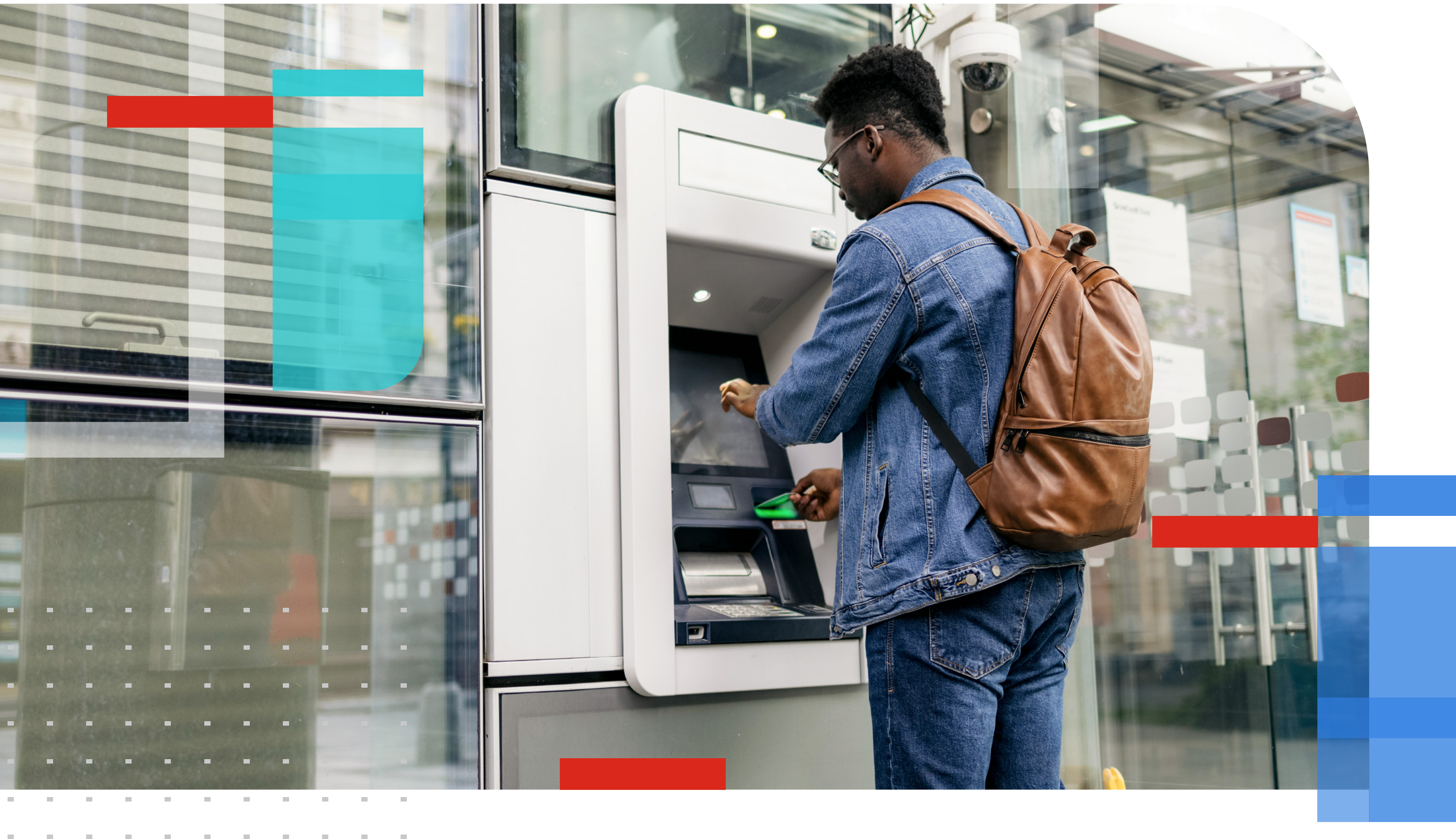
WHITE PAPER

How to Secure an ATM Network

An Integrated Approach to Security



Executive Summary

Exposed, unattended, and geographically dispersed: automated teller machines (ATMs) are among a financial institution's most vulnerable assets. Subsequently, they warrant best-of-breed security. The security platform protecting a bank network should include business-grade next-generation firewalls (NGFWs) guarding the network perimeter and smaller, host-level NGFWs for each ATM. The platform should also incorporate secure software-defined wide area network (SD-WAN) capabilities, endpoint protection, sandboxing, network access controls, and security management products. All of these solutions must automate threat detection and response activities, integrate to share local threat information, and incorporate global threat intelligence from a leading service. Meeting all these different requirements can be a tall order, but finding a comprehensive platform-based solution is necessary to protect the evolving needs of today's ATM networks.

10%

of consumers in a recent international survey said they experienced or became aware of an ATM security breach in the previous 12 months. The data also showed that these respondents were 2.5 times more likely to reduce business or make a purchase with another provider.[1]

The Business Challenges of Today's ATM Network

The global ATM market is projected to reach $34.8 billion by 2030, growing at a CAGR of 5.7%.[2] With more than 3.2 million ATMs currently operating worldwide,[3] the financial services sector faces several rapidly evolving business challenges in maintaining modern ATM networks.

Theft: As the rising number of annual criminal incidents shows,[4] ATMs present an irresistible target for thieves. While some physically steal machines to retrieve the cash inside at a remote location, others plant skimming devices to steal unsuspecting users' debit or credit card information. But one of the fastest-growing ATM threats comes from sophisticated cyberattacks in which hackers remove a bank's restrictions on cash withdrawals. One recent example is FiXS malware, used in a string of attacks against ATMs in Mexico, allowing cybercriminals to spit out cash on demand.[5]

Expanding attack surface: The emergence of "smart ATM" technologies offers customers the convenience of automated branch services while reducing dependence on human tellers for certain transactions. Featuring sophisticated analytics capabilities, smart ATMs also collect massive amounts of data to generate valuable customer insights for banking institutions. But with greater digital capabilities comes greater risk exposure, as cybercriminals aggressively seek out new sources of personally identifiable information (PII) to exploit.

