

Noteworthy Security Companies Newer Approaches To Stay Ahead Of Threats

5/01/2007

IT staff trying to stay a step ahead of malware must run as fast as they can just to stay even. However, effective new tools are coming onto the market that coordinate and incorporate different approaches to security. Many of these tactics consist of what Info-Tech Research Group calls “adaptive security,” which provides consolidated management of systems, users, and data sources to help ensure security. Yet security cannot be allowed to make the network inaccessible or cumbersome for valid users.

Today’s bad guys are criminals trolling for passwords, looking for client credit card information, and basically treating the corporate network as a place ripe for theft. Add to that the fact that today’s small to midsized enterprise is juggling many aspects of security, from intrusion detection to network behavior analysis to virus scanning, and there is a need to gather all of this diverse data and centralize control of the security function. Three companies in particular have newer, unique approaches to security.

Steelcape

“Typically, management is concerned about security. The IT people are concerned about accelerating data. Our goal is to give both what they need,” says Dean Norman, vice president of sales at Steelcape (www.Processor.com/Steelcape-Inc). Steelcape’s approach allows sending data without opening ports. “Everyone has firewalls and open ports. We strive to capture functionality without bothering users.”

Steelcape provides security without layering multiple security protocols, each trying to solve TCP/IP’s security requirements. Steelcape’s approach to the TCP/IP transport layer eliminates the need to open ports, which all but kills the opportunity for security breaches.

One concern for both users and vendors is not getting too far ahead of the curve. “Our approach is easy to try and takes only minutes to set up,” says Norman. It has zones, similar to those used on VLANs. One would expect those using LDAP or Active Directory to have rules in place, but there are several reasons why it does not happen, he says, noting the problems some SMEs have implementing the rules.

Ironically, some of Steelcape’s advances go back to the days of token ring and AppleTalk networks. “They had a lot of functionality,” Norman notes.

Steelcape provides secure interaction by reducing the complexity of security architecture, improving TCP/IP performance by up to 30%, and closing ports to eliminate hacker paths, Norman says. In addition, it provides segregation, digital signature management, and encryption.

Steelcape lets secure data traverse the traditional firewall unhindered. “Our unique protocol lets SMEs use encryption, digital signatures, and a faster communication speed than using the traditional TCP/IP technology for communication,” Norman says. He adds that the solution is not a replacement for TCP/IP but an alternative way of communicating between hosts. “It is 100% compatible with existing TCP/IP version 4 and 6,” he adds.

Because of this flexibility, it makes an ideal VPN or VLAN alternative. Steelcape can be deployed from either a hardware appliance version or specific platform software-based agent.

A user who wanted to test it could set up the basic point-to-point implementation. “It takes minutes to show results,” Norman says. With the product’s Enterprise Manager, users can see adequate reporting, managing of the digital signatures, and encryption rules. It works with all flavors of Windows, as well as Linux, AIX, HP-UX, Solaris, and AS/400. It requires 64MB of free memory, 200MB of disk storage, and at least 5GB disk storage if the reporting option is enabled.