STORMSHIELD

THE ULTIMATE PROTECTION AGAINST UNKNOWN AND SOPHISTICATED ATTACKS

ENDPOINT SECURITY

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield

Endpoint Security

THE SECURITY SOLUTION THAT PROVIDES PROTECTION AGAINST UNKNOWN OR SOPHISTICATED ATTACKS THAT ARE UNDETECTED BY YOUR CONVENTIONAL DEFENSES.

ENDPOINT SECURITY

Today's attacks are becoming ever more targeted and sophisticated in a bid to bypass conventional protection systems. They use advanced infection techniques – such as exploiting unknown vulnerabilities – and employ sophisticated mechanisms to go undetected in the operating system. Threats are no longer restricted to networks: they now extend to sensitive or industrial environments where the potential impact is considerable (risks of physical impairment, production line stoppage, etc.).

Unique protection

Based on a unique technology that analyzes interactions between processes and the system of a workstation or server, **Stormshield Endpoint Security provides proven protection against these sophisticated attacks,** complementing your conventional protection tools.

A series of security layers effectively prevents the system from being compromised and ensures its integrity: it blocks the exploitation of vulnerabilities (e.g. corruption of the memory to run malicious code), prevents viruses – ransomware in particular – from being installed on workstations, detects malicious actions, etc.

Proactive and unconnected technology

Stormshield Endpoint Security is the result of years of research and development and is used to recognize unknown and sophisticated attacks without requiring product updates or a connection to an external system. It is the perfect solution for the protection requirements of off-line environments and is suitable for protecting obsolete environments (e.g. Windows XP which no longer gets security patches).

This technology is used worldwide by significant numbers of clients who need to protect sensitive infrastructures (Defense, Critical Infrastructure, etc.) or have considerable operational and regulatory constraints (Industry, Energy, Point-of-Sale Terminals, etc.).

A complete workstation control solution

Stormshield Endpoint Security allows you to control various workstation behaviors and determine which are considered legitimate and which are prohibited.

Our solution is essential for fighting against data leaks and losses, protecting against external viruses, and blocking the malicious usage of IT equipment provided by the company.

This workstation control covers the use of external communications (Wi-Fi, Bluetooth, etc.), of external devices (e.g. removable peripheral devices, such as USB drives) and ensures workstation compliance (up-to-date Windows patches, clean computers, etc.).

CONTEXTUAL PROTECTION

Stormshield Endpoint Security can react automatically based on its environment. This unique adaptability means it can immediately react when the context changes, whether or not the workstation is connected to the Internet.

Stormshield Endpoint Security prevents security vulnerabilities by:

- Quarantining a workstation if security patches are not applied.
- Configuring a more restrictive security policy if the workstation is outside the infrastructure.

INDEPENDENT PROTECTION

Stormshield Endpoint Security is a standalone protection that does not need an Internet connection to update itself. Its proactive and generic security mechanisms block zero-day threats, without the software needing to be updated or adapted.

LIMITED SYSTEM FOOTPRINT

The advantage of proactive technology is that it has a limited system footprint. Traditional protections involve comparing each process sub-part with signature databases containing millions of entries, which is costly in terms of performance. Stormshield Endpoint Security technology monitors critical areas of the operating system for abnormal behavior.

ULTIMATE SOLUTION

Our protection provides a set of security barriers (firewall, network IDS, application control) that guarantees end-to-end protection of servers, workstations and terminal devices without updating. Stormshield Endpoint Security combines with traditional protection systems (anti-virus systems) by adding an additional layer of security.

TRANSPARENT PROTECTION

The solution provides real-time protection without impacting workstation performance. Stormshield Endpoint Security notifies the user in the event of an attack and immediately routes the information back to the administrator via the central console.

PROTECTION ON THE MOVE

Mobile workstations often lack security or control outside the company's perimeter. They are not covered by the company's various protection barriers (firewall, IDS network, etc.). Stormshield Endpoint Security ensures the security of mobile devices, whether they are inside or outside the infrastructure.

FULL INTEGRATION

Security policies can be applied to groups of users according to several criteria: IP address, MAC address, machine name, but also by using the organization's Active Directory to reduce administrator time and therefore costs. The product integrates with several SIEM products on the market. The product integrates with several SIEM products on the market, so you can take advantage of full visibility of security events across your entire organization.

CONFIGURATION GRANULARITY

The product offers flexibility when configuring the security policy to meet the specific needs of each company. This means that protection is adapted to the needs of your company.

MANAGEMENT COSTS REDUCTION

Our proactive protection can drastically reduce the cost of applying security patches: our product, which proactively protects against zero-day threats, will keep you secure.

Zero-day protection against unknown threats

Protection against exploiting operating system vulnerabilities. Protection against exploiting third-party application vulnerabilities. System memory integrity control. Protection against memory-based viruses (fileless malware).

Protection of workstations and servers

Malware detection by behavioral analysis. Operating system hardening. Application control (white list and black list). Protection against privilege elevation and identity theft. Granular control of user rights. Granular control of the sensitive data exfiltration.

Intrusion prevention

Firewall. Network intrusion detection.

Network access control

Creating context-sensitive policies based on users, machines, connections, and machine compliance. Health and policy compliance audit, regardless of the workstation location. Fully automated disinfection.

Adaptive protection

Dynamic adjustment of user login privileges based on location or context. White list of Wi-Fi access points for your company. Imposition of WPA / WPA2 security standards. Obligation to use VPNs with public access points. HSDPA / 3G modem usage check.

Peripheral device control

Authorization or restriction of peripheral devices by type or serial number. Blockage or restriction of various peripheral device operations. Encryption of removable peripheral devices. Protection against infection. Restriction or control of peripheral devices: USB, CD/DVD/BR burner, network cards, serial/parallel port, Firewire, etc. Evaluation (appropriate or not) and audit of file transfers.

Technical Specifications

SOFTWARE COMPONENTS

Agent
Server
Admin console

RECOMMENDED SYSTEM PREREQUISITES

FOR THE AGENT

Pentium IV 3 Ghz

Memory
512 MB (minimum) / 1 GB (recommended)

Disk space
250 MB (90 MB with agent logs)

Operating systems
Windows XP SP3 (32-bit)
Windows 7 SP1 (32 & 64-bit)
Windows 8.1 Update 1 (32 & 64-bit)
Windows 10 (32 & 64-bit)
Windows Server 2008 SP2 (32-bit)
Windows Server 2008 R2 (64-bit)
Windows Server 2012 R2 (64-bit)

FOR THE ADMINISTRATION SERVER

Processor clocked at a minimum of 1Ghz

Memory
1 GB minimum

Operating systems
Windows Server 2008 SP2 (32 & 64-bit)
Windows Server 2012 R2 (64-bit)

STORMSHIELD

Contact your Regional Sales office today:
WWW.STORMSHIELD.EU/SALES-OFFICES