Complicated compliance: Financial institutions must consider how their practices meet the cross-border regulatory framework of the Payment Card Industry Data Security Standard (PCI DSS). PCI compliance for ATMs is integral to a financial institution's overall compliance strategy. Banks scrutinizing ATM security may find that meeting the PCI DSS requires operating system upgrades on the machines. They also may need to develop a more comprehensive and integrated approach to IT security overall.

Financial institutions must also comply with government regulations across every jurisdiction in which they do business. This means banks with ATMs in multiple countries must meet various IT security standards across their ATM network. This may include the Good Practice Guide (GPG)[6] monitoring control best practices in the United Kingdom or the European Union's General Data Protection Regulation (GDPR)[7] standards for data security. Because ATMs obtain user names, account information, and PINs, a bank's IT infrastructure must be GDPR-compliant if EU citizens use its ATMs.

Rising TCO: Maintaining effective and compliant security practices has traditionally required frequent patching of ATMs. If the bank's security infrastructure does not enable centralized management, human staff may need to travel to each individual machine every time a security update is needed. Staffing dependencies dramatically increase the total cost of ownership (TCO) of the ATM network as it expands, and adding new security personnel may not even be a realistic option for many banks, even if organizations can afford it.

Security staff shortages: Companies around the world face a growing shortage of experienced and knowledgeable IT security staff.[8] The situation is acute in some regions: Security teams are perpetually understaffed and have difficulty filling open positions. Any organization facing this type of resource constraint needs to ensure that the experts it does have on staff are focused on strategic tasks. Rote activities (such as performing manual security patches) not only increase security program workload costs but also, more importantly, divert limited staff resources from higher-value activities like threat hunting. Security teams struggling to manage updates across a dispersed ATM infrastructure may be tempted to ask local employees to apply security patches instead. However, personnel who are not formally trained security specialists may make mistakes that reduce the effectiveness of the security update and possibly even expose the machine, network, and broader organization to an outside attack.

