How To Secure an ATM Network
A Multipronged, but Integrated, Approach to Security
Executive Summary
Exposed, unattended, and geographically dispersed, automated teller machines (ATMs) are among a financial institution’s most vulnerable assets. Thus, 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 a smaller, host-level NGFW for each ATM. It should also incorporate endpoint protection, sandboxing, and security management products. All these solutions must automate threat detection and response activities, integrate with one another to share threat information, and incorporate threat intelligence from a leading service. Meeting these requirements is a tall order, but finding the right solutions is necessary to secure cash repositories around the world.

Best-Of-Breed ATM Network Security
For would-be thieves considering the possibilities, ATMs are an irresistible target. Some choose to physically steal the machine with the goal of accessing its cash in a remote location. Others plant physical skimmers or use other means to steal credit card information. But the fastest-growing threat for networks of ATMs comes from cyberattacks, in which hackers remove a bank’s restrictions on cash withdrawals and then “cash out” at its ATMs.¹ One such scheme in August 2018 resulted in the successful theft of the equivalent of nearly $13 million across 28 countries in two days.² Protecting against these and other cyber threats requires a carefully designed cybersecurity infrastructure. The platform should focus on automation of threat detection and response, integration of security products, and seamless incorporation of world-class 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 respond automatically 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 spread 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 secure widely dispersed ATMs in a timely manner 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 this task. 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 value-added tasks.

Security Solution Integration and Threat Intelligence
Another characteristic of a well-designed security architecture is integration of the various solutions. Like any sizable organization, a typical bank runs an assortment of security products. Some protect the network. Others protect individual machines. No matter how sophisticated these solutions are in their own right, they will be more effective if they operate in an integrated manner.

Within a tightly integrated security platform, products alert one another anytime they detect a threat to the network. Ideally, they can respond to the threat in an automated manner as well, which can provide coordinated threat response across the entire attack surface—from the data center to every individual ATM. Coordinated response is particularly important in combating multivector attacks, which target several potential security vulnerabilities simultaneously. As soon as one of the bank’s security solutions detects a known threat, all can work together to prevent entry to any point in the network.
To protect against unknown threats, the security architecture should also incorporate threat intelligence. When security products integrate not only with one another but also with a reputable 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**

A highly automated and tightly integrated security architecture supports compliance with banking and ATM security regulations around the world. The European Union’s General Data Protection Regulation (GDPR), which took effect in May 2018, requires organizations to deploy state-of-the-art systems for securing personal data. 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 automatically, in a coordinated manner, to detected threats.

The Payment Card Industry Data Security Standard (PCI DSS) more specifically encourages organizations to take a comprehensive and integrated approach to IT security. Automation also supports PCI DSS compliance. Among other actions, the rules require financial institutions to ensure their ATMs’ security patches are always up to date.

GDPR, PCI DSS, and countless other regulations in jurisdictions around the world are easier for banks to comply with when their security platform features automated threat detection and response, integration among security solutions, and incorporation of threat intelligence.

**Key Components of ATM Network Security Solution**

To adequately protect ATMs, branches, and its corporate network, a financial institution requires an automated and integrated security architecture that includes the following components:

- NGFWs
- Secure software-defined wide-area networking (SD-WAN)
- Endpoint protection
- Encryption
- Sandboxing
- Centralized management and monitoring
- Security information and event management (SIEM)

**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 not only signature matching but also analysis of contextual information, 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. Using the same vendor for all the bank’s NGFWs can further streamline configuration and ongoing management, as staff need to learn only one interface.

Ensuring that all NGFWs on the corporate network integrate tightly with other elements of the security infrastructure is crucial. A bank’s NGFWs play a key role in collecting information about threats that are 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 response to all threats, both known and unknown.

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 contain the attack and the damage.
Securing SD-WAN Connections

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, such as 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 speed of service and business rules for traffic prioritization. Having the ability to use multiple delivery channels also reduces cost.

The downside to SD-WAN is that it allows WAN traffic to bypass the corporate data center, forfeiting the benefits of the enterprise firewalls and other security processes that operate there. Realizing this, some SD-WAN technology vendors advocate adding NGFWs at the network edge or at various points along the WAN. For networking teams, this adds more complexity and ultimately increases the total cost of ownership (TCO).

A more efficient 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.

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 level of the endpoint.

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. Thus, they do not share threat information with the network’s other security products, nor do they incorporate externally gathered threat intelligence. In contrast, integrating endpoint protection with the network’s other security products strengthens a bank’s overall security posture.

A sophisticated endpoint protection solution automates threat detection and response and integrates into a network-wide security platform. Running such a solution in each ATM helps the ATM server respond effectively if malware were to get past the host-level NGFW.
Encryption Protects Network Traffic

Because hackers are always innovating, even the most robust security environment will likely experience breaches. For added protection in case a hacker does access its data in motion, a bank can encrypt communications. The endpoint protection solution that secures ATMs should encrypt traffic between the ATM server and the host-level NGFW. Then, the ATM-level NGFW should use 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 would 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.

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 posed by the prospective threat. 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 turns out to be a real threat. As a result, it never has a chance to gain access to the broader network.

Financial institutions should look for a sandboxing solution that addresses multiple security functions (e.g., endpoint, web, mail, and file shares). They also need to find a solution that tightly integrates with the other products in their security platform. The sandboxing software should automatically notify other elements of the security infrastructure, in real time, anytime it discovers a new threat. This can prevent multivector attacks approaching an ATM from successfully breaching any other area of the bank’s network, and vice versa.

Centralization of Management and Monitoring

Visibility and centralized control of corporate security processes are key to threat detection and response. To ensure that they are taking the right actions to mitigate threats, security teams need a high-level view into vulnerabilities and attempted attacks networkwide. Thus, ongoing management and monitoring of the security platform are key considerations in the selection of 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 time and reduce the chance of errors. Such capabilities are important for a bank that must efficiently, but effectively, manage security across dispersed ATM locations. This is especially crucial when managing hundreds, or even thousands, of ATMs spread across a country or throughout the world.

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 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.

SIEM solutions that offer file integrity monitoring further enhance threat response for a bank. That is because if malware reaches an ATM, the first action the bank’s network administrator will take will be to verify the integrity of the files on the ATM server. Automating file integrity monitoring across a set of tightly integrated security products streamlines response to any threat. This requires a unified security platform across ATMs, servers, and clients across the entire network.
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 accelerates response to regulatory bodies and streamlines routine compliance audits.

Conclusion

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

Integration and automation reduce the TCO of an ATM network by minimizing manual effort across corporate security processes. When a financial institution can leverage NGFWs and other network security solutions it already has in place, cost savings grow.

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 respond to threats in a coordinated fashion, a bank prepares its ATM network for the known and unknown threats of the future.


2 “India’s Cosmos bank suffers global ATM cash-out attack,” EAST., August 14, 2018.
