Application Scenarios



ATM Machines

ATMs are very attractive targets for attackers because they contain cash and manage sensitive information like credit / debit card and PIN numbers, while being in unattended or insufficiently surveilled environments.

The wide variety of legacy hardware and software in ATM networks, coupled with a lack of proactive upgrade policies derived from technical and economical constraints make these networks inherently vulnerable environments.

In this scenario, cyber-criminals are extremely agile and innovative in producing new types of targeted logical attacks, which are much more cost effective than traditional physical attacks.

Control Systems In Critical Infrastructures

Automation and control systems in critical infrastructures are increasingly dependent on remote communications and interconnection with IT infrastructure, inheriting some of its risks and vulnerabilities.

A cyber-attack on control systems can cause tremendous damage, from massive denial of basic services to putting both infrastructure and people in potential danger. Therefore, the highest security standards should be applied to these sensitive systems.





Point of Sales Terminals

The nature of Point-of-Sale terminals, that handle sensitive data like card numbers and PINs, makes them very vulnerable to targeted attacks or fraudulent actions.

A whitelisting-based control of the authorized applications or hardware devices allows users to raise the level of confidence in the security of this equipment.

GRGBanking

ATMIA
Education + Advocacy + Connections

inFinite Intelligence

GRGBanking Equipment Co., Ltd.
9,11 Kelin Road, Science City, High-tech Industrial Development Zone,
Guangzhou, China 510663
Tel: +86-20-6287 8545
Fax: +86-20-6287 9976
E-mail: atm@grgbanking.com

Copyright © 2025 by GRGBanking Equipment Co., Ltd.
All rights reserved.

Specifications are subject to update without prior notice.
Please consult GRGBanking or its representative for the latest information.

https://global.grgbanking.com

V202509

GRGBanking

GRGEsm Pro

Endpoint Security Management Platform

GRGBanking's endpoint security management solutions (GRGEsm) is a centralized and modular OT cybersecurity platform that offers a comprehensive set of functionalities to protect, monitor and control your critical devices.





Understand Your Environment

Critical devices provide essential services that need to be available 24/7, 365 days a year. Keeping them secure is paramount to success, as cyber-attacks on critical devices are highly targeted and designed to spot any embedded software vulnerabilities. The consequences of not maintaining such technology properly range from financial fraud to business continuity interruption or even sabotage.

By putting an effective OT cybersecurity strategy in place, based on the right set of protection technologies, it is possible to secure critical devices without disrupting operations or risking non-compliance with sectorial regulations.

GRGEsm Pro is an integrated OT cybersecurity solution that provides the most advanced set of countermeasures to protect and respond to the new generation of cyber-attacks based on malware. It centralizes policy definition and operations at a single point allowing you to protect thousands of critical devices without affecting business continuity and favoring compliance with cybersecurity regulations or corporate policies. (PCI-DSS, NERC...).

Protecting Critical Devices

GRGEsm Pro is a perfect-fit solution to ensure high security standards in fix-purpose devices that are critical to business, such as ATMs, point of sale terminals or critical infrastructure control systems.

- Benefit from award-winning, vendor-agnostic technology specifically designed for critical devices.
- Protect your critical systems from malicious and fraudulent activities, with the most comprehensive layered protection model.
- Easily implementable to quickly comply with your security policies, with minimal performance impact on your devices.
- Save time and money thanks to remote and centralized security operations from a single GUI.
- Block, detect and solve security incidents that may arise from your assets.
- Get real-time visibility into the hardware, software and users installed on your devices, and stay in loop with any changes.
- Execute customized remote actions on your devices in a secure and controlled environment.
- Adapt visibility and permissions to the specific needs of the different operations teams.

Holistic Security Model

GRGEsm Pro is a modular platform that offers a comprehensive set of features to protect and monitor your critical devices, adding an extra control layer that allows users to run custom remote actions to investigate or react to potential incidents.