Inefficiency: Even when security teams can keep all their ATMs updated, manually managing dispersed machines may reduce the effectiveness of network security overall. If monitoring threats requires staff to collect data from individual machines' log files, the security team may not immediately recognize zero-day threats. Further, if security solutions are not integrated throughout the corporate network, the bank's security products will not respond to threats in a unified manner. Security solutions guarding executive desktops or the corporate data center may not be alerted immediately when an ATM's security solution detects an attack. Such a lack of visibility into threats and lack of coordinated response networkwide undermine a financial institution's overall security posture.

The U.S. Department of Homeland Security has designated financial services as one of 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety.[9]

IT/OT convergence: Traditionally, ATMs were connected via "air-gapped" operational technology (OT) networks, meaning they were not directly connected to corporate networks or the internet. This was the standard practice for isolating ATMs from potential threats. But the once-siloed worlds of OT and information technology (IT) are now converging due to demand for new digital capabilities and systems automation.

Today, ATMs may use common wireless technologies (4G/5G/LTE) to connect with bank data centers via encrypted site-to-site VPN tunnels. However, one of the main disadvantages of this IT/OT convergence is that sophisticated cyberthreats have new ways to access previously air-gapped OT assets. To make matters worse, OT systems can be particularly vulnerable to cyberattacks because they were often designed to implicitly trust everything within their environments. While unfettered internet access will never be part of the ATM network, next-gen ATMs will require the ability to route via a secure access service edge (SASE) solution or a secure demilitarized zone (DMZ) perimeter network.

Best-of-Breed ATM Network Security

A carefully designed cybersecurity infrastructure can help financial services institutions reduce the strain of these critical business challenges. A platform-based approach can offer broad security support with visibility and protection of the organization's entire digital attack surface, including ATM networks. The platform should offer automated threat detection and response capabilities, integrate the different security solutions deployed across the organization, and seamlessly incorporate real-time threat intelligence.

Automated threat detection and response

When security products continuously and autonomously monitor different aspects of a bank network, they will recognize threats much sooner than humans monitoring log files would. If the security solutions also automatically respond when they identify a potential attack, threat mitigation will happen much faster. Rapid mitigation can reduce threat impact in any corporate network, but the benefits are magnified in a financial institution that has ATMs deployed across a country, throughout a region, or even around the world.

Automation offers additional benefits in the realm of security patches and updates. It enables a small team to promptly secure widely dispersed ATMs from a central data center, reducing travel time and costs. Automated patch management also eliminates the temptation to engage in the risky practice of having nontechnical staff at each branch handle these tasks. Automation is especially important for small teams in areas facing acute labor shortages, as it enables the few security experts on staff to focus on more specialized, high-value tasks.

Solution integration and threat intelligence

Another characteristic of a well-designed platform architecture is integration of the various security solutions. Like any sizable organization, a typical bank runs various security products. Some protect the network, while others protect individual machines. No matter how sophisticated these solutions are in their own right, they will be more effective if they can share information and operate in synchronization.

Cyberattacks remain a serious risk, and the best banks have a well-protected and future-proof technology infrastructure and superior data security.

Within a tightly integrated security platform, products alert one another any time they detect a threat to the network. Ideally, they also automatically respond to the threat, which can provide a coordinated threat response across the entire attack surface from the data center to every individual ATM. Coordinated responses are particularly important when combating multi-vector attacks, which simultaneously target several potential security vulnerabilities. As soon as one of the bank's security solutions detects a known threat, all can work together to prevent unauthorized entry at any point in the network.

