

## MULTI-LAYERED SECURITY FOR OPTEVA®

Diebold's complete ATM solution offers comprehensive defenses to help mitigate fraud

Automated teller machine (ATM) security is one of the most technically challenging areas of a financial institution's operations and choosing the most effective security program can be overwhelming. Threats at the self-service channel come in many forms and are increasing in frequency and sophistication. A single breach at the ATM can devastate an institution's brand and has been estimated to cost up to \$150,000 per incident for card reissuance and reimbursement.

### Multi-layered security approach:

- Ensures optimal protection across your ATM fleet
- Helps safeguard your customers and your bottom line
- Locks down vulnerable endpoints
- Deploys comprehensive protection

To ensure the most effective coverage, implement a comprehensive approach that includes hardware, software and services designed to protect your ATM fleet against all breaches, today and into the future.

Powered by Agilis®, Diebold's high-performance software platform, and supported by award-winning services, Diebold's Opteva® ATMs are designed with built-in layers of essential security technologies to help prevent dangerous breaches, while strategically monitoring, tracking and logging all suspicious activity. Diebold's software, hardware and support offer the complete package to help you defend against malware and protect customers' critical transaction data by implementing multiple layers of security technology.

### ATM logical protection

#### Symantec® Endpoint Protection

To help financial institutions lock down vulnerable end points and operate safely and securely, Symantec Endpoint Protection Stand Alone Agent v.11.0 comes standard on all Diebold Opteva® ATMs. It offers advanced protection through essential technologies designed to prevent such malware attacks as viruses, worms, Trojans, spyware, adware, bots, zero-day threats and rootkits, all with a single agent and single management console.



INNOVATION DELIVERED®

### Trusted Platform Module

One of the industry's most powerful security tools, the TPM is hardware included in the computer driving Opteva® ATMs. The module helps protect valuable data, making it more secure from external software attacks and physical theft. TPMs provide encryption, authentication, non-repudiation and integrity capabilities that help maximize the security of the system, providing protection from the inside out.

### Encrypting pin pad v.5

Opteva® employs the most advanced encryption technology at the PIN pad through triple Data Encryption Standard (DES) protection, safeguarding your customers and your bottom line. With triple DES the PIN is encrypted in three steps, rather than the older single DES, which uses a single secret key to encrypt the PIN at the ATM and to decrypt the PIN after it is received by the processor. Opteva's EPP v.5 detects tampering and immediately locks down the system and reports activity the moment it senses trouble.

### ValiTech™

The Opteva® Agilis® ATM software includes a built-in feature that offers financial institutions a more secure login methodology that authenticates and validates Diebold technicians assigned to service their fleet. The ValiTech™ Secure Service Token uses two-factor authentication through a password and a secure USB device owned and used exclusively by that technician. ValiTech also provides a detailed audit trail documenting each time a technician is granted access and records all menu activities executed during the service call.

### OpteView®

Diebold's OpteView provides a secure remote-service solution at the ATM that initiates a remote session to troubleshoot if an issue is detected. OpteView can either fix the ATM remotely or dispatch an engineer with the exact information and part needed to correct the problem the first time. With OpteView's built-in data-capture technology, a complete audit trail is available, which helps to ensure that data has not been compromised and outsiders have not gained access.

### USB blocking

ATMs require strong device-level security to safeguard against network breaches. Diebold's Agilis® helps protect ATMs against all unauthorized devices from being attached to the ATM. Through standard-setting software, Agilis® USB blocking prevents software from being loaded onto the ATM and guards against information being removed from the ATM via USB ports, with the exception of authorized devices by the financial institution.

### Secure Sockets Layer encryption

Effective encryption of cardholder data is a critical layer of protection at the ATM. Agilis® enables the deployment of Secure Sockets Layer (SSL) encryption technology, scrambling transmitted data to help protect all communication between the ATM and the host network. It also guards against hackers by helping prevent data from being deciphered for unlawful purposes. Diebold can work with your institution to set up SSL encryption to meet industry requirements.

In today's climate of increasingly sophisticated attacks against the self-service network, Diebold's multi-layered security for Opteva® offers the highest available level of protection, incorporating some of the industry's toughest defenses against ATM fraud. Integrating cutting-edge hardware, software and award-winning services, Diebold's layered approach casts a broad net of protection to help financial institutions deploy a level of technology that helps protect their customers, their assets and their brand.

Contact Information:  
Diebold, Incorporated  
P.O. Box 3077  
Dept. 9-B-16  
North Canton, Ohio 44720-8077

800.999.3600 USA  
330.490.4000 International  
e-mail: [productinfo@diebold.com](mailto:productinfo@diebold.com)  
[www.diebold.com](http://www.diebold.com)

© Diebold, Incorporated, 2010.  
File No. 98-130.