

REPRINTED from

# COMPUTERWORLD®

THE VOICE OF IT MANAGEMENT ■ WWW.COMPUTERWORLD.COM

NOVEMBER 6, 2006

## Macs and PCs, secure together

Attention small enterprises: Relax, Sophos understands you

BY RYAN FAAS

**November 06, 2006** (Computerworld) Small businesses and their networks present a unique security situation. Often such setups can be managed without a full-time systems administrator and possibly without the investment of anything more than a single server for sharing documents and printers. However, despite their modest needs, they are still at as much risk for certain security threats as any larger organization. To the rescue? Sophos, whose new \$362 [Sophos Security Suite](#) is designed with the understanding that small-business needs can be as complex (hack and malware attacks, mixed PC-Mac installations, hectic schedules) as their administration resources are basic.

The security needs of smaller businesses are often not well understood because of their limited (or nonexistent) IT staffs. Even if needs are clear, a lack of funding for large-scale solutions or a lack of expertise in managing solutions appropriate to an enterprise environment can prevent proper security from being implemented.

If I were to say nothing else about the most recently released Sophos Security Suite for Small Business version 2, I'd have to say that the developers truly did understand that customer. From installation and remote deployment to the central configuration of anti-virus, malware, and firewall features to the reporting and resolution of threats, it's clear that Sophos designed this product to be as easy to use and understand as it is effective in promoting solid small network security.

### Simple installation and deployment

The Security Suite's ease of use starts at installation. Though the process does require some modification of the settings of Windows XP's built-in firewall to allow for remote deployment, the process was simple and straightforward.

Sophos recommends that users install the Control Center, which provides centralized management of all features on all supported clients and remote deployment for all Windows 2000/XP clients and 2000/2003 servers, on a Windows 2000/2003 server. That server could be a dedicated security server or one that is being used to provide other network resources. That said, if a server is unavailable, the Sophos Control Center can be installed on a Windows 2000 client or XP PC, though performance will be reduced. A management console for the Sophos Control Center can also be installed on additional computers for remote management purposes.

Not only is the installation painless, but the initial setup wizard is equally intuitive, identifying each step in the process clearly and with language that virtually anyone proficient in using Windows can understand. As part of the initial nine-step setup, current updates are downloaded, the owner's account is verified with Sophos, and the installer gets the option to immediately deploy antivirus and firewall protection.

Remote deployment relies on either Active Directory or NetBIOS to locate computers within a network. Although the deployment features can locate all supported computers in a network (Windows 2000/2003/XP, Windows 98/Me, and Mac OS X), remote deploy-

ment is only supported for Windows 2000/2003/XP PCs.

(Vista will also be supported when available.) For other clients, the control center creates a share that can be mounted for installation. As with remote deployment, the Sophos Firewall can only be installed on Windows 2000 and XP client machines; it is not supported for use on servers.

Provided that the same administrator account name and password exists on all machines supporting remote deployment (which would be the case in an Active Directory domain), you can simply select the computers onto which you wish to install Sophos Anti-Virus and/or Sophos Firewall. The wizard will provide you a list of clients that don't support remote deployment, which you can print out and use as a checklist for manual installation. Once the wizard completes, the selected software will be automatically installed on each remote computer without any further intervention.

### Simple, clear interface

The interface for the Sophos Control Center is equally intuitive. It provides a list of all clients that are being centrally managed, which components are installed, and the status of the machines' virus definitions, firewall, and any current alerts. Above this list are summaries of any current threats, traffic being blocked by client firewalls, and potentially unwanted applications.

Links to the left of the list provide easy access to wizards for manually updating the virus definitions (first on the computer running the Sophos Control Center and from that computer

to every computer in the network), protecting additional computers, and resolving any current threats. There are also links to equally intuitive wizards for configuring virus scanning, automatic updates, how users or administrators are notified of threats and other problems, and managing client firewall configuration. Once again, I have to say that **Sophos really nailed the interface for ease of understanding and use.**

Most of the configuration wizards will be familiar and easy to navigate for anyone who has ever worked with any antivirus software. However, the firewall configuration wizard deserves some special attention. Sophos provides varying levels of complexity in the firewall configuration depending on the expertise of the user. It can be as simple and basic as the Windows XP firewall, providing a default setting of blocking all incoming traffic or it can provide more granular control for less experienced users needing to create rules for specific applications or it can provide a complete rule-based interface for experienced network managers.

