



(c. online)

Group Test: Endpoint security

Michael Lipinski

Products Tested

[Check Point Endpoint Security](#)
[Cynapspro DevicePro Ultimate 2009](#)
[GFI Software EndPointSecurity v4](#)
[Novell ZENworks](#)
[Safend Endpoint Suite](#)
[SkyRecon StormShield Security Suite](#)
[Sophos Endpoint Security & Control](#)
[Symantec Endpoint Protection v11.0.4](#)

Summary

A few of the products really did a nice job delivering an intuitive interface with a very effective and comfortable look and feel. Others required us to really dig into the documentation and work more to move around the various screens.

Both my desktop PC and my notebook computer allow me to perform the tasks associated with my job. These same devices also provide me with the ability to print to a local printer, sync to a PDA device, plug in my camera and transfer images, add new software, attach to my private secured wireless network, as well as any public unsecured wireless network, burn CDs and DVDs, plug in USB devices, and so on.

As our technologies continue to expand to meet the challenges of component integration and data sharing, and as the mobile workforces continue to grow and more people access corporate resources over unsecured public networks, the challenge becomes controlling what data should be allowed to reside on those endpoints or mobile devices and, when allowed, securing that data while at rest and while in transit.

Audit after audit, I am always amazed at the amount of data that can easily walk out of organizations. These challenges have far-reaching implications, such as the protection of the corporate data and of personal identifiable information, and the obvious compliance and audit requirements.

I find myself always weighing the security advantages of totally locking down an endpoint so no applications can be loaded, no port will be active and no unauthorized communications can occur versus the productive gains of allowing people to use the technology we give them to be more effective, productive and innovative. To be effective, endpoint security must balance the security risk with the productivity benefits. The right solution must also address the IT challenges we all face today - mainly, overburdened and understaffed IT departments.

In this month's issue, we reviewed endpoint security solutions. The criteria for the submissions focused on solutions that could manage, assess or control security at the endpoint, were centrally managed, and provided centralized reporting and alerting.

We classify the products into four categories: network security - providing protection like firewalls, anti-virus and spyware; encryption - the ability to encrypt the local drive or partitions, as well as any removable media that would be allowed; port management - providing tools to manage everything from USB ports to printers, CD/DVD devices, communication ports (serial or parallel ports), smart card readers; and various wireless interfaces, such as Bluetooth, infrared and Wi-Fi. The final category addresses the host-based

intrusion protection aspect with solutions that monitor and prevent application loads, registry changes, privilege escalation, and block use of copy/paste features and kernel event management.

We reviewed 10 products - most fit nicely into one of the definitions above. Some spanned the categories and provided protection for multiple endpoint categories. We reviewed eight software solutions, one appliance and a solution that provided software on a PCMCIA [Personal Computer Memory Card International Association] device for controlling remote access and authentication of a mobile PC. We did find a few solutions that provided a very comprehensive set of capabilities, as others focused on one area of protection while providing integration with solutions that delivered the rest.

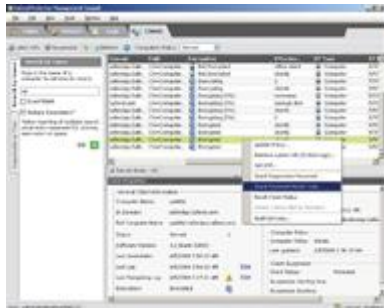
We focused our testing efforts on the server side management, reporting and alerting along with the product's ability to integrate with various directory structures for setup, agent/client deployments and management of the environment. Most of the products required the use of a backend database engine. One or two shipped with their own embedded database, the rest required us to load either a MSDE [Microsoft Data Engine] or SQL database prior to loading the application. This will be something to pay attention to when evaluating these products in your own test labs.

Besides features and functionality, which we will address in the individual reviews, we found a few differences in the products. The first was related to the ease of the installation - some went quickly with a fully integrated install script, while others took some time and required things such as database configuration and loading of various versions of .NET and other dependencies. Another difference we found was in the maturity of the server side component, the management counsel or dashboard.

A few of the products really did a nice job delivering an intuitive interface with a very effective and comfortable look and feel. Others required us to really dig into the documentation and work more to move around the various screens.

Safend Endpoint Suite

Product Information



Vendor: [Safend](#)

Product: [Endpoint Suite](#)

<http://www.safend.com>

Price: \$13 to \$35 per seat

Product Rating

Features	★★★★☆
Ease of Use	★★★★☆
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★☆
Value for Money	★★★★☆
Overall Rating	★★★★☆

For: Installs easily, nice management interface and easy to use.

Against: Reporting module extra and pricy when you add it all up.

Verdict: Nice solution for port management. Built-in best practice for various compliance reports.

Related Group Test

[Group Test: Endpoint security](#)

Reviews For This Vendor

- [Protector v3.1](#)

Safend Protector protects an organization's information from loss and theft by monitoring, detecting and restricting data transfers from the endpoint. Safend Auditor provides organizations with the visibility needed to assess and manage vulnerabilities. The company also has modules for reporting and encryption that were not part of this review.

The Safend Protector and Auditor were loaded on our test server after loading and configuring .NET 2.0 and SQL server. The dashboard was laid out like a file cabinet with tabs across the top and multiple navigation panes below. We were able to find our endpoints by scanning the operational unit (OU). The tool identified devices and the active ports on those devices. This tool was valuable for knowing what was connected to the network at any point. We had to run this tool more than once as we learned that the endpoints have administrative access, but also required remote registry and file/print sharing enabled and ports 139 and 445 allowed on the endpoint firewall.

We were impressed with the management interface. It was one of the better ones we reviewed. It was easy to use and navigate. The server came with sample built-in policies and built-in, best practice reports for HIPAA, PCI DSS and SOX. We liked the customizable end-user messages that can be sent on specified policy violations.

With Protector, we applied customized security policies to all physical, wireless and storage interfaces. It also encrypts and enforces the encryption of all removable media devices. We liked the unique shadowing feature that allows for keeping secure copies of files or specific file types to and/or from removable media. There was no firewall, anti-virus, anti-spyware or IPS support, but the documentation did state that most of the top providers have gone through interoperability testing and were certified with Safend.

Safend provided a comprehensive port management and encryption solution. The documentation was very good. Basic support is provided with the license purchase and upgraded support is available.

Prices for Safend products depend on the number of seats purchased. For the Safend Protector, prices range from \$13 to \$32/seat; Safend Encryptor: \$29 to \$69/seat; Safend

Protector & Encryptor: \$32 to \$89/seat; Safend Reporter: \$5 per seat; Safend Auditor: \$700 to \$5,000/seat.