



Combining proactive security and behavioral-based protections, StormShield fuses a variety of robust security functionalities into an integrated whole. With just a single agent, StormShield allows companies to protect their entire population of desktop and mobile workstations from known or unknown attacks and loss of critical data.

Endpoint and data protection

Far too many companies still rely solely on simple signature-based antivirus technology to protect corporate workstations. Providing such an incomplete security coverage results in considerable financial exposure, and often, losses for many businesses.

Connected to the internet, often used outside of the company's network, workstations are today's main targets for attacks inside and outside the corporate environment. Keylogging, polymorphic viruses, Denial of Service attacks, rootkits are examples of the many threats that are only partially countered by traditional antivirus technologies.

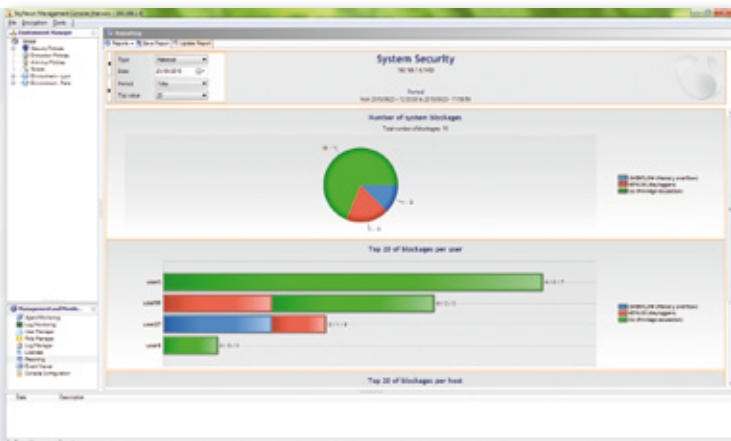
Users themselves contribute to making workstations a weak link in corporate security policies. The lack of effective control exercised by IT

administrators on the extended use of workstations prevents them from protecting the company against abuses and blunders: unauthorized application downloads, unmanaged networks, data leaks, unprotected USB ports and drives, etc.

With **StormShield**, SkyRecon Systems offers a comprehensive and consistent protection of endpoint workstations. Our solution addresses in a transparent manner all risks associated with the use of computers: vulnerabilities, known and unknown software attacks, intrusions, inappropriate use of personal applications, unauthorized connections, critical data theft or loss and many more. StormShield achieves this protection with an unmatched level of granularity thus allowing organizations of any size to protect staff computers without blocking or disrupting user activities.

Benefits

StormShield is the first proactive, multi-layer, real-time defense system for network endpoints. It returns endpoint control to the IT organization, giving administrators fine-grained tools for managing and securing workstations, laptops, and mobile devices. These protections operate regardless of location – within the organization, via home networks and in wireless hotspots. Policies can change dynamically depending on the connectivity context, the current user and the health assessment of the machine, ensuring that security meets or exceeds defined risk levels. Once configured and deployed from StormShield's central management console, policies cannot be disabled or modified by the user, even if that user has local administrator rights.



- Proactive protections addressing zero-day threats and unknown attacks
- Extensive device control and data leakage prevention
- Context-aware policies that dynamically adapt security guidelines to risk levels
- Interoperable with leading NAC infrastructure solutions for an end-to-end NAC solution
- Unified, integrated endpoint security suite that reduces cost and complexity



Features



Host Intrusion Prevention System (HIPS) and Firewall

Proactive Protections

- Protections against known and unknown vulnerabilities
- Protections against known and unknown keyloggers
- Executable files, file types, folders, system panels and registries access control

System Hardening

- Self-learning of legitimate application and operating system behavior
- Spotting and stopping zero-day exploits and unknown malware

Network Intrusion Prevention

- Protocol integrity checking
- Detect and block network intrusion mechanisms such as port scans, ARP poisoning, etc.



Application Control

- Control installation and execution of applications
- Enforce either application whitelists or blacklists
- File-centric controls to limit file access



Network Access Control

- Workstation posture check: patches, anti-virus signatures, applications installed, etc.
- Network health check: simultaneous connection control (Eth., 3G, Wi-Fi), workstation localization (inside or outside the corporate environment), use or not of the VPN
- Interoperable with Juniper UAC, Microsoft NAP, Cisco NAC and many VPN vendors



Wireless Security

- Wireless connections control: Wi-Fi, 3G, Bluetooth, IrDA
- Enforce VPN use at public access points
- Whitelist authorized Wi-Fi access points



Device Control

- Monitoring of operations on removable devices
- Fine-grained access rights to removable storage devices, wireless and I/O devices (printers, keyboards, etc.)
- Control of read and write access at the file type level
- Encryption of data stored on removable devices



Encryption (optional)

- File-based encryption
- Full disk encryption
- Secure file erasure/wipe



Anti-Virus and Anti-Spyware (optional)

- Detects and eliminates all types of known viruses

Technical Description

Software Components

Agent

- Policy enforcement
- Autonomous defense mechanisms
- Integrated log and alert system
- Transparent installation and execution

Server

- Policy distribution
- Log collection

Management Console

- Policy configuration
- User and environment management
- Log monitoring
- Reporting

System Requirements

For StormShield Agent

- **Pentium IV:** 3 GHz
- **RAM:** 512 MB (minimum), 1 GB (recommended)
- **Hard disk space:** 25 MB (90 MB with Agent logs)
- **Hard disk space required for the anti-virus:** 400 MB
- **Operating system:** Windows XP SP2/SP3 32bits, Windows Vista SP1/SP2 32bits, Windows 7 32bits

For StormShield Server

- **Processor:** 1 GHz minimum
- **RAM:** 1 GB minimum
- **Hard disk space:** 1 GB minimum
- **Hard disk space required for a server with anti-virus:** 2 GB minimum
- **Operating system:** Windows XP SP1/SP2/SP3 32bits, Windows Server 2003 SP1/SP2 32bits, Windows Server 2008 SP1 32bits, Windows Vista SP1/SP2 32bits

For SkyRecon Management Console

- **Pentium III:** ~800 MHz recommended
- **RAM:** 512 MB recommended
- **Hard disk space:** 50 MB
- **Operating system:** Windows XP SP1/SP2/SP3 32bits, Windows Server 2003 SP1/SP2 32bits, Windows Server 2008 SP1 32bits, Windows Vista SP1/SP2 32bits
- **.NET Framework:** version 2.0

Encryption

Encryption Standards

AES-128, AES-192 and AES-256

Authentication Methods

- Windows authentication, Windows Active Directory and GPO
- Optional secondary authentication and integration with strong authentication systems
- Optional smart card authentication

Certification

FIPS 140-02