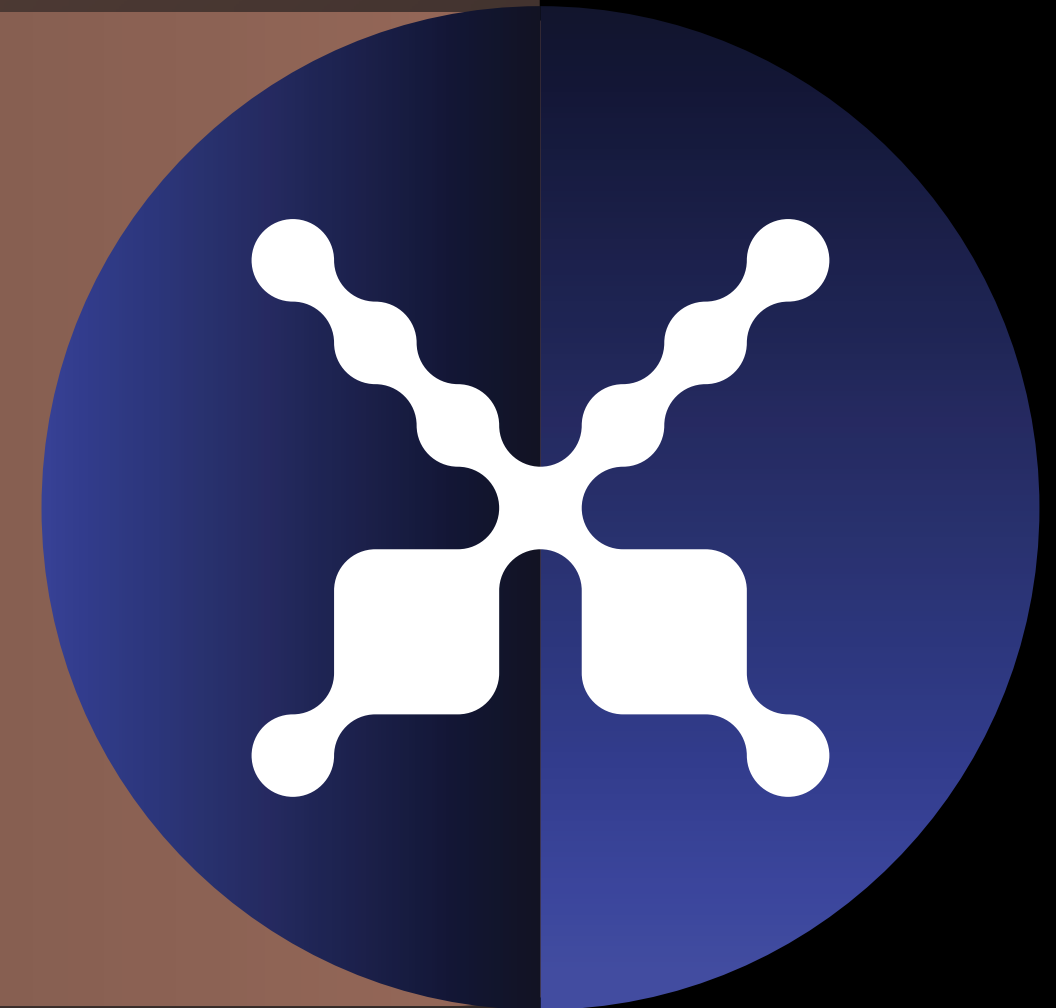


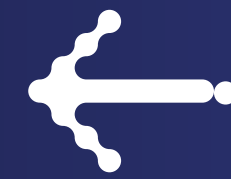
EXECUTION MANAGEMENT SYSTEM

EEMS



Execution Management System

which is abbreviated as EMS, is a native system to prevent the execution of infected and unauthorized files, control the access level to necessary Windows extensions, and control equipment connected to the system.