To protect against unknown threats, the security architecture should also incorporate threat intelligence. When security products integrate with one another and with a reputable global threat intelligence service, they are equipped to respond in concert to zero-day threats as soon as the service recognizes the vulnerability.

Compliance with GDPR, PCI DSS, and local regulations

Compliance with privacy laws and financial regulations in jurisdictions around the world becomes much easier when a bank's security platform includes integration across the various solutions, automated threat detection and response, and incorporation of real-time threat intelligence.

A highly automated and tightly integrated security architecture supports compliance with banking and ATM security regulations worldwide. The European Union's GDPR requires organizations to deploy state-of-the-art systems to secure personal data.[10] While "state of the art" is open to interpretation, it would make sense for the EU to expect security solutions to share data and respond in a coordinated manner to detect threats.

PCI DSS regulations specifically encourage organizations to take a comprehensive and integrated approach to IT security.[11] Platform automation capabilities also support PCI DSS compliance. Among other actions, the rules require financial institutions to ensure their ATMs' security patches are always up to date.

Key Features of an Effective ATM Network Security Platform

To adequately protect ATMs, branches, and the corporate network, an automated and integrated security architecture should include the following components:

- Next-generation firewalls
- Secure SD-WAN
- Flexible wireless connectivity
- Endpoint protection
- Encryption
- Sandboxing
- Centralized management and monitoring
- Security information and event management (SIEM)
- Network access control (NAC)

Perimeter and host-level NGFWs

Every bank needs business-grade NGFWs at the network perimeter to keep malware out. The NGFWs at the network edge should come with built-in intrusion prevention system (IPS) capabilities. IPS features should include signature matching, contextual information analysis, such as user behaviors and heuristics, and network and protocol anomaly detection. Banks selecting perimeter NGFWs should make sure the equipment has only a minimal impact on network performance.

To protect individual ATMs and to prevent them from being used as a vector for attacks across the network, financial institutions need to also look for smaller, host-level NGFWs. The host-level NGFW attached to each ATM should offer zero-touch deployment and central management capabilities to optimize efficiency.

Like many other OT deployments, ATMs often must operate in physical locations with harsh climate exposures. Therefore, these host-level NGFWs should also be ruggedized against variable extremes of heat and cold to provide reliable protection. In addition to environmental resiliency, the security platform should also provide redundancy through cloud-based firewall capabilities. If there is a failure or no way to communicate with a physical site, NGFW virtual machines (VMs) can provide a backup to physical firewalls, ensuring that the ATM network remains protected at all times.

Using the same vendor for all of the bank's NGFWs can further streamline configuration and ongoing management, as staff only need to learn one interface. In support of establishing a comprehensive security platform, it's also crucial that all NGFWs on the corporate network tightly integrate with other infrastructure elements. A bank's NGFWs play a key role in collecting information about threats approaching the network and disseminating that information to the organization's other security solutions. Moreover, NGFWs should tie in with the financial institution's threat-intelligence service. Real-time intelligence sharing across the network facilitates rapid responses to all known and unknown threats.

Finally, financial institutions should consider using NGFWs to segment their 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 an attack and prevent widespread damage.

Secure SD-WAN

Many banks use SD-WAN technologies to connect ATMs to the corporate network. These high-performance edge devices significantly improve WAN utilization. They enable banks to leverage lower-cost connectivity options like cable or DSL and support wireless technologies, such as LTE, WiMAX, and satellite communications. SD-WAN solutions enable a bank to inexpensively achieve redundancy in the connections between its widespread ATMs and the corporate data center. Moreover, SD-WAN technologies can bridge multiprotocol label switching (MPLS) 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.

The challenge with SD-WAN, however, is integrating security. As with legacy approaches to WAN connectivity, backhauling traffic to the data center for centralized inspection bottlenecks network performance. Some SD-WAN technology vendors advocate adding NGFWs at the network edge or at various points along the WAN. But, this approach adds more complexity and increases the total cost of ownership TCO for networking teams.

