SOLUTION BRIEF

Securing Next-Generation ATM Networks with a Unified Platform

Fortinet Protects Extended Parts of Financial Organizations

Executive Summary

Financial institutions need a security platform designed for the unique needs of their extended network infrastructure. This includes automated teller machines (ATMs), which are becoming increasingly attractive targets for physical tampering and cyber exploitation. The Fortinet Security Fabric includes host-level FortiGate Rugged next-generation firewalls (NGFWs) for each ATM location as well as business-grade FortiGate NGFWs for protection at the network perimeter. It also offers best-of-breed capabilities like secure SD-WAN, endpoint protection, sandboxing, and network access control (NAC). Single-vendor solution integration allows local threat information to be shared across the Fortinet Security Fabric while incorporating global threat intelligence from FortiGuard Labs for automated threat detection and responses. This helps banks protect networks and data while ensuring safe and reliable services for customers across all ATM locations.

According to the recent NielsenIQ International Retail Banking Consumer and Technology Survey, one out of 10 consumers experienced an ATM security breach or became aware of one over a period of 12 months.[1]

The Risks and Challenges of Today's ATM Networks

The recent surge in attacks against financial institutions has intensified cybersecurity scrutiny while raising questions about regulatory responses.[2] As the tactics used by cybercriminals evolve, financial organizations must reevaluate how they protect their networked banking infrastructure from increasingly bold and sophisticated forms of exploitation. The exposed and public nature of ATMs makes them inherently vulnerable points of attack, especially as institutions try to take advantage of the latest digital tools and data insights.

As such, today's ATM networks may introduce multiple security risks while increasing operational challenges for financial institutions. These specific problems may include:

Theft: Tactics may include physically stealing an entire ATM, using skimming devices to exfiltrate customer card information, or hacking an ATM to remove a bank's restrictions on cash withdrawals—sometimes called *jackpotting*.[3]

Expanding attack surface: Today's "smart" ATMs can collect large amounts of customer data that banking institutions can use to gain analytical insights. Unfortunately, cybercriminals have also been quick to exploit these new sources of valuable personally identifiable information.

Compliance: Financial institutions must comply with ever-evolving industry requirements like the Payment Card Industry Data Security Standard and privacy laws and government regulations across every jurisdiction in which they do business.

Rising TCO: To maintain security and compliance, ATMs need frequent patching. For some organizations, this means having a security expert travel to each ATM location every time an update is required. Human staff dependencies dramatically increase ATM networks' total cost of ownership (TCO) as they expand.

Staff shortages: Many security teams are perpetually understaffed due to a persistent lack of experienced and knowledgeable IT security staff worldwide.[4] Rote activities, such as manually patching ATMs, increase security program costs and divert staff from higher-value security activities like threat hunting.

Operational inefficiencies: Many financial institutions still rely on an assortment of isolated point security products to protect their ATM networks. This ad hoc security infrastructure typically complicates management processes, inhibits the visibility of threats, and exposes the business to undue risks.

IT/OT convergence: In the past, ATMs were connected via "air-gapped" operational technology (OT) networks, meaning they were not directly connected to the corporate network or the internet. This isolation helped protect ATMs from IT-based cyberthreats. But the once-siloed worlds of OT and IT have converged to support new digital tools and systems automation. Many ATMs now include wireless capabilities (4G, 5G, LTE) to connect with bank data centers via encrypted site-to-site VPN tunnels. However, these connections also offer hackers a pathway to attack and exploit previously air-gapped ATM networks.

Financial Services Networks Need Platform-Based Security

The key to successfully maintaining a highly secure channel is to protect not only the ATM but also the entire ecosystem around it.[6] A platform-based security infrastructure can address evolving challenges by providing visibility and protection across the organization's entire digital attack surface, including ATM networks.

This security platform should include business-grade NGFWs to guard the network perimeter as well as smaller, host-level NGFWs for each ATM. It should also incorporate secure SD-WAN capabilities, endpoint protection, sandboxing, network access controls, and security management products.

The platform's different solutions must also be fully integrated to automate threat detection and responses. It must also be able to share local threat information across the organization to combat multi-vector attacks while applying global threat intelligence from a leading service to thwart emerging variants.

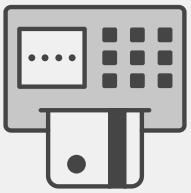
Why Fortinet

The Fortinet Security Fabric offers an ideal platform-based approach for securing financial organizations with modern ATM networks. It combines best-of-breed solutions for enterprise firewalls, host-level firewalls, ATM endpoint protection, and security management.

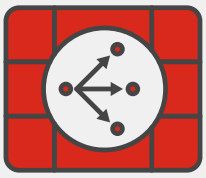
The tight solution integration of the Security Fabric enables advanced automation capabilities that help reduce the TCO of an ATM network by minimizing manual effort across corporate security processes.