Today, various methods and software are used to monitor and control security, and information exchange, preventing the penetration and proliferation of computer malware. Despite different software and solutions, there are still ways for all kinds of threats to penetrate. Due to the lack of detection of all new malware by antivirus software and the possibility of running unauthorized software at the level of network systems, the use of software that prevents executing unauthorized files is a priority and necessity.

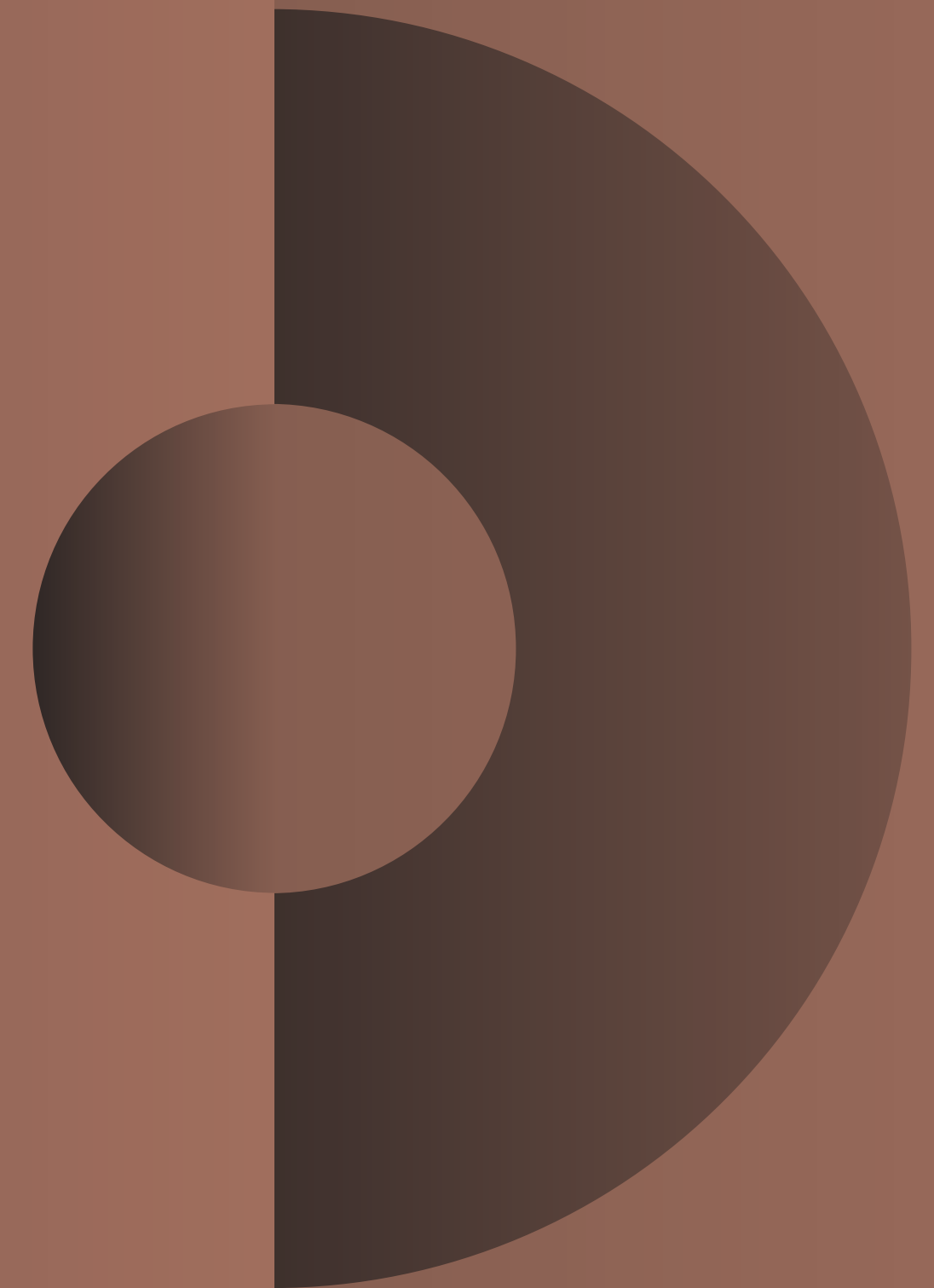
Spara native file management system (EMS) has been designed and implemented to increase the security factor of the systems in the network. The main functions of this system include preventing the execution of infected, unauthorized, and unknown files, controlling the level of access to 48 crucial Windows extensions (executable files, java, script, Powershell, etc.), as well as controlling the devices connected to the system (Network clients and ATMs).

