WHY checker?

**checker ATM Security** is the first security product specifically designed for ATMs and Kiosk infrastructure. **checker** will help you protect your ATM from logical fraud while meeting applicable PCI-DSS requirements quickly and effectively.

**checker ATM Security** assures high-security in ATM environments, rejects unauthorized network connections, restricts access to sensitive information, controls unauthorized devices from being connected to the ATM and blocks any malicious software. Its innovative technology combines application level firewalling, state of the art whitelisting, advanced integrity verification and self-learning capabilities into ATM-specific security policies which are enforced while ATM reliability and performance remain unaffected. **checker** includes centralized monitoring and management functionalities, to complete a unique product with just one single target focus: to prevent your ATM infrastructure from logical fraud.
The introduction of Microsoft Windows and Linux operating systems in financial self-service networks and the use of IP networks as communication mechanisms have resulted in higher security risks due to the vulnerabilities common to open systems. checker mitigates these risks in a simple and effective way, creating a secure communication and execution environment, managed and monitored centrally.

**HOW DOES IT WORK?**

Each ATM fits a checker agent capable of enforcing a Security Policy. This policy contains a list of rules that encloses exhaustive definition of authorized processes, system resources (files and libraries), external devices and permitted communications. This set of rules is created from a checker server by means of state-of-the-art self-learning technology that detects all actions attempted in a regular ATM and proposes adequate rules that will allow you to harden any ATM within minutes.

checker server also enables security monitoring and administration of the ATM network. Communication between the checker agents and the checker server is mutually authenticated and end-to-end encrypted, enabling the ATM’s security to be remotely managed and also ensuring secure, real time notification of security events detected in the ATM.

**TECHNICAL SPECIFICATIONS**

**checker agent:**
- Compatible with Windows NT SP6, Windows XP SP1, SP2 & SP3 and Windows Embedded XP, Windows 7 32 bits.
- Minimum resource consumption.

**checker server:**
- 100% Java application under standard J2EE.
- Support for IBM Websphere Application Server, Oracle Weblogic Application Server and JBoss Application Server.
- DBs supported: MySQL, IBM DB2, Microsoft SQLServer and Oracle.
- Easy integration of centralized event logs with third party software (syslog, HP OpenView, ArcSight, etc.).
- Real time monitoring.
- Advanced web-based user interface.

**MAIN FEATURES**

**checker in the ATM:**
- Policy-based control of process execution and resource access.
- Integrity verification of binary (executable) files and system resources using digital signatures.
- Control and verification of the resources used by the Java virtual machine (JVM): Java libraries, native and class libraries, using digital signature.
- Control of incoming and outgoing communications, providing source and destination filtering for addresses and applications.
- Control of read & write operations over the file system and the windows registry.
- Filtering of key pressed events from a connected keyboard.
- Control and verification of the libraries and drivers used by ATM applications.
- Controls unauthorized devices from being connected to the ATM.
- Control of card magnetic stripe information being written in ATM storage.
- Security incidents reports in both local log and server log.

**checker in the Server:**
- Real time administration of the ATM network´s security.
- Administration of network topology, pooling the ATMs into any number of nodes.
- Real time monitoring of the threat level in each ATM or node with access to security incidents reported at ATMs or node level.
- Generation of summary reports on the incidents reported in a given period of time.
- Self-learning assistance for definition of security rules (processes, registry and file system resources, incoming and outgoing communications, JAVA resources, etc.).
- Role-based access to console.
- Internal software distribution tool for checker agent updating.
- Remote ATM reboot capability.