

# Are you secure?

Defining true zero-day protection and unified threat management **Interviewed by Troy Sympson**

**T**he realm of Internet security is ever-changing and often confusing, even to the savviest IT professional. Hackers are creating new malware, spyware and viruses practically by the minute, and if you're not protected, your company is in danger of losing customer trust, putting yourself at a competitive disadvantage or even opening yourself up to legal troubles. Simple virus detection isn't enough anymore, according to Craig Davis, executive vice president of SLPowers. With so many servers and computers online these days, viruses propagate so quickly that millions of computers can be infected before anti-virus software even knows that virus exists.

"Your network firewall may not be doing all that it should be doing," Davis says. "Companies today need a firewall that offers multiple levels of protection, including junk e-mail filtering, anti-virus capability, an intrusion detection or prevention system, and World Wide Web content filtering, on top of traditional firewall features. These application-layer firewalls use proxies to process and forward all incoming traffic, though they operate in a mode that is transparent to the end user. Companies need to do more than just monitor their Internet traffic, they need true zero-day protection and unified threat management."

*Smart Business* asked Davis what true zero-day protection and unified threat management mean and why they're so important in today's business climate.

## What is true zero-day protection?

One-day protection would mean that an attack can be handled within one day of identifying it, but we understand that businesses cannot be inoperative for an entire day. Zero-day protection refers to the ability to defend against threats that are not yet known. This way when a new attack emerges, there is no window of vulnerability for the network being attacked. There are many new attacks launched each year; however, most of these attacks use techniques closely related to previous attacks.

Nevertheless, zero-day protection requires our ability to identify an attack-like behavior and be able to respond to it, even if the attack is not yet identified. By understand-



**Craig Davis**  
Executive vice president  
SLPowers

ing the typical classes of attacks, defense mechanisms can be developed that defend against whole classes of attacks. This is much more effective than the reactive, signature-based technologies that rely on fingerprinting each new attack as it emerges.

## Why is the 'true' so important?

Many vendors make zero-day claims, but in reality, their security solutions rely solely on signature-based scanning. Signature-based security technologies fingerprint each new attack after it emerges, so protection comes when this fingerprint, or signature, is added to the system. Although they have some very good global methodologies for quickly detecting new threat outbreaks and updating their signatures, this is not zero-day protection. By their nature, signatures are reactive; they cannot protect against new, previously unknown attacks until an update is available. But this technique is only one piece of a complete solution. You need zero-day protection combined with robust signature-based scanning to have comprehensive unified threat management.

## What is unified threat management?

It is an emerging trend in the appliance security market referring to the ability to

manage all potential security threats using a single device. Unified threat management appliances have evolved from traditional firewall and VPN appliances into a solution that has many additional capabilities, such as URL filtering, spam blocking, spyware protection, intrusion prevention and gateway anti-virus, as well as centralized management, monitoring and logging capabilities, all functions previously handled by multiple systems.

## What are the benefits of unified threat management?

Unified threat management solutions are significantly more efficient with regards to cost, management and space efficiency. Integrating multiple security capabilities into a single appliance means that you can purchase and use fewer appliances, eliminating the cost of building layered security with separately purchased solutions and training on each of those devices. Plus, it stops attacks at the network gateway. The multilayered security approach offered by unified threat management appliances lets you avert catastrophe by blocking a broad range of network threats before they have the opportunity to enter your network. Malicious code will not have the opportunity to disable security at the desktop or server level, and business-critical files and applications remain available to keep employees on the job.

Using separate security systems for layered security means also using different management consoles to configure each system. Because the management paradigms of these systems are typically very different, it is time-consuming to make sure the different security policies on each system work together to provide adequate protection. Log information that is stored in different formats and in different locations makes detection and analysis of security events difficult.

**CRAIG DAVIS** is the executive vice president for SLPowers in Boca Raton, Fla. Reach him at [cdavis@slpowers.com](mailto:cdavis@slpowers.com) or (561) 886-5090.

**Insights Technology** is brought to you by SLPowers