



Research News

- Applications & Software
- CIO Topics
- Consumer Electronics
- Industry Specific
- Networks & Telecom
- Platforms & Peripherals
- Security
- Semiconductors
- Services
- Vendor Topics

Analyst Café

Directories

Events

advertisement

Research News

Filed under: Security

[» Get The Weekly Research News Recap](#)

Gartner: Top 5 Steps to Dramatically Limit Data Loss and Information Leaks

Gartner, Inc. - August 10, 2006

Public exposure of private data is becoming a regular occurrence, but the majority of these incidents can be prevented if companies implement the proper security best practices, according to Gartner. Gartner analysts have identified the top 5 steps to prevent data loss and information leaks. The first is deploying content monitoring and filtering.

"From lost laptops to misplaced backup tapes to accidental e-mails filled with sensitive information, we seem to be in the midst of a data loss epidemic, with tens of millions of individuals receiving data loss notification letters this year," said Rich Mogull, research vice president for Gartner.

"Data loss and information leaks are not random acts of nature too costly to prevent," said Mogull. "By following these five steps, enterprises can dramatically reduce the risk of their valuable structured or unstructured information ending up in the wrong hands and forcing an embarrassing public disclosure."

The top 5 steps to prevent data loss and information leaks are the following:

1. Deploy Content Monitoring and Filtering (CMF). A CMF solution monitors all outbound network traffic and generates alerts regarding (or sometimes blocks) activity based on inspecting the data in network sessions. CMF tools monitor common channels, including e-mail, IM, FTP, HTTP and Web mail (interpreting the HTTP for specific Web mail services) and look for policy violations based on a variety of techniques.

"CMF tools are best at detecting and reducing information loss from accidents, such as e-mailing the wrong file to the wrong person, or bad business process, such as exchanging HR data over an unencrypted FTP connection," said Mogull. "CMF won't stop all malicious activity and can be circumvented by a

More Current News



- » Personal Data Protection Concerns Continue in Japanese Financial Services Industry, Says Celent
- » Endpoint Authentication/NAC Technologies Top Global 2000 Security Priorities, Says TheInfoPro
- » Majority of Home Wi-Fi Users Are Securing Their Networks, Says JupiterResearch

News from this Firm



- » **Gartner Releases 2006 Emerging Technologies Hype Cycle and Priority Matrix**
- » **PDA Shipments Reached Record High in Second Quarter of 2006, Says Gartner**
- » **Business Activity Monitoring to Drive Technology Innovation for Investment Services Firms, Says Gartner**

Directory



- » Gartner, Inc. Firm Profile
- » Gartner, Inc. Analyst Profiles

knowledgeable attacker. Still, most information leaks are the result of these accidents or bad processes, and CMF is evolving rapidly to address more malicious attacks."

2. Encrypt Backup Tapes and (Possibly) Mass Storage. Gartner analysts highly doubt that many of the reported lost backup tapes containing consumer records eventually result in fraud. However, because there is no way to know for sure, companies have to assume exposure anyway. Encryption can ensure that the data will still be safe.

"During the past few years, tools have emerged that significantly improve the performance, manageability and simplicity of encryption," said Mogull. "For large tape installations, we recommend in-line encryption appliances. For tape drives connected to local systems or servers, companies may want to consider software encryption. Older mainframes may need an in-line appliance with an adapter for mainframe protocols, while new software solutions can take advantage of extra processors or cryptographic coprocessors in more current models."

3. Secure Workstations, Restrict Home Computers and Lock Portable Storage. Workstations and laptops can be a major source of loss, especially when a poorly configured or out-of-date enterprise or home computer is compromised by a virus or worm, and by losing portable storage media, such as a Universal Serial Bus (USB) drive or CD-ROM.

"There's really no excuse for not keeping an enterprise system up-to-date with the latest patches, a personal firewall, antivirus and anti-spyware software," said Mogull. "These precautions alone will prevent the vast majority of commonly encountered Internet attacks."

4. Encrypt Laptops. If organizations give employees portable computers, employees will store sensitive data on it. Policies don't matter: Users will always use the tools they acquire, and sensitive data will always end up in unexpected places.

"There is only one tool to protect sensitive information on a lost laptop: encryption, preferably whole-drive encryption from a third-party vendor," Mogull said. "Whole-driven encryption, as opposed to file and folder encryption, involves very little user action, protects all data on the computer, and is not vulnerable to the same kinds of recovery techniques that skirt the protections of passwords or other controls."

5. Deploy Database Activity Monitoring. Most organizations struggle to secure existing databases that are rarely designed with effective security controls. While companies eventually need to encrypt some of the data in their databases, database activity monitoring is a powerful security control that's easier to implement and more viable than encryption for many types of data.

"Database activity monitoring tools observe all activity within a database, record this activity in a secure repository and generate instant alerts for unusual activity," Mogull said. "Through detection of unusual behavior, database activity monitoring can limit insider misuse of database systems, enforce separation of duties for

Next Events for this Firm



- » Economics of IT Conference - August 22, 2006
- » RetailVision Fall - August 28, 2006
- » Financial Services Technology Summit - August 28, 2006

Research News Recap

The Weekly Research News Recap - *published weekly*

A recap of the Research News published over the previous 7 days, organized by category and date.

Delivered by email, every Friday morning.

Who should subscribe?

- Anyone interested in research produced by the high tech industry analyst firms
- High Tech Product Professionals
- Corporate Librarians
- Consumers

» [Opt in for this Free Newsletter](#)

» [See a sample](#)

database administrators and limit certain external attacks, all without affecting database performance."

About the market research and advisory

Additional issues related to the state of the security industry will be presented at the Gartner IT Security Summit, September 18-19, at the Royal Lancaster Hotel in London.

Also see the Gartner Security and Privacy practice area, at the link below, for links to free and premium Gartner content.

» [Story on Analyst Firm Website](#)

» [Discuss this story at Tekrati Weblog](#)

© 2000-2006 Tekrati Inc., All rights reserved. (650) 839-1000

[Legal Statement](#) • [Privacy Policy](#) • [About Tekrati](#) •  • [Be a Sponsor](#) • [Tekrati Weblog](#) • [Analyst Profiles](#)