



Get ready to pull the plug on

# Legacy Log Management

COMPLIMENTARY  
WHITE PAPER  
[Read now >](#)

[Access Control](#) [Application Security](#) [Authentication](#) [Data Security](#) [Privacy](#) [Identity Management](#) [Security Monitoring](#) [Wireless Security](#)

## Feeling vulnerable? Try assessment tools

Ellen Messmer (Network World) 27/07/2004 08:54:34

It was a requirement that come June, high-volume merchants and payment processors that do business on the Web and want to work with MasterCard International had better have conducted quarterly vulnerability assessments of their Web sites. MasterCard warned last year that it won't do business with them otherwise.

"We believe the majority of events we read about with worms could be averted through vulnerability assessment," says John Verduschi, vice president of e-business and emerging technologies at MasterCard, which has drawn up a list of a dozen approved network-based scanning services, including Ubizen, its preferred provider.

With an estimated 7 percent of all of MasterCard's US\$921.6 billion in annual card purchases now taking place on the Web, it's no wonder that the global payments company is making vulnerability assessment mandatory.

And with companies like MasterCard requiring its partners to use such offerings, it's also no wonder there are dozens of vendors competing in the market, which makes choosing vulnerability-assessment options a challenge.

One way to narrow down the choice is to determine whether a host- or network-based offering best meets your needs.

Host-based tools reside on servers and desktops as software agents that can log on to a host to report back to a management console. Competitors in this market include Bindview, Computer Associates International, Harris International, IBM, Internet Security Systems, Sanctum and Symantec.

On the other hand, network-based tools scan remotely in ways similar to a hacker probe. Some of the players are the same as in host-based vulnerability assessment, such as IBM, ISS and Symantec. Others, such as nCircle Network Security and Qualys, specialize in network-based offerings, and freeware such as Nessus also has supporters.

There are pros and cons to each approach.

Host-based tools are generally more expensive, says John Pescatore, a security analyst at Gartner. The products can cost US\$750 to US\$1,000 per server, which adds up across a big network.

But host-based offerings provide rich information, which might explain why a third more host-based products than network-based ones are sold annually.

"They can do several things you can't do from the network, such as check user access logs or who touched the financial data on a server," Pescatore says.

The downside of host-based offerings is that computers have to be idle to do security checks, says Bill Kline, senior security engineer at US-based Paymentech, one of the high-volume credit card processors asked by MasterCard (and Visa) to follow new guidelines this year. Staff must carefully schedule inspections, and if host-based tools aren't used correctly they can damage data on a server, he adds. Paymentech uses Symantec's host-based Enterprise Security Manager and network-based offerings from KaVaDo and TruSecure to keep its 600 servers secure.

Network-based vulnerability assessment comes in the form of hardware, software or services. As with many offerings, vulnerability-assessment services are a good option for organizations short on IT staff or security specialists.

"We had constraints with resources," says Dan Klingler, manager of information security at Hershey Foods. Using the Qualys service lets Hershey centrally scan 325 Windows NT servers and 125 Unix servers without adding staff.

Drazen Drazic, general manager of Security-Assessment.com, distributor of QualysGuard in Australia concurs with Klingler. "We've found that organisations are looking for solutions that automate vulnerability assessment as much as is possible, to protect them against all new and emerging threats and without requiring a huge human investment.

"QualysGuard is providing our clients with a solution that has the smarts built into the system and results are consistent no matter who the system operator is or where QualysGuard is run from."

Network-based offerings can cost from a few hundred to thousands of dollars per month, depending on the number of IP addresses and other variables. And custom services can usher in customer-based pricing. MCI's Digex Web-hosting unit utilizes Sanctum's AppScan application scanner and Symantec's NetRec as well as the host-based Enterprise Security Manager as part of a custom service. There's no set monthly fee, but setup starts at US\$10,000.

Drazic said QualysGuard has pricing structures to suit small to large enterprises and consultants alike. Pricing can be subscription based, allowing organisations unlimited scanning of all their servers, PCs and networking devices for a 12 month period. This is priced from as AUD\$6500 through to clients having the ability to pay per scan and which starts from AUD\$12.

### The down side

Deploying network-based vulnerability-assessment tools can present some pitfalls.

Problems can arise when scanning internal servers, desktops and public-access Web servers. That's because firewalls and other means of blocking off sub-nets are often already in place to deter this kind of inspection.

