



CMP

United Business Media

InformationWeek

Business Innovation Powered By Technology

Feb. 6, 2006

TECHPORTAL

SECURITY

Data Security Deluge

The popularity of security-management software rises as more vendors enter the market and prices fall

WHEN SOFTWARE DESIGNED to manage the loads of information collected from security systems debuted a few years ago, its high cost and complexity stood in the way of its adoption. Yet for some businesses, managing such data is now a requirement in order to comply with government regulations on the collection and retention of data.

Nowhere is this pressure felt more than in the health-care and financial-services markets. Take Genesis HealthCare, which finds itself needing to comply with state data privacy laws in the 12 states where it operates, in addition to compliance with various federal laws. "Firewalls alone produce reams of [data] logs per week," says Bruce Forman, director of information security for the \$1.5 billion-a-year health-care provider, which has more than 200 locations, 400 servers, and 38,000 employees.

Once companies get past the up-front investment, security-management software can save them time and

More Security

Worldwide revenue from security information- and event-management software



Data: IDC

check to see if a setting on a password policy is compliant with the company's overall password policy or if an FTP event is starting on a server where it's not supposed to. "Security information- and event-management software isn't new; the main thing that's changed is that now we're in a world that's more heavily regulated," Forman says.

At least two dozen companies offer this type of software, including big

NetIQ, Network Intelligence, and Symantec. IDC projects the market for security information- and event-management software will grow to more than \$635 million in sales by 2009, up from \$267 million last year.

Genesis is using ArcSight's Enterprise Security Management suite of software, which has helped to consolidate threat information that affects its Linux, Unix, and Windows systems. Genesis feeds ArcSight ESM with data from its open-source Nessus vulnerability-scanning software, intrusion-detection systems, and firewalls in an effort to help Forman figure out how to prioritize his security responsibilities.

"You can also designate which systems in your environment have to adhere to different regulations," such as the Health Insurance Portability and Accountability Act or Sarbanes-Oxley, Forman says. "Assuming you can figure out the most important things to look for, then having something that puts all of your log information in one place gives you some comfort over how well you're doing keeping your network secure."

In a move to extend its appeal to companies under the gun of regulatory compliance, ArcSight last week disclosed details about ArcSight's Compliance Insight Packages, which works with the company's ArcSight

SECURITY-MANAGEMENT APPS CAN SAVE COMPANIES TIME AND MONEY.

money by automating controls that make sure their systems are in compliance. It will let users, for example,

vendors such as Cisco, Hewlett-Packard, and IBM and pure-play security vendors including ArcSight, McAfee,

ESM software and follows National Institute of Standards and Technology standards to provide 85 reports that assess the effectiveness and internal controls necessary to keep security efforts in sync with regulatory requirements. The Compliance Insight Packages module is scheduled to ship by June.

The key to making such software accessible to small and midsize businesses is making it more affordable. Gartner's June Magic Quadrant report for Security Information and Event Management technology estimates that initial software deployment costs are in the \$200,000 to \$400,000 range,

in addition to a substantial investment in server hardware, storage, database software, and implementation service.

The good news: As demand for security-management software grows, prices appear to be dropping in some cases. ArcSight says the starting price for its Enterprise Security Management software suite is about \$75,000, and competitor eIQNetworks launched Enterprise Security Analyzer 2.1, which starts at about \$56,000.

Some business-technology managers have had a hard time in the past justifying to upper management

spending on security because the return on such investments isn't easily quantifiable. But security-management software, with its ability to help IT professionals better understand threats and enhance a company's ability to deal with those threats while ensuring compliance with government rules, is becoming more appealing. As for return on investment, preventing a single attack that could lay waste to a company's tech infrastructure or avoiding hefty fines for violating regulations turns out to be a pretty good return.

—LARRY GREENEMEIER
(lgreenem@cmp.com)

The logo for ArcSight features the word "ArcSight" in a sans-serif font. The "Arc" is in red, and "Sight" is in black. To the right of the text is a stylized icon consisting of a red arc and two black lines that intersect to form a shape resembling a lens or a camera viewfinder.

ArcSight, a leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM™ enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading worldwide companies across many verticals—and more than 20 of the largest U.S. federal agencies. For more information, visit www.arcsight.com.