

IdeaByte

Managed Security Monitoring: The Domain of Counterpane

March 31, 2000

Steve Hunt

Catalyst

Analyst observations

Question

What is managed security monitoring?

Answer

A comprehensive security architecture must include some way of determining the current state of security at any point in time. Traditionally, system audit logs served this purpose. But, many companies complain of having inadequate resources — either security staff or money — to monitor those logs. In response, dozens of consulting and software firms are responding with a range of outsourced services that include monitoring these logs. A close look at those services, however, shows that the actual daily monitoring of back office systems will have to be done by a focused, dedicated 24x7 operations center. Most of these consulting firms are not in a position to host such an operation.

Giga believes that outsourced monitoring will provide a viable and sustainable market for a fairly small number of managed security monitoring service providers. These providers will likely resell their dedicated monitoring service to the individual consulting firms. In the year 2000, two or three firms will offer dedicated monitoring services, and will sell those services wholesale to countless consulting firms [9p].

The newest of these firms, **Counterpane Internet Security** (www.counterpane.com), is the one best positioned to capitalize on the emerging managed security monitoring market. Counterpane combines a highly skilled security staff with a business model focused on providing managed security monitoring. Other firms who will claim to offer similar services will not, in fact, have as viable a business model as Counterpane.

ISS (www.iss.net) for example, acquired **Netrex** last year. Now ISS is promoting a service called ePatrol that combines the outsourced services of firewalls, virtual private networks (VPNs), perimeter intrusion detection and network monitoring. While ISS can make similar claims as Counterpane — profiting from experienced security staff, tracking all new security threats, and 24x7 monitoring — ISS's service is limited to monitoring ISS brand devices, with very few exceptions. Counterpane, on the other hand, is vendor-neutral in the sense that any system, from the mainframe to the Windows 2000 domain will be monitored.

The market for managed security in general is growing. Giga has found that nearly half of all companies who outsource their firewall today would be willing to outsource the daily monitoring of system logs. That ratio will be much higher among those companies that outsource the physical firewall box, the configuration, or the auditing of the firewall. In addition, well over half of all companies who hire outside monitoring of perimeter intrusion detection would consider hiring a managed security monitoring provider.

Managed security monitoring will explode during the next three years as corporations realize the extent to which e-business initiatives require a comprehensive security posture. Counterpane is kicking off the next big trend in security outsourcing.

© 2000 Giga Information Group