiClient’s TCO came in better than average. In addition, NSS Labs gave FortiClient one of the best security-effectiveness scores of the 20 products in the test.
**Encryptic Traffic**

To protect data in motion on its network, a bank needs to encrypt network traffic. Fortinet solutions offer effective, easy-to-implement encryption technology. FortiClient can encrypt traffic between each ATM server and its associated host-level FortiGate NGFW. The NGFW uses IPsec virtual private network (VPN) security to exchange encrypted information with systems in the bank’s data center. This two-level encryption helps prevent connection sniffing, reducing the chance that the financial institution will become a victim of fraud.

Some banks choose to run multiple VPN connections from each ATM to the data center. This minimizes encryption-related latency, which could impair the ATM user experience. Link load balancing is a good idea. However, a bank taking this approach must make sure each connection is secured using IPsec VPN. FortiGate NGFWs make this setup more feasible because the VPN technology is integrated into the NGFWs. Thus, the bank does not need to deploy any additional appliances to achieve redundancy.

**FortiSandbox Sandboxing**

Code that raises an alert within a bank’s Security Fabric should be tested in a sandboxing solution before entering the network. Running questionable code through Fortinet FortiSandbox prevents unknown and advanced threats from reaching the broader network and, ultimately, its ATMs.

FortiSandbox addresses multiple security functions within a corporate network—endpoint, web, mail, and file shares. Banks that have already installed FortiSandbox can leverage the same appliance to protect ATMs spread across all their branches. The endpoint capability in FortiSandbox enables banks to implement advanced threat protection on each individual ATM.

**FortiManager, FortiAnalyzer, FortiSIEM, and NGFWs’ FortiDeploy**

Fortinet management and analytics tools centralize visibility into system vulnerabilities and detected threats. They also centralize control over vulnerability patching and policies implemented across each security device. Such centralization is imperative for effectively managing security on any network. It is even more crucial for a bank’s ATM network, where IT staff are managing machines spread across a country.

FortiManager provides automated, single-pane-of-glass visibility into security across all the solutions in the Fortinet Security Fabric. Able to scale to 10,000 managed devices, FortiManager provides transparency across a bank’s entire attack surface, including every ATM. FortiAnalyzer analyzes a bank’s security risk. It displays the findings through an intuitive, actionable dashboard that drills down into the specifics of each detected threat. The deployment capability in FortiGate NGFWs—designated as FortiDeploy—automates the configuration of security solutions. This streamlines and accelerates deployment of a hostlevel NGFW and endpoint protection at each ATM.

The combination of these capabilities minimizes the staff time required to oversee even the most widely dispersed ATM network. These tools are particularly important for financial institutions facing staff shortages in the IT security arena.

Management capabilities in the Fortinet Security Fabric are further enhanced by security information and event management (SIEM). Here, FortiSIEM provides file integrity monitoring for solutions across the Security Fabric. This accelerates threat mitigation by enabling the security team to verify the integrity of files on ATM servers.

In addition, easy access to threat detection and response data enables much faster response to compliance audits. This improves the organization’s risk posture. FortiSIEM saves staff from manually pulling log files from each machine individually in order to demonstrate compliance. Out-of-the-box reports in FortiSIEM address regulations or guidelines, including:
Payment Card Industry (PCI)
Control Objectives for Information and Related Technologies (COBIT)
International Organization for Standardization (ISO), including ISO 28001
National Institute of Standards and Technology (NIST), including NIST 800-53 and NIST 800-171
North American Electric Reliability Corporation (NERC)
Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense
General Data Protection Regulation (GDPR)
Sarbanes-Oxley (SOX)
Health Insurance Portability and Accountability Act (HIPAA)
Gramm-Leach-Bliley Act (GLBA)
Federal Information Security Modernization Act (FISMA)
Good Practice Guide 13 (GPG13) from the U.K.’s National Cyber Security Centre

Conclusion

Even if a financial institution’s security infrastructure is sound, its network of ATMs generates a multitude of points of vulnerability. The FortiGate product line includes some models well-suited to serve as host-level NGFWs for each ATM. Other FortiGate NGFWs provide enterprise-grade protection for the network perimeter. FortiClient is geared toward offering maximum protection for endpoints such as ATMs. Other elements of the Fortinet Security Fabric are designed to keep the entire corporate network, including the ATM network, secure.

Tight integration of these solutions and threat-intelligence sharing means advanced threats can be stopped faster and more effectively. Threats identified at the ATM are immediately flagged across every ATM and the broader Security Fabric. Likewise, threats identified elsewhere in the Security Fabric are communicated in real time to each ATM NGFW.

In addition to improving security effectiveness, the Security Fabric approach is imperative in controlling the TCO of ATM security. Remote hardware and software deployment, as well as patch management, dramatically improve staff productivity across widely dispersed ATMs. A bank taking a Security Fabric approach may also be able to secure ATMs while deploying less equipment. Specifically, it can leverage best-of-breed Fortinet security solutions that it already has in place to protect its corporate network.

Ultimately, automating and integrating security solutions minimizes a bank’s risk. Attackers will always target ATMs because they hold cash that may be seen as providing an easy payout. An automated, tightly integrated security architecture based on the Security Fabric is a bank’s best bet for combating malicious attacks.
4 Thomas Skybakmoen, "2018 SD-WAN Comparative Report: Total Cost of Ownership (TCO)," NSS Labs, August 8, 2018.
5 Ibid.
8 Ibid.
9 Ibid.