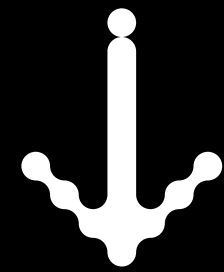


EMS function for ATMs

The security monitoring and control issue in ATMs is so vital that the unauthorized withdrawal of banknotes (physical and non-physical attacks) by abusers is an undeniable and ongoing phenomenon. One of the latest attacks used by the attackers is removing the ATM camera and connecting the keyboard (and other devices such as USB) through the interface to the camera cable so that they use their techniques to withdraw banknotes.

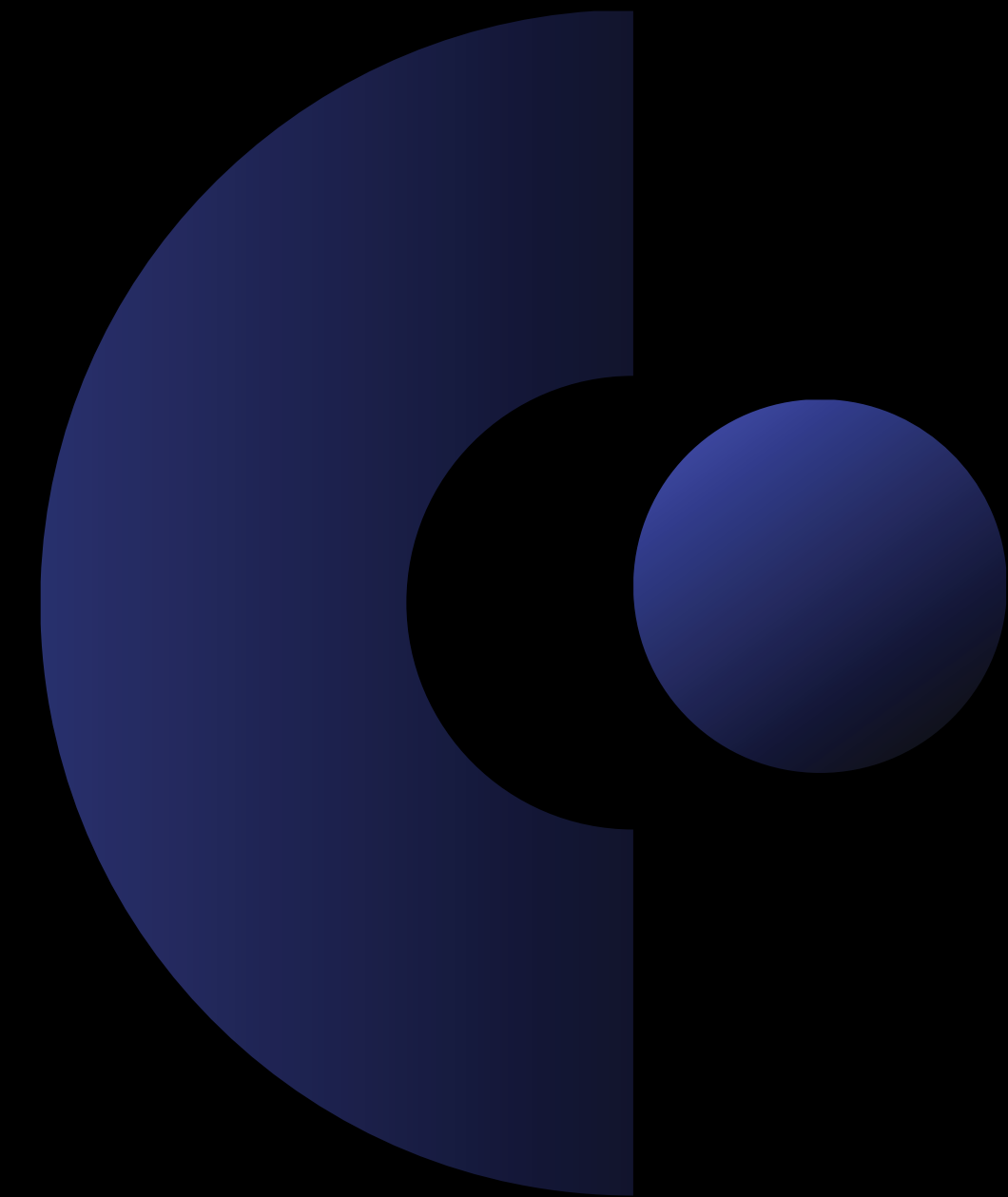
According to European Association for Secure Transactions (EAST) research, ATM hacking in Europe in the first half of 2020 increased by 269% over the same period last year. Based on the statistics and the fact that almost most ATMs have been hacked, ensuring these devices' security is one of the necessary measures for every bank and financial institution. One way to maintain security is to control and check the different devices that are connected to ATMs and the system in general.





