Protecting Your Computer

Protecting The Computing Endpoint

(NAPSA)—Information technology is everywhere. At home, at work, at school, at the corner store, in coffee shops, libraries, airports and everywhere in between. In fact, advances in information technology and the Internet have made the world a highly interconnected place where people across continents can communicate and transact business in near real time.

And new computing devices make it even easier. On-the-go professionals take their laptops on the road and hook up to different wireless networks to work on business and personal tasks. With an Internet connection and their laptop, they can bank online, check stocks, catch up on news, shop for a new ring tone for their phone, check work and personal e-mail, play games, download music and more.

Smartphones, portable music players, thumb drives and other peripheral devices also make computing convenient and simple.

The trouble is, these devices—called “endpoints” in technology vernacular—also represent potential targets for hackers and their malicious code. By hitching a ride on a vulnerable laptop, smartphone or even a home desktop computer, hackers not only gain access to the information that resides on the hacked system, but they can also sneak onto a corporate network when the unsuspecting user connects from home, the road or elsewhere.

These possibilities are causing businesses of all sizes to re-evaluate how they deal with such devices. Outfitting each device with individual security products is not an option. On one hand, today’s threats are so sophisticated that they require specific security technologies. For example, viruses and Trojan horses are stopped by antiviruses, while spyware and rootkits are addressed by antispyware. Worms can be stopped by a firewall, while intrusion prevention technology can thwart buffer overflow and so-called “zero-day” exploits. Identity theft can be managed by device control solutions, and network access control tools can prevent unprotected endpoints from connecting to the company network.

On the other hand, installing such a collection of products would likely overburden any device and lead to incompatibility problems, management challenges and so on.

Fortunately, there’s a better way. Software vendors are introducing an innovative new tool that combines all of these essential security capabilities in a single, integrated solution. Not only does this next-generation tool deliver a complete range of security technologies, but it also works together with technology that ensures that every device connecting to the company network is properly protected.

As a result, end users and businesses benefit. End users benefit by knowing they are not the unwitting conduit through which malicious code can enter their company network. And businesses benefit by knowing that any laptop, smartphone, desktop or other device that interacts with the network has been audited for compliance with security standards and is only allowed access once it meets such standards.

Perhaps one of the most compelling aspects of this advanced new tool is its remediation capabilities; that is, any device that falls short of the established security requirements is brought up to standards—automatically.

The security and management implications of such a solution are significant, as businesses and their employees finally have a simple yet reliable way to protect valuable information assets while leveraging their computing devices of choice anytime, anywhere.

For more information about protecting your computing endpoints, visit www.symantec.com.