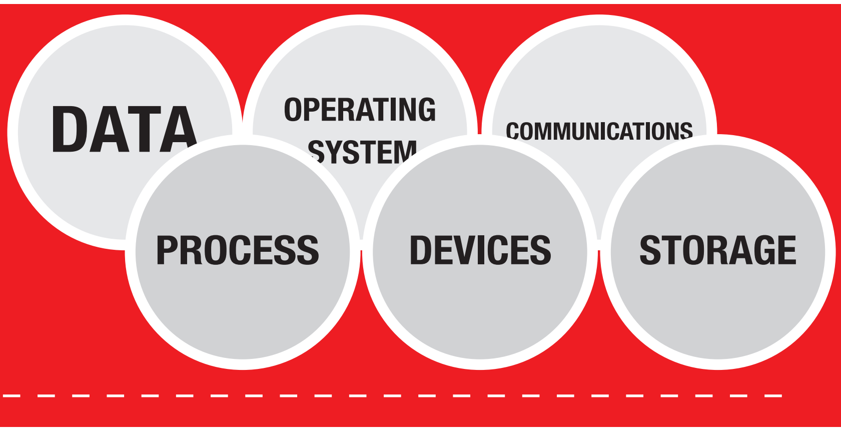
The ultimate ATM Security Solution

Checker ATM Security

Are your bank's ATMs and Kiosks properly protected?

CONSULTANCY | INSTALLATION | ONLINE SUPPORT | ONLINE TRAINING

If not, they might already be **under attack without you knowing it**. Now is the time to check out *Checker ATM Security* and find out just how quick and easy it is to protect your ATM and kiosk network.



DATA

OPERATING SYSTEM

COMMUNICATIONS

PROCESS

DEVICES

STORAGE

Checker ATM Security currently protects more than 150,000 ATMs in 33 Countries.

Security solutions that protect ATM's
from hackers and cybercrime

SPL GROUP

Checker ATM Security features

Checker preserves your ATM application software, libraries and operating system integrity, leveraging cryptographic signatures and Hard Disk Encryption designed specifically for ATMs. *Checker ATM Security's* state-of-the-art technology effectively controls the execution of legitimate processes and prevents malware infection using thorough whitelisting protection combined with application level communications firewalling. Supervises the usage of ATM peripherals such as keyboards, Graphical Operator Panels and USB drives to stop any possible attack; prevents data sniffing or manipulation by enabling VPN-based communication encryption and guarantees PCI-DSS compliance by preventing card data storage in the clear, among many other features.

Centralized, comprehensive security administration and monitoring, ranging from operator alerts to management-level dashboard, is built on top of *Checker ATM Security's* best of breed cyber protection technology to ensure this amazing combination of security features can be properly, easily and securely managed in large, diverse multi-vendor ATM networks in complex organizations.

Operation System Protection

Integrity Protection

Integrity validation of critical operating system processes and resources.

Any detected alteration will be reported.

Resources Use Protection

Use of operating system resources (registry, libraries and drivers) is granted or denied on a process-by-process basis.

Non-permitted use of resources will be blocked and reported.

Multi-version support

Supports different versions, fix packs and service packs of the operating system deployed in an ATM network.

Integrity validation supports different versions of the same (authorized) program or resource.

Devices Protection

Plug & Play Hardware Protection

Detects the connection of new hardware and allows or denies mounting.

Unauthorized devices will be blocked and reported.

Device Access Control

Use of connected hardware filtered on a process-by-process basis.

Non-permitted use of connected hardware will be blocked and reported.

USB Flash Drives Control

Reliable control of authorized USB drives for easy, yet secure maintenance. Supports content encryption and authentication of authorized USB drives.

Data Protection

- **File System Protection**
  Access to local files and directories is granted or denied on a process-by-process basis.
  Illegal access to restricted data will be blocked and reported.

- **Integrity Protection**
  Integrity validation of sensitive data files.
  Data illegally altered will be blocked and reported.

- **DLP Capabilities for ATM**
  Detection of track2 data storage in the clear.
  Writing data that follows a track2 pattern will be reported.

Communications Protection

- **Firewall**
  Filtering of incoming and outgoing communications by protocol, port, address and local process, provides high level firewalling functionality matching the process whitelist.
  Non-permitted communications will be blocked and reported.

- **VPN**
  Checker-managed IPSec tunneling enables encrypted communications between existing applications in ATMs and servers with no need to modify the applications.
  Permitted communication will be transparently tunneled.

Storage Protection

- **Full Hard Disk Encryption**
  ATM hard disks encryption can be fully managed from the *Checker ATM Security* console, including remote commands to encrypt or decrypt ATM disks.

- **Zero Downtime**
  The encryption can be commanded from the server and the disk can undergo the encryption process while the ATM keeps operating. Therefore, there is no relevant downtime associated to the encryption of an ATM network.

- **Smart Environment Detection**
  Decryption is only possible for a specified ATM environment.
  The ATM environment is defined as a configurable combination of identifiers associated to the ATM hard disk, the ATM hardware and the ATM network.

Process Execution Protection

White Listing

List of permitted and approved processes. *Processes not included in this list will be blocked and reported.*
Self-learning feature allows whitelist creation in a matter of minutes.

Integrity Protection

Integrity validation of whitelisted process and its resources.

Processes or resources illegally altered will be blocked and reported.

Resources Use Protection

Use of local resources (files, directories, libraries and drivers) filtered by whitelisted process.

Non-permitted uses of resources will be blocked and reported.

Java Resources Loading Control

Detailed list of all resources loaded by the Java Virtual Machine (this feature is critical but not provided by most whitelisting solutions).

Loading of non-permitted Java resources will be blocked and reported.

smart environment detection WINDOWS BLOCKING

AUTO LEARNING DEVICES IPSES

security dashboard HTTPS JAVA MULTIVENDOR

SIGNATURE

HARD DISK ENCRYPTION FIREWALL checksum

TRACK 2 WHITELISTING SERVER

INTEGRITY PREVENTION

PCI-DSS ACL CENTRALIZED

VPN LOW-FOOTPRINT

MONITORING ALARM SECURITY

We invite you to attend one of our technical
or information sessions by emailing sales@spl.net