Solution Brief

BROADCOM®
SOFTWARE

Host-based Protection for ATMs

Introduction

Automated Teller Machines (ATMs) are one of the most high-value customer touch points in the banking industry. As customers perpetually demand extra services and more user-friendly interfaces, banks demand more cost-effective solutions for interfacing with customers. ATMs require increased flexibility to meet customer expectations and are becoming more capable and connected than ever before.

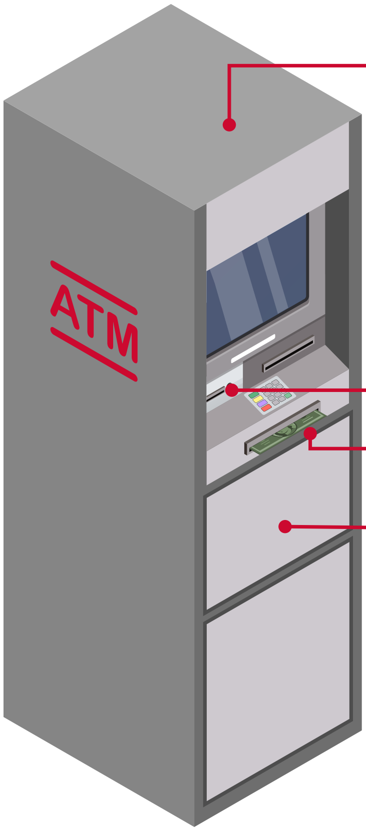
Providing a direct interface to cash inevitably makes ATMs a target in numerous sophisticated ways—with new methods being regularly exposed. Attack methods extend from physical (such as skimming and pin cameras) to virtual through malware. Above all, the customer must trust the ATM. Assuring integrity from the very start of the supply chain through to the installers and operators is essential.

Banks and ATM operators must protect their ATMs and meet their compliance obligations for operating in a heavily regulated industry sector. But doing so can be challenge. ATMs can be considered a single-use device—they have a dedicated function and run a specific application with predictable input and output. Yet ATMs are frequently built using common operating systems such as Microsoft Windows, capable of so much more than required. They are subject to vulnerabilities and often exploited in similar fashion to a laptop or workstation.

Symantec™ Critical System Protection

Symantec Critical System Protection can help. It provides a policy-driven, host-based, least-privilege approach to endpoint security and compliance.

Symantec Critical System Protection has two enforcement components that can be independently activated on ATM systems: prevention and detection. The prevention component has proactive enforcement rules that stop malicious activity before it occurs and



Device	Possible attacks
ATM Computer	• Connection of USB devices • Connection to hard drive • Boot mode modification
Card reader decodes data from bank cards	Card data interception
Cash dispenser issues banknotes from the safe	Black box
Network equipment connects the ATM to the processing center and remote admin. servers	• Interception of network traffic • Spoofing of processing center • Attack on available network services • Attach on network devices • Connection from the bank's internal network • Spoofing or hacking of software update server

Symantec Critical System Protection Capabilities

Protection

- Intrusion Prevention
- Intrusion Detection
- System Hardening
- Application Allow-listing
- Application Sandboxes
- Vulnerability and Patch Mitigation

Detection and Compliance

- Real-Time Monitoring and Auditing
- Intrusion Detection
- File Integrity Monitoring
- Configuration Monitoring
- Tracking and Monitoring of User Access
- Logging and Event Reporting

Beyond Host-based Protection

Controlling what can and cannot be run on a machine is only part of the ATM protection story. Best practices like code signing and protection, secure management, authentication, and encryption all play a part in a robust ATM security strategy.

To find out more about protecting ATMs and single use devices, visit broadcom.com/products/cyber-security/endpoint

the detection component monitors for system activity as it occurs and can trigger event-based actions. Both components provide granular control over logging using policy settings to give visibility into actionable events as well as the efficient management of high-volume events necessary for regulatory or forensic purposes. Thus, in combination, the components provide unique capabilities to both secure a system and address regulatory compliance requirements. This includes regulations such as PCI-DSS that requires companies to deploy file integrity monitoring for critical system and application files changes. Detecting that an important operating system binary like svchost.exe was recently modified is very different from preventing the modification in the first place. Symantec Critical System Protection lets you configure and use both detection and prevention as needed to address your auditing, compliance, and security requirements.

System Hardening and Application Control

Controlling which applications can run on your ATM devices is one of the most vital steps to protecting against unauthorized access and attack. Symantec Critical System Protection policies provide thousands of pre-built rules that comprehensively monitor and harden the operating system of enterprise systems and require minimal tuning. Memory controls detect buffer overflows and unusual memory allocation and permissions, complimenting an effective device hardening strategy. Single-use devices such as ATM terminals perform predictable functions, meaning the device should always be in a known state, with known applications performing known behavior.

Symantec Critical System Protection can be configured to enforce application allow-listing, ensuring only predefined programs can be executed with specific attributes controlling the manner in which they are called. Furthermore, program execution can be contained within a sandbox, allowing strict control over the behavior of the application. This is particularly useful where operating system permission levels allow unnecessary actions to be carried out. Privilege de-escalation can be configured, ensuring that even an admin user account can have its ability constrained to the minimum functions necessary for the device purpose.

Adding another layer of security to your defenses, Symantec Critical System Protection provides rule-based, system-level—as well application-level—firewalls to block network-based attacks against your ATMs. The firewall lets you restrict which applications on the ATM systems can communicate on the network and which ports they can use. To circumvent network restrictions and application controls, some cybercriminals will try to steal credit card data through physical access to an ATM. As ATMs become more advanced with computer-like characteristics, the methods for unauthorized physical access often increase in sophistication. Symantec Critical System Protection enables you to block and granularly control devices connected to your ATM systems' communication interfaces, such as USB ports. It can prevent all access to a port or only allow access from certain devices.

Intrusion Detection

The Symantec Critical System Protection detection policies monitor files, settings, events and logs, and report anomalous behavior. Features include the following:

- Sophisticated policy-based auditing and monitoring
- Log consolidation for easy search, archival, and retrieval
- Advanced event analysis
- Response capabilities

To further harden the device, it provides a combination of file integrity monitoring and registry integrity monitoring.

Deployment

Symantec Critical System Protection can be deployed in managed or standalone modes. This is particularly useful for device manufacturers who create an out of the box security policy for their product, ensuring the device is adequately hardened from the moment it is activated. Manufacturers, integrators, and device operators may choose to deploy the agent after market on devices being newly deployed or previously installed. Administrators can opt for configurations where the agent communicates with the management console for policy updates and reporting, providing real time visibility of your security posture.

Symantec Critical System Protection also supports modular installation of components, deploying only the code required to perform the protection and/or detection functions as defined in the agent configuration. This allows manufacturers and device operators to efficiently deploy in resource-constrained environments.

BROADCOM®
SOFTWARE

For more product information: broadcom.com