Organizations Must Employ Effective Data Security Strategies

Rich Mogull

Organizations can best protect data through a hierarchical data security approach that accounts for host, application and network security. New technology advances, including encryption, database activity monitoring, and content monitoring and filtering, offer significant security value.
WHAT YOU NEED TO KNOW

Organizations can best protect data and limit information loss from internal and external threats through a hierarchical content security approach that accounts for host, application and network security. Organizations should look at new technology advances including encryption, database activity monitoring, and content monitoring and filtering in developing their data security strategy.

STRATEGIC PLANNING ASSUMPTION(S)

By 2007, 40 percent of new enterprise security spending will be directed toward data security issues, not perimeter security (0.7 probability).

ANALYSIS

Practically every week, a new headline announces the latest unapproved exposure of enterprise data. Be it credit card numbers, health records, or intellectual property, we are seeing an increasing emphasis on securing (or failing to secure) enterprise data, not just enterprise networks. Enterprises are storing an ever-increasing wealth of information on their IT systems while attackers realize there’s a lot more money to be made stealing credit card numbers or product plans than defacing a few Web sites. Network security advances are dramatically reducing the damage from traditional Internet-based attacks, particularly worms, viruses and script kiddies, and new advances in data security are evolving to protect enterprise data, particularly from internal incidents.

Most organizations recognize the risks of external attacks, insider threats and the value of data, with insider involvement in the majority of large, loss-bearing incidents. As interest increased, so did market opportunities, and there are a wealth of products on the market directly addressing (or claiming to address) data security issues. Still, many organizations struggle with taking a comprehensive approach to data security, understanding how to use and position products under various circumstances, and the role of data security in an overall security program. Products are typically not as mature as their network security equivalents, and security managers must again navigate a landscape of smaller point products.

The Role of Data Security

Data security is about protecting data from unauthorized access and unauthorized use after legitimate access. Data security is primarily focused on keeping bad people from good content and keeping trusted people from misusing good content (maliciously or otherwise).

Data security is a logical view for implementing and understanding security, such as network security or application security. Data security is not a specific market or product space but includes a range of solutions, some of which aren’t even pure-security products. We can break the defensive security stack into four of these logical views (see Figure 1).
Data security can't stand on its own; it relies on good network, application, and host security.

The remainder of this note will focus on highlighting data security technologies and controls (see Figure 2).

**Access controls** restrict basic access to an object and are implemented in the file system or database system. Basic access controls restrict read and write privileges based on a user's identity (including group identity) and successful authentication. Third-party products, applications, and some storage and operating systems can provide more granular or role-based access controls. Access controls protect an object in its home repository and do not follow the object when it moves to another repository. Many organizations struggle to effectively manage the proliferation of unstructured data and properly establish and manage identities and roles, weakening their access controls. Still, access controls are the most fundamental security control for unstructured data and are built into every major operating, file and database management system.

**Encryption** restricts the ability to read an object; it provides additional security by requiring a key to decrypt the data. Encryption applied to an object stays with the object in motion, unlike access controls, but can be removed by anyone with the key. In a business environment, in which encryption is tied to established access controls, it may not provide significant additional security, so it's important to use encryption under the correct circumstances. Once an object is decrypted, all controls are gone. Gartner recognizes three methods of encryption: hardware, software and network appliances. See “When and How to Use Enterprise Data Encryption” for details and
selection criteria for enterprise file and storage encryption. Encryption is most effective under two circumstances, and it may not enhance security when applied for other reasons:

- Data is mobile so that backup tapes, laptops, e-mail or even a hard drive are subject to theft.
- To enforce segregation of duties when access controls can’t apply. This is particularly useful to protect sensitive information from an administrator that needs full access to a system, such as credit card numbers in a database or sensitive files in shared storage.

See "Use the Three Laws of Encryption to Properly Protect Data" for more guidance on when to use encryption.

Additionally, all relational database management systems (RDBMSs) support encryption of specific fields (by column) within database tables, and third-party products with more-advanced features are available. Field encryption is only recommended to enforce separation of duties to protect data from database administrators. It may be difficult or even impossible to implement in an established database, but it can be effective in databases designed in advance for encryption. Alternatively, organizations can encrypt the database files or media. See "When and How to Use Database Encryption" for detailed information on database encryption issues and options.