A more effective approach is to leverage high-performance SD-WAN functionality within NGFWs. Essentially, financial institutions can use their NGFWs to provide a secure, integrated environment in which to deploy SD-WAN as needed and manage it efficiently. This solution uniquely combines advanced NGFW and SD-WAN capabilities (including 5G connectivity) as well as device identification and classification features within ruggedized and non-ruggedized appliances.

Flexible, futureproof wireless connectivity support

Like many other OT systems, remote ATM deployments are often designed for extremely long life cycles. An effective security platform for ATM networks should provide futureproof options for current and future wireless connectivity standards (5G/LTE) as well as backward compatibility with older wireless technologies (4G).

Endpoint protection to enhance ATM security

In addition to protecting edges of the network and deploying internal network segmentation, banks need to have an endpoint protection solution guarding each ATM. The product should be designed specifically to detect malware and automatically mitigate threats at the endpoint level.

Many vendors offer endpoint protection solutions built to perform these functions, but they have a critical weakness: They are entirely standalone and reside in silos. As a result, they do not share threat information with the organization's other security products, nor can they incorporate externally gathered threat intelligence.

In contrast, integrating endpoint protection with other solutions in a platform-based security architecture strengthens a bank's overall security posture. A sophisticated endpoint protection solution helps automate threat detection and responses across the network. Running such a solution in each ATM helps the ATM server respond effectively if malware gets past the host-level NGFW.

