

Means to an endpoint

ENDPOINT SECURITY REPRESENTS A PRIME GROWTH OPPORTUNITY FOR SAVVY VARs

By Frank Ohlhorst

TODAY'S SECURITY PRODUCT LANDSCAPE is littered with solutions, each promising network protection, yet breaches continue to happen at an alarming rate.

According to the latest survey conducted by the think tank Ponemon Institute, the costs of security breaches have risen 43 percent since 2005. That rise has been driven by affected companies scrambling to notify customers, bring in investigators, invest in new security technology and respond to lawsuits.

Ponemon's "2007 Cost of a Data Breach report" also shows the total average cost of a data breach grew to \$197 per compromised record, an increase of 8 percent since 2006 and 43 percent compared to 2005. The average total cost per reporting company was more than \$6.3 million per breach and ranged from \$225,000 to almost \$35 million.

While those numbers may be scary, they highlight the importance of implementing proper security and also demonstrate that opportunities are only growing for security VARs. The big question becomes: What can VARs do to prevent breaches and secure the network?

Some claim the answer lies in layers of security, artfully combining VPNs, firewalls, appliances and other secu-

rity technology to create a prophylactic of secure protection. And many VARs have made a comfortable living integrating those various solutions into what should be comprehensive security—yet the breaches, infections and compromises still happen.

The result is the addition of even more layers, more technologies and more

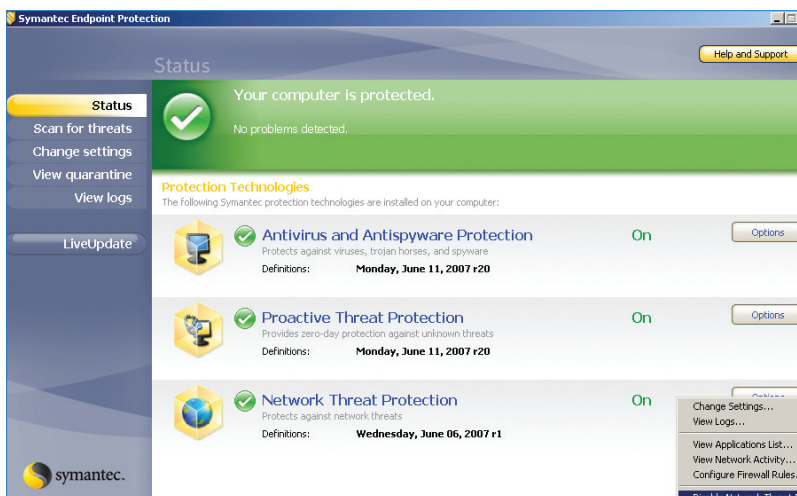
administrators consider the endpoint to be the final piece of the puzzle, or the last layer to address. That perception is arguably 180 degrees out of sync; the endpoint should be the first layer to control and protect. Simply put, control the endpoint and you can control all network security.

As simple as that may seem, vendors have done their best to confuse the issue.

What is endpoint security? Some think it is centered on NAC (network access control) solutions, such as those offered by Cisco Systems, Microsoft and TCG. Some claim that endpoint security is all about desktop security products driven by policy engines, while others feel that endpoint control should be built with user authentication and access-control technologies.

The truth is it takes

a combination of those technologies to build proper endpoint security solutions, which will rely heavily on the VARs' integration skills. Some vendors have done the heavy lifting for the VAR by creating preintegrated endpoint security products that are both simple to deploy and manage. That said, VARs need to realize that most of those "canned" solutions are aimed at the small-business market and assume that the target business has full control of the endpoint.



Symantec's endpoint security approach also tackles anti-virus and anti-spyware.

management overhead to combat the detected threats, which is great for the VARs' pockets. The downside is that customers become suspicious of the solutions offered, critical of the VARs' ability to protect the environment and just plain sick and tired of escalating costs.