The most important reasons for ATMs' weakness in cyberattacks are:

- Nonuse of up-to-date windows (use of Windows XP and 7 in ATMs)
- Nonuse of security software such as antivirus (due to slowness and overload in ATMs)
- Nonuse of software that prevents unauthorized files and devices from running and connecting

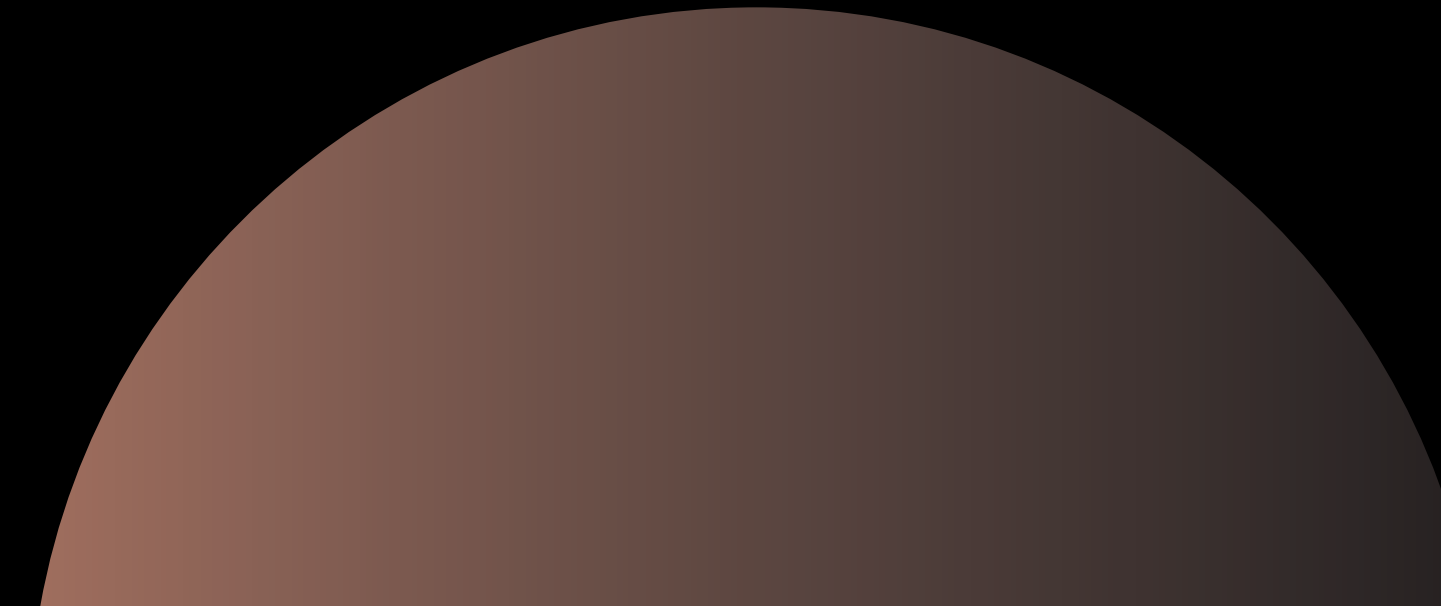




Two significant differences between EMS security solutions and similar products in ATM protection:

