

Reduce the Risk of Data Leaks With Content-Filtering Tools

Rich Mogull

A major leak of health information highlights the risks posed by failing to protect sensitive data from exposure. Content-filtering tools offer a simple, cost-effective solution to this problem.

NEWS ANALYSIS

Event

On 20 February 2005, public health authorities in Palm Beach County, Florida, acknowledged a major leak of confidential medical information. A county employee mistakenly attached a list of patients infected with HIV (human immunodeficiency virus) to an e-mail message addressed to several hundred recipients.

Analysis

The leaking of confidential data is a long-standing problem that is receiving increasing attention from regulatory agencies and the news media. Data leaks can expose enterprises of all types — not just government agencies — to serious regulatory, public-relations and financial risks. The Palm Beach County leak, for example, probably violates the Health Insurance Portability and Accountability Act, and could result in financial penalties. Gartner estimates that 80 percent to 90 percent of data exposure result from established businesses processes — such as insecure File Transfer Protocol (FTP) exchanges — or employee error.

Enterprises can prevent such leaks, simply and cost-effectively, by implementing outbound content-filtering tools. These tools fall into two categories:

- **Content monitoring and filtering tools:** These tools — from vendors including Reconnex, Tablus, Vericept, Vidius and Vontu — monitor multiple communication channels, such as e-mail, instant messaging and FTP, and inspect the content for policy violations. In some cases, they can block or quarantine violations, and some vendors' products can block outbound e-mail.
- **E-mail filtering tools:** These tools — from vendors including CipherTrust, IronPort Systems, MessageGate, Proofpoint, SurfControl and Tumbleweed Communications — only monitor e-mail, but they always include blocking capabilities and often offer more granular quarantining or encryption than multiple-channel solutions. Many of the vendors in this market partner with encryption vendors such as PGP, Sigaba and ZixCorp to deliver automatic encryption of sensitive e-mail.

Recommendations: Enterprises that deal with sensitive data — particularly financial and health information — should implement an appropriate content monitoring and filtering solution.

Analytical Source: Rich Mogull, Gartner Research

Recommended Reading and Related Research

- "Maintain Regulatory Compliance Without Neglecting Core Security Requirements" — Security professionals need a strategy for responding to increasing regulatory hype. **By Rich Mogull**
- "The 2005 Planning Guidance for Compliance" — IT departments should prepare to assume a more prominent role in compliance management. **By French Caldwell and others**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509