

Protecting Customer Data at Rest and in Motion

More and more organizations are turning to encryption to protect critical data. It is spreading from corporate laptops where it has made big inroads to desktops and servers. Without a doubt encryption solves a lot of the risk associated with data at rest that IT administrators face daily. But, what about the rest of the risk associated with access and proper use?

There many ways to encrypt data and handle encryption keys. A well-designed encryption strategy will be flexible in that it can do whole disk encryption, file encryption and be able to easily handle removable devices, including USB drives, iPods, CD/DVD burners, and FireWire devices. The StormShield solution utilizes integrated AES-256 encryption to protect the data in all of these scenarios - encrypting data in memory and in swapfiles as it is being used as well! It also provides a sophisticated system with a multiple authority mechanism for encryption keys - ensuring proper data access and protection, regardless of how the data is accessed and regardless of how the systems/devices are used.

Data leak prevention is a hot topic right now because of the many opportunities for data to leave the bank environment. We are seeing quite a bit of interest in USB security as the devices are widely used as they are inexpensive and take on so many common form factors that help business get done. StormShield can control USB usage at a very granular level: by user, by machine, and/or by unique USB device. StormShield can even enforce encryption on all files written to the USB devices and ensure that the encryption follows the files as they are transferred to systems outside of the business - even non-business systems.

Network Access Control (NAC) is also garnering quite a bit of attention these days. At SkyRecon, we go far beyond your typical perimeter-based NAC with our over-arching implementation of comprehensive endpoint-to-network Access Control. StormShield can control who is using the machine, where it is connected and what applications are running (or not) - locally at the endpoint, while connecting to the network, and while inside the network. This granular Access Control allows administrators to determine exactly how information is being accessed, by whom, from where, and via which applications. StormShield takes Group Policies to the next level by allowing IT departments to enforce their security and compliance policies in such as way as to control precisely how employees should be using applications, machines and network resources - and most importantly - the data that these components have access to.

Managing disparate security technologies from multiple vendors is a daunting proposition for overworked IT departments. StormShield directly addresses this problem and has solved it in a single, multi-layered, lightweight endpoint protection, data encryption, and access control client that is managed remotely from a single management console. Data extraction and leakage are controlled, as are unauthorized and compromised devices. Our built-in Host Intrusion Prevention (HIPS) and firewall software provides protection from zero day attacks that traditional signature-based-only products are unable to adequately address.

When the StormShield client installs on a machine, it only occupies around 16MB and represents the industry's first unified endpoint security solution to provide risk-based single-policy control and enforcement for all layers of endpoint security. Not only does it provide access control, encryption, device control, integrated firewall and intrusion prevention for zero-day attack protection, but our clients can turn on other modules at any time: signature-based anti-virus and anti-spyware, anti-keylogging, and wireless network security, for example. Banks already have perimeter firewalls, email filtering and other good perimeter protections in place; the StormShield solution thoroughly - and affordably - protects the weakest link: the endpoint.



Sean Martin
Vice President

Sean Martin, CISSP, is Vice President SkyRecon Systems. Sean brings nearly two decades of experience in building, launching, and delivering consumer and commercial security products to businesses and institutions globally. He has held numerous senior-level manager positions at Symantec Corporation, where, during his 13-year tenure, he was responsible for delivering, launching and marketing the company's endpoint protection, policy management and security incident management solutions. Prior to Symantec he served as a software engineer and network engineer for the Valley Crest Companies. Sean holds the CISSP certification from ISC² and completed his BS in Business Administration from the University of Phoenix.



Contact Info:

<http://www.skyrecon.com>