The big problem is that most VARs and their customers ignore the most logical layer to protect—the endpoint. In reality, all breaches, infections and compromises and most malicious activity can be traced to an endpoint. Most security

A good example of that style of solution comes from Symantec and its Symantec Endpoint Protection Small Business Edition. The product is built from the ground up to protect endpoints from threats, which by doing so also protects the network. For VARs, Symantec's Endpoint Protection product line proves to be a good starting point for those looking to get into the endpoint security market. The product is not shockingly different from the typical desktop security product, but does add the basics of endpoint security and keeps things simple.

With a software-based endpoint security product, Symantec has an advantage. The company is able to integrate several of its desktop security offerings into a single, cohesive product that can be managed by a network administrator. Having a stock of in-house security products allows the company to avoid the integration hassles associated with third-party products and helps preserve the overall look and feel of the product.

Interestingly, Symantec's offering eschews hardware-based NAC technology and solely relies on software components to handle and alleviate threats. For most of the small businesses out there, especially those running in a single-server environment, Symantec's product should prove adequate. For businesses with branch offices, multiple servers or users who are not always "in-band," VARs should consider a solution that incorporates NAC and Identity Management.

Symantec Endpoint Protection Small Business Edition is a two-piece product, with a client portion that runs on the endpoint and a management portion that runs on a server. Simply put, the server side of the product pushes policies and controls down to the client system via an agent. All activity and statuses are rolled up into the management application.

Symantec offers the expected desktop security capabilities of anti-virus, anti-spyware and a desktop firewall, but then adds the new elements of intrusion prevention and self-enforcement. The product also adds Symantec Mail Security for Microsoft Exchange. VARs should note that Symantec's product is designed only for Microsoft environments and supports only Windows Vista, 2003, XP and 2000 (Service Pack 3 and later).

The server portion of the product installs on Windows 2000 or Windows 2003 servers. The console portion of the product can be run on Windows 2000


be pushed down to the subject PCs and all PCs' security settings are managed from a single console.

This approach simplifies policy definition and reporting. Those networks looking to adhere to compliance requirements will find the integrated reports an excellent source of documentation for compliance reporting. The product offers both graphical and text reports, and the console supports drill-down capabilities to focus on an individual PC or problem.

To meet ongoing and future threats, the management console has a connection to Symantec's threat network, which is constantly updated with new signatures and anomaly identification schemes. Those updates are pushed down to the PCs automatically, which helps to ensure that zero-day threats are accounted for.

A major part of an endpoint security solution is the ability to control access to the PC. Here, Symantec incorporates its Device Control capabilities, which via a policy can control what an attached device can do. That includes locking down USB ports, external drive connections and so on, thus eliminating concerns about data leakage or the introduction of malware.

What's more, Symantec's firewall element helps to prevent malicious activity on the PC by closing off unused or unauthorized ports, while also controlling which applications have access to the network, either locally or remotely. Solution providers can fine-tune the firewall to allow only authorized applications to run or access the network and then enforce that control via policies. One of the best ways to secure a network is to prevent unknown or unauthorized applications from having access in the first place.

One thing is clear: Endpoint security is a growth market for the channel, and savvy VARs can use products such as those from Symantec to enter the market and then scale up to larger, more profitable solutions. 

Product file

- ▶ **Vendor** Symantec (www.symantec.com)
- ▶ **Product** Endpoint Protection Small Business Edition
- ▶ **Features** Desktop security capabilities such as anti-virus, anti-spyware and a desktop firewall, as well as intrusion prevention, self-enforcement and Symantec Mail Security for Microsoft Exchange
- ▶ **Opportunity** Solution providers can use the product to enter the security market and then scale up to larger, more profitable solutions

(SP4), Windows 2003 (SP1) and Windows XP (SP1). For those looking for integration into additional e-mail servers, the company does offer a version called "multi-tier protection," which adds support for Domino and SMTP mail servers.

The product is easy to deploy and manage. The company includes wizards and deployment tools that can automate most of the installation process for both the server and the client PCs. That simplicity is enhanced by the product's use of a single agent and a single management console. Only one agent needs to