TechTarget
Security Media

SearchSecurity.com SearchSecurity.co.UK SearchSecurity.in SearchFinancialSecurity.com SearchMidmarketSecurity.com
SearchSecurityChannel.com INFORMATION SECURITY DECISIONS FINANCIAL INFORMATION SECURITY DECISIONS INFORMATION SECURITY

SearchMidmarketSecurity.com Pocket E-Guide

Endpoint security suites: What to consider before renewal

The shift to Web-based malware and the explosive growth in the amount of threats has forced organizations to move away from signature-based detection. Vendors are now focused on providing complex endpoint security suites with multiple malware detection features, such as full-disk encryption and host-based intrusion prevention (HIPS).

In this expert e-guide, get tips on what you should consider before choosing, keeping, or upgrading your endpoint security software. Review endpoint security suite management issues, as well as how to negotiate with vendors.

TechTarget
The Technology Media ROI Experts

SearchMidmarketSecurity.com Pocket E-Guide

Endpoint security suites: What to consider before renewal

Table of Contents:

Think about performance, data protection when choosing endpoint security suites

Resources from ESET

Think about performance, data protection when choosing endpoint security suites

by Neil Roiter

Antimalware protection is no longer just about signature-based antivirus and antispyware. It has evolved into the use of complex endpoint security suites with multiple malware detection techniques and features, such as host-based intrusion prevention (HIPS) and full-disk encryption.

This two-part tip will cover some of the key points you should consider in choosing, keeping or upgrading your endpoint security software before your next subscription renewal. The second part will focus on centralized management of endpoint security suites and negotiations with vendors.

PERFORMANCE DISTINGUISHES ENDPOINT SECURITY SUITES

The shift to Web-based malware and the explosive growth in the sheer number of threats has forced security vendors to move away from reliance on signature-based detection and bundle in various forms of behavior-based and anomaly detection, HIPS and whitelisting/application control.

"You should only buy what you need, however, malware is getting pretty nasty," said Ed Skoudis, co-founder and senior security consultant with InGuardians Inc. "These packages are pretty all-inclusive, and it doesn't cost vendors any more to put these capabilities into the software."

Testing these complimentary technologies against various strains of malware and attack techniques is very complex. It's tough to tell which vendors, if any, do a measurably better job; the truth is they all miss more than they care to admit.

"Generally speaking, the market is commoditized," said Natalie Lambert, senior research analyst at Forrester Research Inc. "In my opinion, in terms of detection, if you're looking at individual technologies, is there a need to switch out? No."

Performance is another matter. You can and should test the client software's speed and how it impacts performance on fully loaded company laptops and desktops. Run the products on standard company PCs with all your applications.

"You really should evaluate performance, because users will notice the change and complain," Skoudis said. "They will call the help desk, and you don't want that."

ENDPOINT DATA PROTECTION CONSIDERATIONS

Midmarket firms have to deal with many of the same security and compliance issues as large companies do. That means you have to be concerned with the data on your laptops and DVDs, USB drives and MP3 players, and perhaps guest access controls and hygiene checks on devices coming onto the company network.

Not long ago, desktop protection was pretty straightforward: primarily signature-based antivirus and antispyware and, probably, a personal firewall. Your business' requirements have changed, and endpoint security suites are complex products designed to meet those requirements. Here is more you need to consider:

Full-disk encryption. This is rapidly becoming must-have security for midmarket companies that are concerned about data breaches and, in particular, state breach notification laws, PCI DSS and other regulations.

Device control. Some companies have gone to the extreme of disabling USB ports, but device control allows them to take a more flexible approach. This can range from prohibiting all use of removable storage to policy-based controls that require use of corporate USB drives, encrypting copied data, content-based controls over what can be copied, etc.

Application control. This is some form of whitelisting, a valuable approach that can prevent malware from running on company PCs by limiting the number of authorized applications. This can get messy in complex environments with many different desktop images. Application control may also include blacklisting to enforce restrictions on IM, P2P, Skype, etc. Whitelisting can be particularly effective if you run only a handful of apps.

DLP. Endpoint data loss prevention provides insight into what users are copying to their PCs and what they are doing with it, but everything you add has an impact on performance, and if it adds cost, consider passing on it, at least until you are prepared to deploy it as part of a larger DLP project. "DLP [in an endpoint security suite] is using a sledgehammer to crack a nut," said Lambert.

Our business is to secure your business.

ESET NOD32 Antivirus 4

Fast, Effective, Proactive, Antivirus and Antispyware

Our award-winning proactive threat-detection technology delivers the most effective protection from viruses, spyware, and other internet threats. ESET software blocks most threats the moment they are released, avoiding detection latency common to competing products. And with super-fast, super-easy operation, we keep your users productive, and your help-desk load down.

www.eset.com

eset

Resources from ESET

ESET NOD32 Antivirus 4 Trial

PCI DSS v1.2: Best Practices and Useful Tips

Regulatory Compliance Alignment: How Antivirus Supports Your Compliance Initiatives

About ESET
ESET provides award winning security solutions that combined fast system scans with the ultimate in proactive protection against both known and unknown online threats. ESET NOD32 Antivirus was awarded "The Best Proactive On-demand Detection" and "The Best Overall Speed Performance" for 2008 by AV Comparatives.

By delivering state-of-the-art endpoint security, ESET Smart Solutions™ increases your security while reducing your TCO. ESET's updated Remote Administrator delivers a highly scalable enterprise-ready defense against malware, reducing your attack surface resulting in fewer help-desk loads. A light system footprint and blazing fast scanning speed can even extend the useful life of PCs and laptops.

ESET has also been named to the INC500 for the third consecutive year, and has an extensive partner and customer network, including corporations like Intel, Canon, Dell and Microsoft.