

Vynamic™ Security



Self-service device protection from
break-ins and other attacks

Vynamic™ Security

Self-service device protection from break-ins and other attacks

Vynamic™ Security is a solution which ensures a comprehensive approach to the protection of ATMs, payment terminals, automated teller safes and other devices from all types of break-in, hackers' attacks and other threats. The modular system enable to close the most vulnerable parts of the terminal infrastructure of banks and other organizations.



FUNCTIONS AND BENEFITS

■ Comprehensive approach

The use of progressive IT-infrastructure security methods, such as trusted software lists (whitelisting) and a restricted environment of each authorized process (sandboxing) ensures a comprehensive approach to the security of terminal networks.

■ Flexible implementation

The solution constitutes three independent modules: Hard Disk Encryption, Intrusion Protection and Access Protection. Each of these modules are used against a specific threat type.

■ Multi-level security

The architecture of Vynamic Security entails multiple layers of protection. In case of first level intrusion, automatic scenarios would be launched to ensure a complete progression halt of the attacker.

■ Support for devices from most manufacturers

Vynamic Security is a multi-vendor solution which can be implemented to protect terminals made by various manufacturers. This allows to consolidate terminal service processes and reduce the total cost of ownership.

■ Ease of use

The software automatically handles manual updates of antivirus databases and system scans. Thus, the solution considerably simplifies the terminal network administration processes and lowers the cost of ownership.

■ Compliance with security standards

Solution is compatible with operating systems Windows XP, Windows 7 and Windows 10. It fully conforms to PCI DSS security standards and could be adapted to the requirements of different regulators.



APPLICATION

■ Hard Drive theft

Data located on the ATMs hard drive is encrypted through the Hard Disk Encryption module ensuring device operation in only specified software/hardware environments.

■ Intrusion attempts

The Intrusion Protection module eliminates various software vulnerabilities. The current module provides access control for users, processes and applications making ensuring operation only at necessary access levels with specifically required resources.

■ Internal fraud

The Access Protection module allows to establish a strict and absolutely controlled system for providing rights to different user groups: Service Engineers, System Administrators and other staff.