Key Fortinet solutions for ATM networks include:

- **FortiGate NGFWs** featuring Fortinet Secure SD-WAN
- **FortiGate Rugged NGFWs** for resilient host-level protection
- **FortiGate Cloud-Native Firewall** (CNF) redundancy protection
- **FortiClient** endpoint protection
- **FortiExtender** wireless WAN connectivity
- **FortiNAC** network access control
- **FortiSIEM** security information and event management



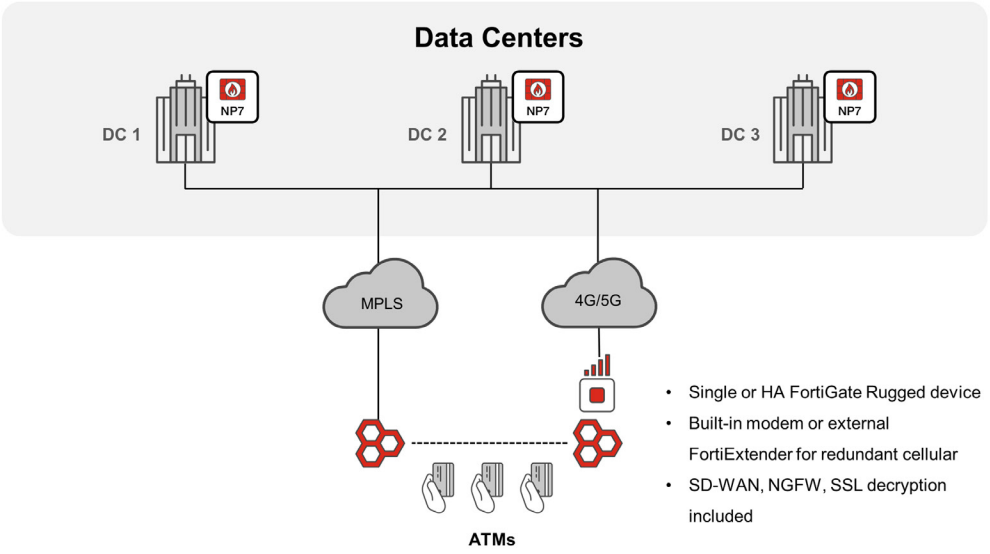
Industry research shows that there has been a 165% increase in ATM attacks year-over-year.[5]



Because each remote ATM connects to two data centers, the platform must also be able to apply SD-WAN and quality of service rules to steer and secure traffic appropriately, something its legacy point-to-point routers were unable to achieve.[7]

Next-Generation ATM Connectivity

Increased accessibility for rugged environments



Goal	Capabilities	Benefits
■ Provide the next generation of connectivity to connect and protect ATMs	■ Rugged device capable of withstanding extreme heat and cold ■ SD-WAN built in for greater resilience ■ IPS, AV, device detection, and additional security profiles in one appliance ■ Flexible IPsec site-to-site policy with quantum- safe encryption keys ■ 4G or 5G available ■ Powerful small form factor to fit in a small space	■ Preserve data privacy and achieve regulatory compliance

Figure 1: Next-generation ATM security

Use Cases for ATM Network Security

The Fortinet Security Fabric supports a comprehensive array of critical use cases to protect and even future-proof today's ATM networks.

Unified firewall capabilities: Using the same vendor for all of the bank's NGFWs streamlines configuration and ongoing management, as staff only need to learn one interface. As the foundation of Fortinet's comprehensive platform, FortiGate NGFWs tightly integrate with all other Security Fabric elements, gathering and sharing the latest threat information across all parts of the organization's defenses.

FortiGate NGFWs at the network perimeter help keep malware out. FortiGates feature built-in intrusion prevention system (IPS) capabilities that include signature matching, analysis of contextual information, such as user behaviors and heuristics, and network and protocol anomaly detection. FortiGates can also be used to segment the organization's corporate network. In the event of an attack, isolating any infected ATMs or other systems through internal network segmentation can effectively stop the lateral spread of a threat and prevent widespread damage.

FortiGate Rugged NGFWs protect each ATM at the host level to prevent them from being used as a vector for attacks across the broader network. They offer zero-touch deployment and central management capabilities to optimize security team efficiency. Because ATMs can be deployed in outdoor environments with direct exposure to extremes of heat and cold, FortiGate Rugged NGFWs are purpose-built to provide reliable protection when operating in harsh climates.

FortiGate Cloud-Native Firewalls provide a cloud-based backup to physical FortiGates so that the ATM network remains protected at all times. Financial institutions need virtual machine redundancy in case of a failure or if there's no way to communicate with a physical site.