- Most security software, most notably antivirus, will be disabled in SafeMode. Abusers highly notice this weak point in ATMs. By disabling or deleting the antivirus in this environment, they enter the Windows environment (non-SafeMode) and by running their file, they withdraw the banknote illegally. In this case, the advantage of the EMS system is that it also runs in SafeMode and performs its policy control process, which includes preventing the execution of unauthorized files and disabling unauthorized devices.
- They are deactivating all types of mice and keyboards connected to the ATM and their dependence (activation) on the connection of approved flash memory in the server policy (each flash has a unique serial number). By connecting an authorized flash memory by the nurse (support expert), the mouse and keyboard are activated, and by leaving the flash memory, the mouse and keyboard will be deactivated. The connection and disconnection report of all authorized and unauthorized devices will be sent to the server panel.

Features of Spara's EMS

- Installing and activating the client version (EMS Agent) by the server panel
 - Preventing the execution of unauthorized files (different types of computer malware, infected files, etc.)
 - Preventing the execution of unauthorized software and essential parts of Windows (such as Telnet) even for users with an admin access level
 - Licensing software installation by a secure and approved setup
 - Control of devices connected to the system (mouse, keyboard, USB, external hard drive, mobile, Bluetooth, WiFi, etc.)
 - Sending a report of unauthorized files and devices connected to the system
 - Grouping systems to facilitate updating the list of authorized files
 - System security protection in SafeMode and network outages (no connection to a server)
 - Self-defense system for preventing unauthorized user activity
 - Notification of unauthorized access to files and devices with SMS
 - Non-occupation of system resources (CPU/RAM) due to monitoring software and user activity
- 

