

A MULTI-LAYERED APPROACH TO ATM SECURITY



Strategic layers of
security technology
mitigate breaches

With increasing frequency, the media releases in-depth coverage of high-profile data breaches in which consumers' personal data is seized through sophisticated malware designed to clean out bank accounts and destroy identities. The fear and mistrust these crimes breed in the minds of consumers is only equaled by the damage done to the brands and reputations of the financial institutions affected. Once such a breach occurs, rebuilding consumer confidence and loyalty can take years. What's more, the costs to financial institutions related to card reissuance and reimbursement is estimated to average up to \$150,000 per incident.

ATM attacks come from several sources both internal and external, including:

- Virus attacks
- Hacker attacks
- Phishing
- Internal breaches
- Third-party service provider attacks

As a result, ATM security is one of the most technically challenging areas of a financial institution's operations. To ensure the most effective

coverage from these types of threats, financial institutions must implement a comprehensive multi-layered security approach that includes hardware, software and services designed to protect against all breaches, today and in the future. Software or hardware alone can't do the job. Without complete protection providing layer upon layer of security, financial institutions could spend exorbitant amounts of capital to get disappointing – and damaging – results.

To assist financial institutions in implementing a high level of multi-layered protection that incorporates some of the industry's toughest defenses against ATM fraud, Diebold developed its comprehensive Security Protection Suite. The suite offers protection packages for each major threat category—fraud, physical and logical. Diebold's Logical Security Protection is designed with strategic layers of essential security technologies that help prevent dangerous breaches, protecting all the vulnerable endpoints in an ATM network while monitoring, tracking and logging suspicious activity. It offers a broad net of multi-layered protection using cutting-edge tools, all of which can be managed by the financial institution or Diebold. Implemented separately, this level of protection could be overwhelming, not to mention time-consuming, for financial institutions.



INNOVATION DELIVERED®

And these days, adopting effective security is not optional. The Payment Card Industry Security Standards Council developed Data Security Standards (PCI DSS) mandating specific security measures for protecting stored, processed and transmitted cardholder data. The following solutions can help financial institutions meet these new requirements, saving them from costly fines, while protecting consumers' critical assets, as well as their own.

Close the doors on malware

Cyber thieves will stop at nothing to gain access to sensitive data. That means strong firewall and intrusion detection is a critical layer of protection that controls traffic in and out of the network. One of the industry's toughest software solutions is ATM Endpoint Protection by Symantec®. Its standalone firewall agent comes standard on all Diebold Opteva® ATMs. Endpoint Protection locks down the ATM at every point of vulnerability, providing:

- Comprehensive protection that includes a blend of standard-setting technologies to stop existing and unknown threats before they penetrate the network.
- Network threat protection through the industry's strongest firewall and blocking capabilities that prevent malware from entering the ATM system.

Without the proper guards, access also can be gained at the physical ATM. That means financial institutions need strong device-level security to safeguard against network breaches that can devastate an ATM fleet. Diebold's Standard ATM, in managed server mode, includes unmatched USB blocking software that protects ATMs against unauthorized devices being attached to the ATM. USB blocking offers an additional layer of security to help impede unauthorized software from being loaded onto the ATM and guards against unauthorized information removal from the ATM.

Because malware never sleeps, an additional level of security can be achieved with Advanced Endpoint protection that works at the firewall and beyond in a managed mode, protecting ATMs by constantly monitoring, analyzing and authenticating sources attempting to connect to the ATM. Symantec's

software doesn't stop there. It also offers best-in-class malware protection that includes antivirus and antispyware protection, providing:

- Proactive protection through threat scanning that tracks behaviors of unknown applications to enhance detection and reduce false positives.
- Threat landscape intelligence by leveraging the Global Intelligence Network to deliver an unparalleled view of the entire Internet threat landscape, resulting in actionable protection and peace of mind against evolving attacks.