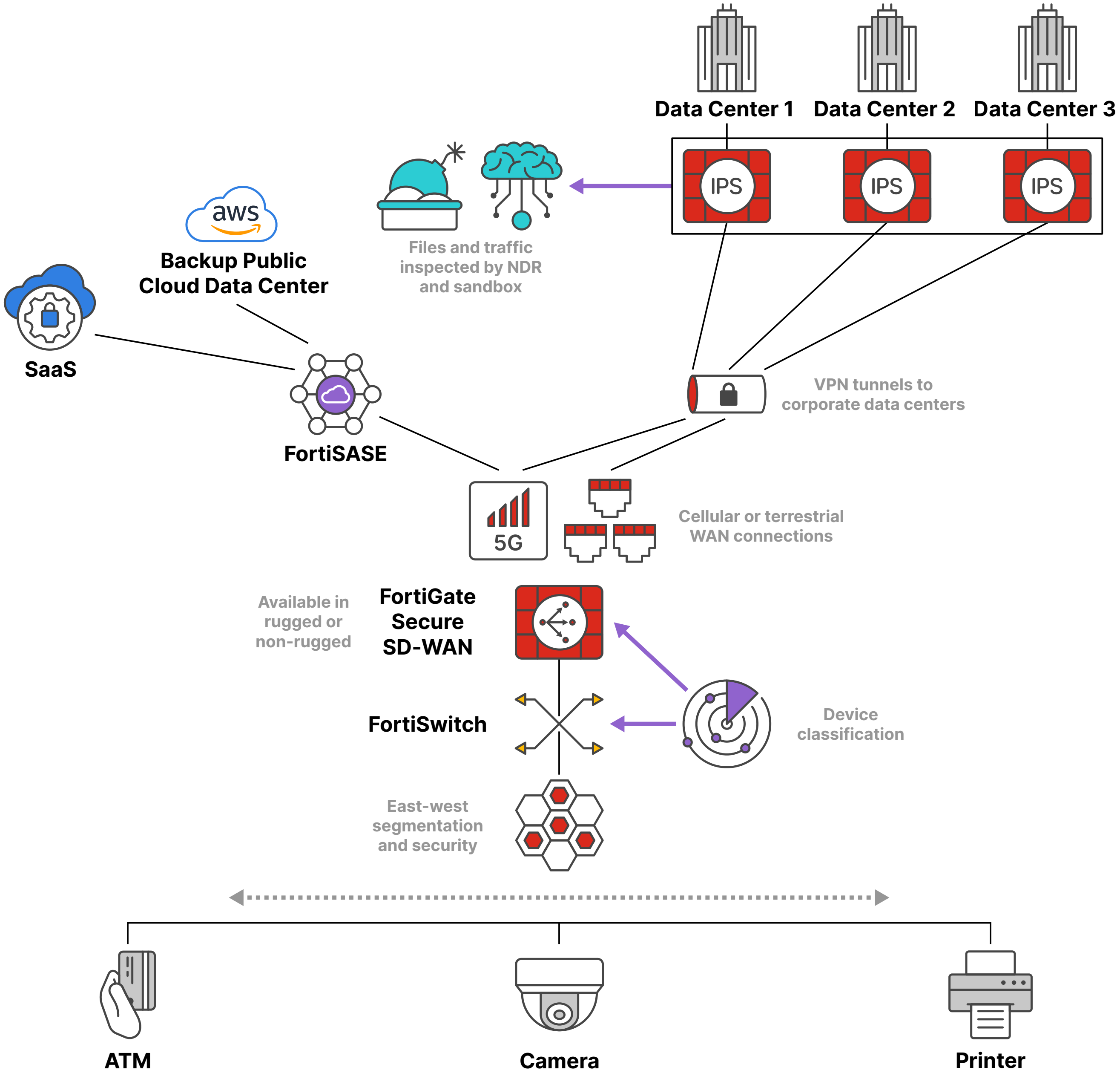

Data Center 1
Data Center 2
Data Center 3
IPS
IPS
IPS
Files and traffic inspected by NDR and sandbox
aws
Backup Public Cloud Data Center
SaaS
FortiSASE
VPN tunnels to corporate data centers
5G
Cellular or terrestrial WAN connections
Available in rugged or non-rugged
FortiGate Secure SD-WAN
FortiSwitch
Device classification
East-west segmentation and security
ATM
Camera
Printer

Figure 1: Next-generation ATM security

Encryption protects network traffic

Because hackers are constantly innovating, even the most robust security environment will likely experience breaches. A bank can encrypt communications for added protection so a hacker can't access its data in motion. An effective endpoint protection solution that secures ATMs encrypts traffic between the ATM server and the host-level NGFW. Then, the ATM-level NGFW uses IPsec virtual private network (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 encryption does not affect ATM throughput, which could impact system performance and frustrate customers, financial institutions can run multiple VPN connections from each ATM to the data center, thus enabling link load balancing. When doing so, the institution must secure each connection using an IPsec VPN solution.

The key to successfully maintaining a highly secure channel is to protect the ATM and the entire ecosystem around it.[13]

Sandboxing isolates possible threats

When a bank's perimeter NGFW, ATM-level NGFW, or endpoint protection solution detects questionable code, the security platform needs to determine the risk the prospective threat poses. Sandboxing technologies provide a safe environment for executing code that might be malware. They can automatically test flagged code for advanced and unknown threats without exposing the rest of the bank network. Further, a sandboxing solution can automatically destroy any code that is a real threat. As a result, the threat never has a chance to gain access to the broader network.

Financial institutions should look for a sandboxing solution that addresses multiple security functions (such as endpoint, web, mail, and file shares). They also need to find a solution that tightly integrates with the other products in the security platform. The sandboxing software needs to automatically notify other security infrastructure elements in real time whenever it discovers a new threat attacking an ATM. This can prevent multi-vector attacks from successfully breaching any other bank network area and vice versa.

Centralized management and monitoring

Visibility and centralized control of corporate security processes are key to threat detection and response. To ensure security teams take the right actions to mitigate threats, they need a high-level view of vulnerabilities and attempted attacks networkwide. Ongoing management and monitoring of the security platform are key considerations in selecting security solutions to protect an ATM network.