Benefits of Spara's EMS

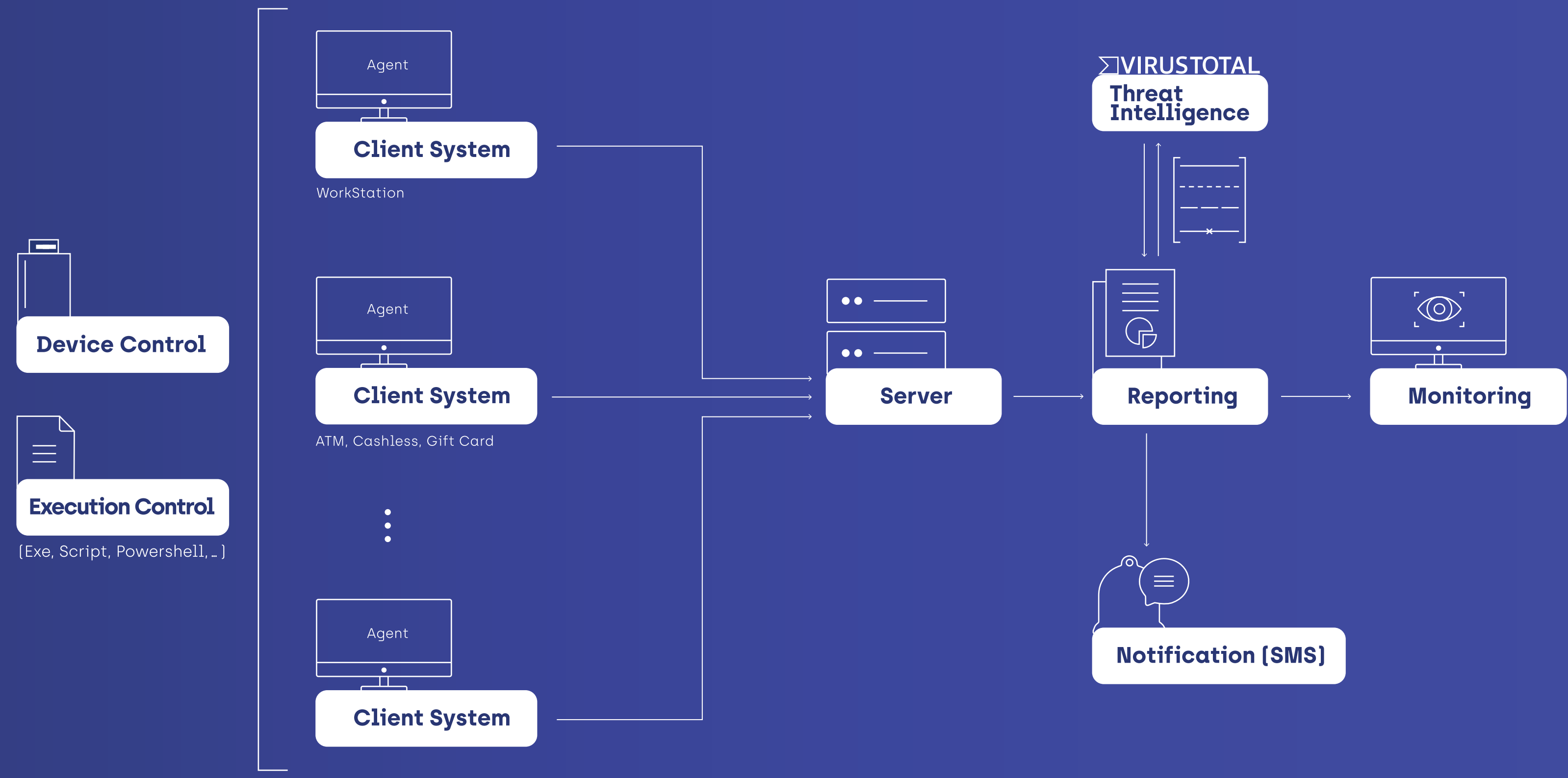
- Providing a safer environment for the authorized withdrawal of banknotes from ATMs (many bank's ATMs are outside the branch and do not have branch security policies)
- It is a local product that meets the new needs and requests of customers
- It is a separate security layer and complementary to other security software (such as antivirus, etc.)
- Monitoring and controlling the process of executing files and connecting devices
- It is a centralized system for rapid response to cyberattacks (Restriction and policy implementation)
- Integration of application software versions in network systems and deactivation of different versions of software
- Sending an alert SMS in case of security problems such as blocking the execution of unauthorized files or connecting/disconnecting a specific device to the ATM
- Checking all types of unauthorized files detected by dozens of the world's best antiviruses (by connecting to a virustotal system)

EMS function in controlling the access level of files

By installing and activating this software system, the network systems will be within a defined range, and only files whose signature (hash) is defined in the server management panel will be executable. Otherwise, they will be recognized as unauthorized files and will be prevented from running. In other words, executable files on network systems are defined, and the entry of new executable files will be controlled and monitored in every possible way.

By activating the client version, *. Com, *. Scr and *. Exe files will be monitored and controlled. Access level permission to 45 other important extensions (such as DLL files, scripts, registry, PowerShell, Jar, etc.) is optional on client windows. The access level to each of the extensions can be selected and applied in the following three modes:

- Nothing
- Monitoring
- Restriction



Device Control

Execution Control

Client System

WorkStation

Client System

ATM, Cashless, Gift Card

⋮

Client System

Agent

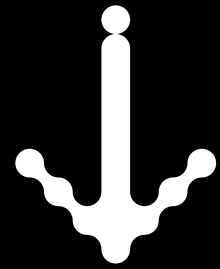
Server

Reporting

VIRUSTOTAL
Threat Intelligence

Monitoring

Notification (SMS)

