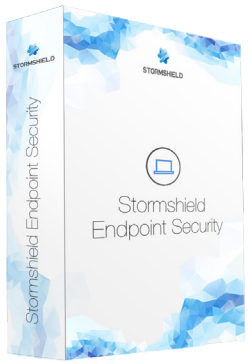
STORMSHIELD



STORMSHIELD ENDPOINT SECURITY

THE ONLY SOLUTION THAT PROVIDES TRUSTED PROTECTION AGAINST TARGETED ATTACKS AND APT

Drawing on a unique system analysis technology, Stormshield Endpoint Security is the only solution that provides proven protection from both known and unknown targeted attacks and APTs.

Seamless and perfectly adapted for large-scale deployments, Stormshield Endpoint Security integrates into a single agent all the security services needed for protecting workstations and servers, ranging from peripheral device control to the encryption of disks.

ISSUE

Corporations today have to contend with advanced attacks that grow in number and intelligence, the consequences of which are often drastic. Now more than ever, businesses are forced to adapt to this context and come up with innovative ways to protect and monitor the network. For the past 11 years, the Stormshield Endpoint Security suite has consistently kept threats at bay thanks not only to a comprehensive suite of modules for general workstation security, but also to an exclusive technology that protects against APT exploitation with proven effectiveness in actual real-life conditions. Proactively blocking 93% of Windows XP vulnerabilities, Stormshield Endpoint Security boasts the best verifiable statistics on the market, while keeping false positives extremely low.

ADVANTAGES

- The only anti-APT technology with a proven track record against the exploitation of uknown vulnerabilities.
- A global approach to the issue of data leaks through the Device Control, APT Protection and Encryption modules.
- A Core Defense module covering all basic security needs such as application control, firewall, HIPS, NIPS, etc.
- Security policies capable of dynamically adapting to the context of each individual workstation.
- Easily integrated architecture, agents that are simple to deploy and a centralized administration console.

ABOUT

Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space CyberSecurity, run the Stormshield brand and offer innovative end-to-end security solutions both in France and worldwide to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

WWW.STORMSHIELD.EU

Phone

+33 9 69 32 96 29

The cost of a call may vary according to the country you are calling from and your telecoms operator.

E-mail contact page

SOFTWARE COMPONENTS

- **Agent**
- **Server**
- **Administration console**

SYSTEM REQUIREMENTS

For the agent

- Pentium IV: 3 Ghz
- Memory: 512 MB (minimum), 1 Gb (recommanded)
- Disk space: 250 MB (90 MB with agent logs)
- Required disk space with antivirus: 400 MB
- Operating systems: Windows XP SP3 (32bits), Windows Vista SP2 (32bits), Windows 7 SP1 (32/64bits), Windows Server 2003 (32bits), Windows Server 2008 (32bits), Windows Server 2008 R2 (64bits)

For the administration server

- Processors speed of at least 1 Ghz
- Memory: minimum 1 GB
- Disk space: minimum 1 GB
- Operating systems: Windows Server 2003 R2 (32/64bits), Windows Server 2008 SP2 (32bits), Windows Server 2008 R2 (64bits)

APT PROTECTION

- 3rd-generation vulnerabilty protection: several layers of protection make it possible to detect each attack.
- Implementation of ASLR technology on older operating systems (Windows XP) unique to the product.
- Enhancements to ASLR technology to allow the detection of common malicious techniques enabling this protection to be bypassed.
- Measures against heap spraying attacks that facilitate the exploitation of JavaScript vulnerabilities.
- Memory statuts control.
- Thorough analyses of process code in order to identify executions in kernel mode that were unplanned in the application's code.
- And many other features: honeypot, ret-lib-c prevention, pass-the-hash detection, etc.

DEVICE CONTROL

- Full tracking of operations on any type of removable peripheral device.
- Granular access privileges to removable storage devices.
- Access control with reading and writing privileges depending on file type.
- Encryption of data stored on removal devices.
- Bluetooth control, 3G/4G, Wi-Fi connectivity, protocol validation.
- Validation of VPN use at public access points.

CORE DEFENSE

- HIPS protection: continuous behavioral analysis, self-learning system for legitimate applications, protection from keylogging and raising privileges, rootkit detection.
- Firewall with network protection: prevention of ARP cache poisoning, illegitimate sessions, identity spoofing, etc.
- Application control: control over the installation and execution of applications, validation of application whitelists of blacklists, protection from closure applications, access to control files and regisitries.

ENCRYPTION

- Transparent disk encryption.
- Centralized encryption policies based on the file/folder.
- Deletion of secure files and cleanup of exchange files.
- FIPS140-02 certification.

ANTIVIRUS

- Detects and cleans up all known issues.
- Analyzes files in real time or upon request.
- Analyze e-mails even before they reach your mailbox.
- Seamless management of the module by the Stormshield Endpoint Security management console.

Arkoon Network Security
1 place Verrazzano - CS 30603 69258 - Lyon Cedex 09