Effective verification and authentication

It's a balancing act. Securing access at the ATM against known threats is one thing, but threats by trusted providers can deliver a devastating blow. Financial institutions must allow third-party providers access to their ATM fleet, which unfortunately invites insider threats. But now, financial institutions can implement controls beyond simple trust. With Diebold's secure service token, institutions can securely authenticate and validate Diebold technicians assigned to service their fleet. ValiTech™ uses two-factor authentication through a password and a secure USB device owned and used exclusively by that technician. This technology not only delivers an additional layer of protection for financial institutions through access control, it also provides a detailed audit trail documenting each time a technician is granted access and records all menu activities executed during the service call.

Password administration helps lock the front doors

Obviously, securing all access to the ATM is critical. And sometimes the least complicated efforts pay off with immeasurable benefits, such as consistent password management. Every ATM is delivered from the manufacturer with two passwords. The restricted user account has a hardened, random password not known by the manufacturer. The second account is the administrative account, which has a known default password that should be changed immediately by the financial institution. Unfortunately, leaving the administrative default password in place is a common

Through the regular monitoring and review of a comprehensive multi-layered security program, financial institutions can meet threats head-on – internal or external, physical or logical – that arise, strengthening their bottom line and ensuring consumer trust.

practice although highly unsafe: it's comparable to leaving the store unlocked after everyone leaves for the night. And using default passwords is the easiest way for a hacker to access the ATM's internal network. Diebold strongly recommends that the default administrative password be immediately changed when the ATM is put into service and that passwords are changed on a continuing basis at least every 90 days. A professional services provider such as Diebold's Professional Services team can assist financial institutions in implementing effective password management by connecting the ATM to an active directory environment.

Protection from the inside out

Helping protect ATMs against unauthorized access to critical ATM resources is essential. Diebold leverages Wave System Corporation's industry-leading security software tools for Opteva, to help financial institutions gain an embedded layer of protection that ensures only authenticated, certified platforms to communicate with critical ATM devices, thus strengthening the integrity of the terminal.

Wave's software enables Diebold's ATM applications to directly interact with an important security hardware module within the ATM known as a Trusted Platform Module (TPM). The TPM is industry-standard security hardware and is included in the computer driving Diebold ATMs. TPMs provide encryption, authentication, non-repudiation and integrity capabilities that can be used to maximize the security of the system. The TPM is a powerful security tool because information is protected by hardware, making it more secure from external software attacks and physical theft.

Secure consumer data across the wires

Bank account data is under constant siege. Cybercriminals continuously work to design new Trojan horse programs to capture consumers' valuable information during data transmission from the ATM to an authorized system. A breach at this level can result in massive loss of consumer confidence,

costing a financial institution its consumer base, not to mention the capital associated with efforts to repair the damage. That's why it's imperative to implement a strong encryption program that scrambles data with each keystroke, ensuring the information can't be compromised as it is transmitted. Diebold's Agilis® software supports Secure Sockets Layer (SSL) encryption technology, which does just that. A professional services provider such as Diebold can assist financial institutions in implementing effective protection across their network.

Immediate software updates

With all the necessary security software working interactively across a financial institution's ATM network, managing and maintaining the system's integrity can be a significant drain on resources. That's where high-level security patch deployment comes into play. Diebold's Software Deployment solution validates and downloads the most up-to-date security patches across an institution's system, while identifying and tracking software versions and patches. This helps categorize and manage critical and noncritical systems to help institutions know exactly what's at work throughout their system.

Putting it all together

Enlisting a professional security services provider such as Diebold for the management and monitoring of all security events and software across the ATM channel can assist financial institutions in staying compliant with PCI DSS requirements and in providing additional layers of security to help protect consumer data.

For more information about Diebold's comprehensive multi-layered security approach, visit www.diebold.com.

Contact Information:
Diebold, Incorporated
P.O. Box 3077
North Canton, Ohio
44720-8077

800.999.3600 USA
330.490.4000 International
e-mail: productinfo@diebold.com
www.diebold.com

© Diebold, Incorporated, 2010.


INNOVATION DELIVERED®