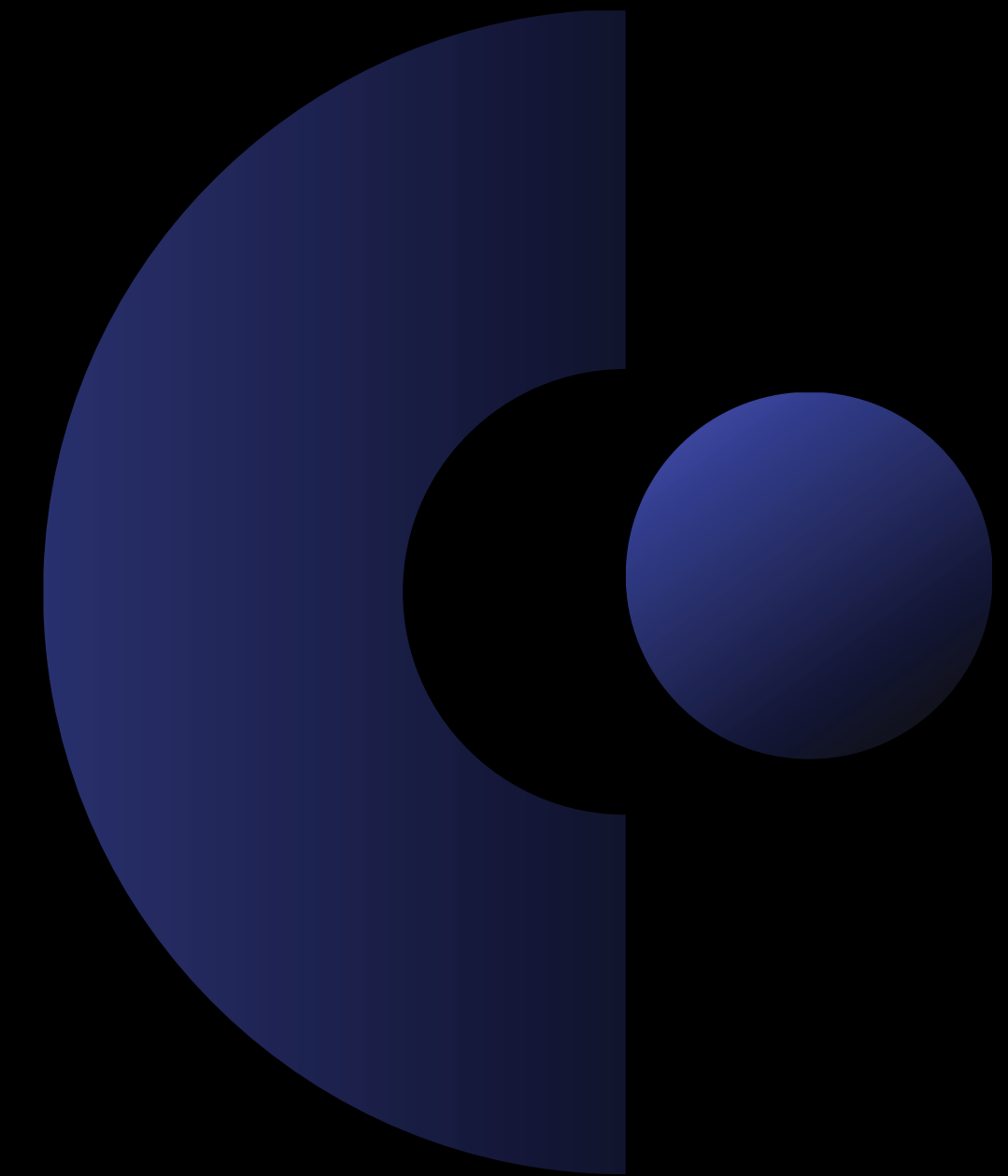


Control of the equipment connected to the system by EMS

Another added value that this software system can bring to organizations is the control of devices connected to the system and ATMs. Device control (connection and disconnection) can be selected and applied based on the selection of the device type in the server panel and the following three sections:

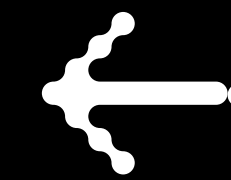
- Mouse and Keyboard
- Storage devices
- Bluetooth and WiFi and mobile tethering

In case of deactivation of peripheral memories such as USBs, only USBs whose serial numbers have been introduced to the server panel will be allowed to be used. Also, if the policy related to mouse and keyboard devices is disabled, by connecting the USBs whose serial numbers have been introduced to the system, the mouse and keyboard will be activated, and when the authorized USB is removed, the mouse and keyboard deactivation policy will be automatically applied.