Centralized management and monitoring: With a single, unified dashboard, FortiManager establishes visibility and centralized control of security processes to help accelerate threat detection and responses. It also helps limit the time needed to deploy security on each new ATM. With automated configuration of ATM security and zero-touch management features, FortiManager can minimize deployment times while reducing opportunities for manual configuration errors. This value becomes exponential when managing hundreds or even thousands of ATMs spread across a country or throughout the world.

Secure SD-WAN: Many banks want to use SD-WAN to connect ATMs to the corporate network, but they run into issues with regard to security, cost, and complexity. FortiGate NGFWs include high-performance Fortinet Secure SD-WAN capabilities, solving all three challenges. Fortinet Secure SD-WAN provides inexpensive redundancy in the connections between widespread ATMs and the corporate data center. Our solution bridges multiprotocol label switching and metro Ethernet tiers, directing traffic to the best connections as determined by the speed of service and business rules for traffic prioritization. Having the ability to use multiple delivery channels also reduces costs.

Futureproof wireless connectivity: Similar to other remote OT deployments, ATMs typically have extremely long life cycles. The combination of FortiGate Rugged NGFWs and FortiExtender wireless WAN provides ATM networks with futureproof options for current and forthcoming wireless connectivity standards (5G, LTE) as well as backward compatibility with older wireless technologies (4G).

Endpoint protection: Banks also need to have endpoint protection guarding each ATM. FortiClient is specifically designed to detect malware and automatically mitigate threats at the endpoint level. FortiClient also continuously shares threat information with all other parts of the security platform as an integrated part of the Fortinet Security Fabric. It also makes use of the latest global threat intelligence research from FortiGuard Labs to help detect emerging and zero-day threat variants.

Encryption: FortiGate Rugged NGFWs use IPsec VPN security to send encrypted communications to the bank's data center. This two-level encryption helps prevent connection sniffing, which reduces the chance that a bank will fall victim to card fraud. To help ensure that this encryption does not affect ATM throughput (impacting system performance for customers), Fortinet's approach allows financial institutions to securely run multiple VPN connections from each ATM to the data center for link load balancing.

Sandboxing (zero-day detection): When a FortiGate or other Security Fabric solution detects potential malware, FortiSandbox automatically tests flagged code for advanced and unknown (zero-day) threats without exposing the rest of the bank network. It then safely destroys any code that turns out to be an actual threat while notifying the rest of the Security Fabric platform to prevent multi-vector attacks.

File integrity monitoring: FortiSIEM security information and event management facilitates the collection, storage, correlation, and analysis of information from endpoints throughout the corporate network (including ATMs) and from the NGFWs on the network edge. This enables a bank's security staff to oversee an appropriate and coordinated response anytime a threat is detected. Collecting and storing security information in one place can also accelerate responses to regulatory bodies and streamline routine compliance audits.

Network access control: Fortinet's FortiNAC solution allows organizations to implement port-level security on the ATM level (Layer 2), effectively locking down communications between the ATM and the main data center. FortiNAC automatically ensures that only users who are authenticated and devices that are authorized and compliant with security policies can enter the ATM network. It can be configured to detect any unusual or suspicious network activity and respond with immediate action, such as isolating the device from the network to prevent the potential spread of the attack. FortiNAC also maintains a perpetual inventory of users, devices, and their level of access as an active discovery tool to uncover previously unknown devices that may have gained access to all or parts of the network.

Conclusion

Even under the best circumstances, financial institutions must face multiple challenges when maintaining a modern ATM network. Organizations must ensure the availability and security of remote machines deployed across thousands of physical locations and exposed to harsh weather conditions. As targeted attacks against ATMs become more brazen and inventive, banks need a security platform designed to comprehensively protect all parts of their organization.

The Fortinet Security Fabric provides a comprehensive, single-vendor platform for securing today's ATM networks and the broader financial services organization. From ruggedized host-level NGFWs to secure SD-WAN capabilities to network access controls, Fortinet integrates best-of-breed security solutions for automated detection and responses to the latest forms of attack. This, in turn, enables banking institutions to better serve their customers while protecting their assets.

[1] "How to protect ATMs from advanced threats," ATM Marketplace, April 11, 2023.

[2] "The rise of cyberattacks on financial institutions highlights the need to build a security culture," SC Magazine, March 8, 2024.

[3] "Examining cutting edge ATM software attacks," ATM Marketplace, May 19, 2023.

[4] "Distribution of companies experiencing a shortfall of skilled IT security personnel worldwide from 2018 to 2023," Statista, May 11, 2023.

[5] "Banks Fighting ATM Crime," ATMIA, July 14, 2023.

[6] "How to protect ATMs from advanced threats," ATM Marketplace, April 11, 2023.

[7] "Fortinet Improves Resiliency and Operations to 1,000+ ATMs," Fortinet, February 21, 2024.

FORTINET

www.fortinet.com

June 1, 2024 7:22 PM

2636682-0-0-EN