**Enterprise digital rights management (DRM)** uses encryption to provide granular controls tied to the individual object. Unlike basic encryption, enterprise DRM follows the object throughout its life cycle, but requires deep integration with the business infrastructure and applications, and may not work between different organizations. Example controls include read, edit, forward, copy, paste, delete or expire the file after a set time. Enterprise DRM is complex and is only just becoming effective.

**Logical controls** further enhance content security and support access controls, especially in structured data systems and applications. Security can be significantly enhanced through proper database and application design and effective use of structured data management systems features. For example, referential integrity supports the integrity of the data and enhances access controls. All major RDBMS products allow administrators to assign restrictive access to tables while granting wider access to table views, an essential security mechanism. RDBMS products include additional vendor-specific security features, such as data labeling for multilevel security, triggers and row-level access controls, but applying these to established databases may impact performance. Logical controls typically need to be programmed into applications, but third-party tools are emerging to apply controls to legacy applications and centralize management. Some database and application firewalls, traditionally used for intrusion prevention, can externally apply more robust logical controls for legacy systems or off-the-shelf applications.

**Activity detection and monitoring** can detect unusual or unapproved activity in applications, on servers or workstations, in storage or in database management systems; often generating immediate alerts. Activity is usually monitored using a network sniffer, an agent or through near-real-time log analysis of the host's audit logs, often together with a network device to limit impact to the host. Off-the-shelf solutions exist for databases, host systems and certain applications, while some security information and event management tools can aggregate and correlate logs to track file access. Native database auditing is included in all RDBMSs, but it can dramatically impede performance depending on the depth and breadth of auditing applied. Third-party tools resolve some of these performance issues while including advanced alerting features based on user behavior, for example, sending an alert to a security administrator if a database administrator runs a query on credit card numbers. Activity monitoring for data security serves two roles:

- Detecting unusual patterns and activity
Creating forensic records for later investigations

Content monitoring and filtering. Recent advances in detecting and preventing information loss are dramatically improving the enforcement of corporate policies. The market is divided into two categories: content monitoring and filtering pure-play solutions, which monitor and filter multiple channels, and single-channel solutions, which monitor only e-mail, instant messaging (IM), or another channel in which content functions may be secondary to its primary application (for example, a proxy filter). Purchasing decisions still tend to be made based on the buying center: Messaging teams purchase e-mail security solutions, security teams buy content monitoring and filtering solutions, and network teams purchase uniform resource locator (URL) filtering solutions (which don’t even scan content). Gartner expects significant market turmoil during the next two to three years as these products expand features and bleed into competitors’ markets.

Pure-play content monitoring and filtering tools represent the most comprehensive solution for detecting information loss. Such tools monitor network traffic for specific inbound or outbound content based on rules or signatures using deep-packet inspection. At a minimum, they monitor e-mail, Web activity and instant messaging, but may monitor other channels or even internal activity. Gartner is already seeing single-channel filters — dedicated to just e-mail or IM — expand into this space through partnership and acquisition. Passive monitors sniff the network and generate alerts and logs of activity. Proxy filters sit in-line and block or quarantine activity.

E-mail content filters examine e-mail traffic using linguistic analysis. Many of these tools are complete secure e-mail boundary solutions, but some don’t include the antivirus or anti-spam technologies required for that category. Due to the store-and-forward nature of e-mail, complex handling policies can be applied, such as quarantine of suspicious content or automatic encryption.

IM security products "proxy" IM traffic for known protocols and may include content filtering based on keywords or regular expressions.

Bringing it Together

The data security markets today are dominated by smaller point solutions, and enterprises should not expect significant out-of-the-box integration for the next few years. These point solutions can still offer enterprises significant benefit, and Gartner recommends organizations begin deployment, rather than waiting for point markets to settle.

Enterprises can start by identifying critical data to protect (customer financial and health information is a great place to start) and gaining a better understanding of who has access to the data through identity management. Encryption is excellent for protecting data subject to physical loss (for example, backup tapes and laptops), while content monitoring and filtering immediately identifies potential information leaks, even when they can’t be blocked. Database activity monitors are a low-impact way to protect information in databases and adopt segregation of duties for administrators.

Other technologies, such as database encryption, host activity monitoring or enterprise DRM, are extremely valuable but may take more planning and resources to implement. These are long-term security solutions that should still be part of any data security strategy.

Key Issues

What are the most-effective technologies and best practices to protect networks, systems, applications and data?
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
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509