Comparison of security solutions to prevent the implementation of various threats

| Threat | Firewall | Antivirus | Whitelist Application |
|-----------------------|----------|-----------|-----------------------|
| Malware | | | |
| Trojan Horse | ● | ● | ● |
| Worms | ● | ● | ● |
| Downloader | ● | ● | ● |
| Key Logger | ● | ● | ● |
| Backdoor | ● | ● | ● |
| Zero-day Viruses | ○ | ○ | ● |
| Fake Anti-Viruses | ○ | ○ | ● |
| Tools | | | |
| Proxy Software | ○ | ○ | ● |
| Shareware | ○ | ○ | ● |
| Threat Sources | | | |
| Internet | ● | ● | ● |
| Network Share | ● | ● | ● |
| USB drive | ○ | ● | ● |
| CDRom | ○ | ● | ● |
| Time Killers | | | |
| Games | ○ | ○ | ● |





Prerequisites for using the Spara EMS

Server Requirements:

| Title | Descriptions |
|---|--|
| Hard disk volume | Hard Disk: 300 GB At least two drives should be included (100 GB should be allocated for Windows drive) |
| Required Windows (64-bit version) | Microsoft Windows Server 2012 2016 2019 |
| CPU & RAM specifications to support up to 1000 client systems | RAM: 16 GB CPU: 4Core |
| CPU & RAM specifications to support up to 3000 client systems | RAM: 24 GB CPU: 6Core |
| CPU & RAM specifications to support up to 5000 client systems or higher | RAM: 32GB CPU: 8Core |

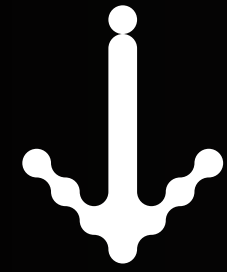
Network Requirements:

Opening the desired network port for communication between server and client and vice versa.

Software client requirements:

Support for 32-bit and 64-bit Windows:

- Windows XP (SP3)
- Windows 7
- Windows10
- Windows10 LTSC



EMS is suitable for which businesses?

The implementation of this product will be practical and suitable for departments, organizations, companies, and banks that need to determine policies to ensure security, control execution, and manage devices in Windows systems and devices under their domain.



About Spara

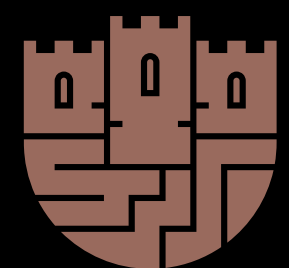
Today cyber risks are a critical threat to all organizations worldwide. In the past, organizations tried to provide their cyber security only by using the security equipment and software available in the market. But today, cyberattacks have a very complex structure, so it is no longer possible to deal with them using traditional methods. Therefore, to deal with advanced cyber threats, organizations need to use advanced detection and prevention systems to identify them in the shortest possible time in case of cyber penetration.

In this regard, "Spara" company and a group of the best cyber security experts in the country have produced new products, diverse services, and comprehensive cyber security solutions. "PAM", "EMS" and "EDR" are the most important products of Spara. Spara's security services and solutions also include a wide range of security services such as "Security Operations Center", "Penetration Test", "Threat Hunting", "Red Team", "Governance, Risk Management, and Compliance", "Incident Response", "Consulting" and "Training".



We have been trusted by:





سپارا
SPARA



+98(0)21-22275003



info@spara.ir



www.spara.ir