

Safeguarding the Enterprise Endpoint and Data

The greatest threat to enterprise security today is at its endpoints - the desktops, laptops, and other devices used by company personnel in the field, on the road, and in the office. Meeting demanding regulatory requirements, foiling attacks, and obstructing new viruses with these relatively uncontrolled systems presents a significant challenge to IT administrators.

SkyRecon Systems addresses this challenge with the proven, award-winning StormShield Security Suite. Providing consistent, powerful, 360-degree protection, this modular system 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 theft of critical data, without disrupting user activity.



Why is the Endpoint Vulnerable?

Because it is traditionally the least protected part of the network, the endpoint has become both a major focus of external attack and a source of problems created by internal errors. Almost every day, it seems that the media announces another stolen laptop carrying private data, a key-logging attack that allows access to financial accounts, or a significant virus or denial-of-service (DOS) attack on a major corporation that started at a single workstation.

Even more significantly, internal breaches can be caused by disgruntled employees and contractors; users who upload superfluous applications containing security holes, respond to “phishing” messages, or engage in illicit downloads. The user is a large part of the reason why the endpoint is a “blind spot” in the overall IT strategy, as administrators need to be able to enforce policies without impacting the user’s ability to work.

The Need for Integrated Security at the Endpoint

More than 99% of companies today have antivirus protection, yet 68% of large enterprises have suffered some type of attack. Why aren’t these companies protected? Recent studies have shown a 29% increase in bot-infected systems worldwide, a 23% increase in Trojans, and a 54% increase in loss of information due to the theft of a USB key or other data storage medium.

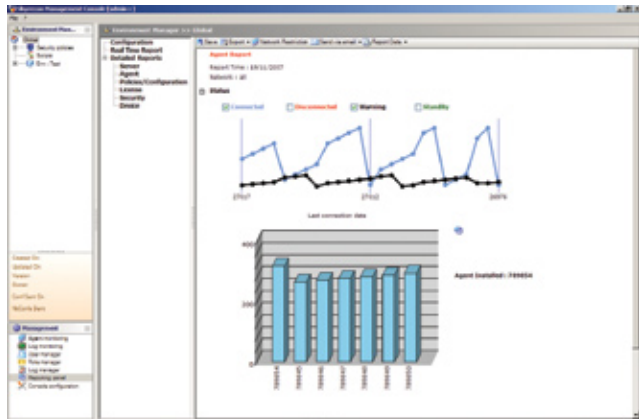
The reason is that traditional endpoint security companies usually address security issues with a single point solution, such as antivirus, encryption, etc. While these technologies may be powerful, they are by definition limited to the risk being addressed, leaving the endpoint open to other types of attack.

Neither is investing in a variety of point solutions effective. Most cannot integrate with each other to completely shield corporate information, and they can have a major performance impact on the endpoint.

The Stormshield Security Suite

StormShield 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 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 administrator rights.

With its combination of simple, central manageability, comprehensive and distributed protection, and complete control, StormShield enables IT organizations to regain complete control of their endpoint security infrastructure.



Policies Configuration Report

Benefits

- Single, integrated endpoint security suite that reduces cost and complexity
- Comprehensive endpoint security to increase security and ensure compliance
- Context-aware policies that dynamically adapt security guidelines to risk levels
- Unique behavioral security to address zero-day threats and unknown attacks
- Management console to monitor enterprise-wide endpoint security posture in real-time
- Interoperable with leading NAC infrastructure solutions for end-to-end NAC solution

Features

Host Intrusion Prevention System and Firewall

Rule-Based Protection

- Executable files, file types, folders, system panels and registries access control
- Inbound and outbound application connection control

System Hardening and Behavioral Analysis

- Detect, alert and block generic attack mechanisms such as memory overflow or keylogging
- Self-learning of legitimate application 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 or floods

Application Control

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

Network Access Control

- Check running applications, signature files and patch updates
- Client-based enforcement of NAC policies
- Fully-automated remediation
- Interoperable with Juniper UAC, Microsoft NAP, Cisco NAC and many VPN vendors

Wireless Security

- Control ad hoc mode and Bluetooth connectivity
- Enforce VPN use at public access points
- Enforce authentication and encryption protocols
- Whitelist authorized WiFi access points
- Enable "No WiFi" policy inside or outside the company

Device Control

- Fine-grained access rights to removable storage devices
- Control by type, model, and serial number
- Control of read and write access at the file type level
- Encryption of data stored on removable devices
- Control over classes of USB devices
- Monitoring of operations on removable devices

Content Encryption

- Transparent, on-the-fly file encryption
- Centrally managed encryption policies based on folders and file types
- Optional secondary authentication and integration with strong authentication systems
- Password-protected, self-extracting encrypted containers
- Secure file shredding and swap-file cleaning

Anti-Virus

- Detect and delete all forms of viruses
- Keep PCs free of spyware
- Anti-Rootkit: detects unseen threats on PCs

System Requirements

Agent

Microsoft Windows® 2000 SP4, XP SP1/SP2/SP3, Vista
20 MB available hard disk space

Server

Microsoft Windows® Server 2000, 2003, 2008

Management Console

Microsoft Windows® 2000, XP