### **Powerful features**

Ease of use would be meaningless if powerful features weren't on board. **Sophos's anti-virus solution is comprehensive, with features such as genotype and behavioral genotype protection that allow the software to detect potential viruses before definitions for a virus are released.** Genotype protection, which looks for the file characteristics of known viruses, and behavioral genotype protection, which looks at which APIs and resources a process or application is accessing, provides a greater chance of identifying new viruses.

Since these features rely on constantly accessible rule sets, they enable Sophos to identify viruses before they run, thus preventing potential damage.

I also liked the Potentially Unwanted Applications feature, which allows users of the Suite to create a list of trusted processes. Applications outside this list will simply not be allowed to run. It's slightly misnamed — the name and description of this feature implies that it can be used to control which applica-

tions may be run on the computer (i.e., to prevent an employee from playing Solitaire all day long).

While it will intercept many peer-to-peer file sharing applications as well as some remote management tools, this feature is designed to block adware and spyware processes rather than full-blown applications. It's effective with minimal setup. It's also simple to allow additional applications or to track down processes that are mistakenly identified and disabled.

The package includes respectable reporting capabilities. Reports can be generated manually at anytime, or forward-thinking users can set up schedules and automation. Reports are viewable within the Sophos Control Center, or the software can automatically e-mail them to a designated address — especially handy for small businesses that have outsourced much or all of their IT support.

### **Complements network protection, doesn't replace it**

Given its feature set, some businesses might assume that the Sophos Security Suite provides all the security they need. The features of this product are impressive, but they don't remove the need for a network firewall or other intrusion prevention technologies. The product is designed to protect workstations from common threats — viruses, malware and internal network attacks — that a network-wide solution cannot.

The client firewall feature is intended to complement, not to replace, a network firewall, and does the job in two ways. First, it prevents attacks from other computers on the same network (either by a malicious user or by a malware infected computer). Second, it provides added security for mobile computers that are taken off the network and used by employees on the road or at home, where they would normally have minimal or no protection.

### **Less intuitive cross-platform support**

Probably the only area of use that I found less than intuitive was the process of managing Mac OS X clients. Although the process of loading the Mac OS X antivirus software was very sim-

ple, there were times that I found locating Mac clients for remote management to be somewhat difficult. I had little trouble locating Macs that were bound to an Active Directory domain using Apple's Active Directory plug-in, but locating Macs in other configurations was more hit or miss. However, it's possible to configure the Mac client to query an internal server for updates, which provided a relatively easy workaround. Also, some additional documentation for organizations using Macs as well as PCs would have been helpful.

### **Flexible licensing, 24/7 tech support**

Sophos offers a flexible licensing model for the Small Business Security Suite. Pricing is based on both the number of seat purchases and the length of support contract. During the term of the support contract, users get free 24/7 technical support as well as access to all application updates released during the contract. This provides companies with the knowledge that they will receive as much support as they need, a plus for businesses employing very limited or no permanent IT staff. However, some businesses may balk at the support contract model, preferring a one-time expense.

Having worked with small businesses both as an IT manager and as a network support consultant, I have to say that I had high standards for the Sophos Security Suite for Small Business. I expected it to both provide powerful centralized management for all client security needs as well as an intuitive interface that could be used by both experienced systems/network administrators and users that had only basic desktop support skills. Sophos managed to hit the mark on both of these points for Windows 2000/2003/XP networks.

**For small businesses relying solely on Windows 2000 and better PCs and servers, this product is an excellent solution. For more diverse networks that include Macs and PCs running Windows 9x, it is a good, if not perfect, choice.**

The logo for Sophos, consisting of the word "SOPHOS" in a bold, blue, sans-serif font.