In addition, if there's no coordinated staff approach, network administrators might think the network is somehow under attack because of the scans.

"It takes special coordination with the intrusion-detection systems and the firewall people," says Don Jankowski, manager of technology risk management at Xcel Energy, about his recent experience in deploying the proVizor Security Risk Measurement network-based scanner from Black Dragon Software.

It took Xcel, the fourth-largest electricity and gas energy company in the US, a few months to install and train IT staff to begin using the four proVizor appliances it purchased to scan for vulnerabilities across its network of 800 servers and 14,000 desktops across 12 states.

Jankowski says the company has plans to do a complete scan of its environment every quarter, but far more frequently for critical workstations. Operating systems are being scanned first, applications next.

Robert Geiger, director of Unix administration and security at Reader's Digest Association, says it's a good idea to have the testing provider clearly define in advance what it plans to do, including any denial-of-service attacks. And if the question comes up, say 'no' to hiring hackers past or present as a matter of trust, he adds.

Ken Saruwatari, product manager at Foundstone, which makes the Foundstone Enterprise scanner used mainly by large companies, says scans can be traffic-intensive and therefore most organizations do them during hours when the network is least in use for business purposes.

Network-based vulnerability-assessment products are increasingly becoming available as appliances, which can make them easier to deploy than host-based software. Computer Associates, Foundstone and PredatorWatch are among the companies selling such boxes.

Some observers say going with host- or network-based tools isn't necessarily an either/or situation.

"In IT, everyone always wants one tool for everything," says Anthony Passaniti, head of IT security for the global reinsurance firm Swiss Re, which uses a variety of network- and host-based tools. "But a skilled craftsman needs a tool kit with specialized tools."

The Swiss Re division uses Application Security's network-based AppDetective for its databases because it focuses on database vulnerability checking, Passaniti says.

Eric Pulaski, CEO of security products vendor BindView, says no one vendor offers it all in vulnerability assessment. His company makes host-based vulnerability-assessment agents for software from Check Point Software Technologies, Microsoft, Novell and others as well as a network-based tool that can be used to locate rogue computers, but the company doesn't have an agent for every popular application. The same is true of even bigger companies, such as CA and IBM, he says.

[Add to iGoogle](#)

[Print this story](#)

[Digg this story](#)

More by [Ellen Messmer](#)

**Top Stories** **Most Popular**

- [World Cup security: Preparing for the unexpected](#)
- [Uni CIOs call for greater copyright law protection](#)
- [Enterprise risk management: all systems go](#)
- [Why your information security stinks & what to do](#)
- [Security experts wrestle with cyberattack scenario](#)

### Additional Resources

Newsletter Subscription

Sign up for our CSO Online newsletters!

CSO Online Data Security Briefing [Weekly]

CSO Online's weekly briefing for data security executives helps identify the data security factors that put business success at risk, and offers technical, operational or procedural safeguards.

[Join](#)

RSS Feeds

**RSS**

[Show all RSS feeds](#)

### News

- [Intel's McAfee acquisition a mobile play](#)
- [Intel to buy McAfee for \\$US7.68 billion](#)
- [Facebook location service unlikely to have game component](#)
- [Swedish Pirate Party to host Wikileaks servers](#)
- [Telcos set to dominate cloud market over next two years: analyst](#)

[More >](#)

COMPLIMENTARY WHITE PAPER

Get ready to pull the plug on

## Legacy Log Management



**Most Popular** **IT Media Releases**

- [Cloud still too dark for legal information](#)
- [APAC security software revenue to grow 17.8 per cent this year: Gartner](#)
- [Telcos set to dominate cloud market over next two years: analyst](#)
- [gotalk PrePaid VoIP To Challenge Skype in Australia and New Zealand](#)
- [Law enforcement push for stricter domain name rules](#)

### Get a job



- [Test Analyst](#)
- [IT Project Manager & Program...](#)
- [Oracle onDemand Programmer](#)
- [Project Manager - PRINCE2 / PMBOK](#)
- [National Executive Projects...](#)

### Whitepaper



### Pulling the Plug on Legacy Log Management

When it comes to log management, CSOs have been left in the lurch. According to this IDG Research Services survey, organisations are poised to "rip and replace" legacy technology for better compliance and security. Read more.

[Read Whitepaper](#)