Some providers of firewalls, endpoint protection, and other security products also offer tools that centralize management and monitoring of the entire security infrastructure. In addition to providing the requisite visibility, these tools minimize the time required to deploy security on each new ATM. Automated configuration of ATM security, with zero-touch ongoing security management, can shrink deployment times and reduce the chances of configuration errors. Such capabilities are important for a bank that must efficiently and effectively manage security across dispersed ATM locations. This is especially crucial when managing hundreds or even thousands of ATMs spread across a country or worldwide.

SIEM for file integrity monitoring

A SIEM solution facilitates the collection, storage, correlation, and analysis of information from endpoints throughout the corporate network (including ATMs) and the NGFWs on the network edge. This enables a bank's security staff to oversee an appropriate and coordinated response any time a threat is detected.

SIEM solutions that offer file integrity monitoring further enhance threat response for banks. If malware reaches an ATM, the bank's network administrator will first verify the integrity of the files on the ATM server. Automating file integrity monitoring across tightly integrated security products streamlines the response to any threat. This requires a unified security platform across the entire network, including ATMs, servers, and clients.

The visibility that some security management tools provide, combined with SIEM capabilities, can greatly enhance a bank's ability to comply with regulations focused on data protection. Collecting and storing security information in one place can also accelerate responses to regulatory bodies and streamline routine compliance audits.

Network access control

An effective security platform for ATM networks should also include NAC capabilities to implement port-level security on the ATM level (Layer 2), effectively locking down communications between the ATM and the main data center. NAC solutions automatically ensure that only authenticated users and devices that are authorized and compliant with security policies can enter the ATM network. They 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.

NAC also maintains a perpetual inventory of users, devices, and their level of access. It is an active discovery tool to uncover previously unknown devices that may have gained access to all or parts of the network, requiring IT administrators to adjust security policies. Restricting network access also means controlling the applications and data within the network, which will become an even larger target of cybercriminals in the smart ATM era. The stronger the network controls, the more difficult it will be for any cyberattack to infiltrate the network.

Modern ATM Networks Require Platform-Based Security

Every ATM represents a potential point of vulnerability for the customer cards it processes, the cash it stores, and the corporate network as a whole. Subsequently, a bank's security architecture should incorporate best-of-breed solutions for enterprise firewalls, host-level firewalls, ATM clients, and security management tools. It also must ensure that these solutions are tightly integrated.

Integration and automation help reduce the ATM network's TCO by minimizing manual effort across corporate security processes. When a financial institution can leverage the NGFWs and other network security solutions it already has, the cost savings can be even more significant.

At the same time, an automated and integrated security platform reduces risk. By building an infrastructure in which geographically dispersed machines automatically receive the latest security updates and can coordinate to respond to threats, a bank prepares its ATM network for any known and unknown future threats.

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

[2] "Automated Teller Machines (ATMs) Global Market to Reach $34.8 Billion by 2030: Robust Branch Automation Initiatives Offer Significant Growth Opportunities," Globe Newswire, March 14, 2023.

[3] "Some Crucial ATM Statistics To Understand Its Expansion Worldwide In The Banking Sector," Enterprise Apps Today, updated February 28, 2023.

[4] "ATM crime continues to proliferate," ABA Insurance Services, March 3, 2023.

[5] "Crooks 'jackpot' ATMs in Latin America with new FiXS malware," SC Media, March 6, 2023.

[6] "The BCI Good Practice Guidelines (GPG)," Business Continuity Institute, accessed December 23, 2023.

[7] "Complete guide to GDPR compliance," GDPR, accessed July 31, 2023.

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

[9] "Critical Infrastructure Sectors," CISA, accessed July 26, 2023.

[10] "Data protection in the EU," European Council, June 1, 2023.

[11] "PCI DSS Quick Reference Guide," PCI Security Standards Council, November 2, 2022.

[12] "McKinsey's Global Banking Annual Review," McKinsey & Company, December 1, 2022.

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

FORTINET

www.fortinet.com

December 27, 2023 1:13 PM

228491-B-0-EN