Voltage
security

I've Got DLP. Now What?

Powering More Effective Data Loss Prevention
with Voltage Security

Table of Contents

Overview

2007 is likely to be remembered as the year when terms such as "data breach" and "information security" became permanently fixed in the public mind. It was a year that featured a stunning succession of breakdowns in IT security, brazen hacking incidents and gross mistakes that led to major losses of personal information. Just a few highlights[1]:

▸ TJ Maxx suffered the biggest corporate data breach to date, loosing more than 100 million individual records to hackers.

▸ U.S. Department of Veteran Affairs potentially exposed the identities of nearly a million VA patients and physicians involving several incidents.

▸ Fidelity National Information Services suffered an insider data theft incident where 8.5 million customer records containing credit card, bank account and other personal information was stolen.

▸ Dozens of other incidents—lots of stolen or lost laptops, storage devices and tapes—plagued a who's who of major American institutions from both the private and public sector, including Citigroup, Gap Inc., The Nature Conservancy, the University of Arizona, Duke University, KB Homes, Johns Hopkins Hospital, the U.S. Dept. of Agriculture, Caterpillar Inc. and many others.

In response to this wave of information leaks and outright thefts, many organizations are sharply increasing their investment in security technologies. One class of information security offering in particular, data loss prevention (DLP), has already been embraced by many organizations, or is receiving close scrutiny by a growing number of IT security decision-makers. What many early adopters are finding, however, is that while DLP solutions can do a great job of identifying security weaknesses and even preventing data leaks, few if any are capable of providing a comprehensive information security solution on their own. Moreover, DLP systems that are capable only of blocking or quarantining information can often be counterproductive by interrupting important business processes. DLP drives successful efforts only when implemented alongside other technologies that allow organizations to address their security weaknesses in a timely and cost effective manner.

Data Loss Prevention – Constant Vigilance

Data loss prevention systems can provide a highly effective solution to a range of information security vulnerabilities, from preventing malicious theft and inappropriate data downloads to deterring common mistakes such as emailing or copying files containing sensitive information. There are multiple variants on the basic DLP model, but virtually all systems on the market combine the same basic attributes of a) identifying sensitive content and b) restricting that content, either

---

[1] All statistics: Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm

from being accessed by unauthorized individuals or from leaving the organization via copying, email, FTP, etc.Technological approaches vary, though virtually all

systems use a type of crawling technology to sift through content stored within the IT infrastructure, and identify and pinpoint the location of sensitive content. Some vendors rely on data fingerprinting whereby at-risk content is "registered" with the DLP system, which then uses this memorized template to compare with data as it is screened in the future. Others employ "described-content" technologies that rely on a series of "if/then" scenarios to uncover at-risk content. For example, any 16-digit number would automatically get flagged as a possible credit card account number. The DLP engine could then employ further queries to determine whether the number meets check-sum criteria of genuine account numbers. When validated through these kinds of screening techniques, sensitive data such as PCI-regulated content, protected health information (PHI), or intellectual property can then be handled according to set policy. But here is where DLP systems in their basic form often fall short: they don't provide the full range of data handling capabilities needed to maintain policy compliance while also fully enabling critical business processes.

Block or Quarantine – Antithetical To Business Processes

The beauty and value of DLP systems is that they can, in relatively short order, answer most of the critical questions pertaining to effective data security. What files and data are sensitive and require protection? Where does this sensitive information reside, and which systems require further monitoring? More advanced DLP systems enable organizations to make the next logical jump to determine which individuals have access to this content (in other words, who are the people with the potential to expose sensitive data) and then gain an understanding of the business functions that rely on free access to this information. Finally, DLP systems can monitor data traffic and block sensitive information from being accessed or copied by unauthorized personnel, or sent outside the network via email or FTP, for instance. These are all highly useful capabilities. The vulnerability here, however, is that conventional DLP is very much a container-centric or black/white approach. Many DLP systems automatically quarantine sensitive information and block access to it for all but a small number of authorized users. Similarly, DLP systems can identify sensitive data stored on laptops, USB drives or similar endpoints and then block this data from being accessed, copied or sent beyond that device or beyond the network edge according to prescribed "handling rules." This kind of thinking, that information is safe inside the container and unsafe outside, seems logical but it doesn't take into account the ways organizations today share information with users inside and outside the firewall. Take just a few examples of business processes today that depend on sharing sensitive or even regulated content via the Internet or other form of digital transmission.

- Companies involved in product design and manufacturing transmit highly proprietary intellectual property to their supplier partners and manufacturing partners overseas. It is crucial that these partners have access to product designs in order to purchase raw materials and tool up for manufacturing.

- Mortgage lenders and escrow officers often rely on email and FTP to transmit real estate transaction documents between homebuyers, sellers and real estate agents. In a difficult real estate market where interest rates can shift dramatically day-to-day, slowing the process with paper documents and couriers can have a seriously negative impact on the success of the transaction.

- Many doctors and healthcare providers have adopted digital x-ray and CAT scans. The ability to instantly share this kind of medical information across facilities and among specialists in various locales is increasingly crucial to rendering timely diagnoses, boosting productivity and keeping medical costs as low as possible.

In each of these scenarios a conventional DLP system that blocks access or quarantines sensitive information as it is created or discovered would create a barrier, interrupting the flow of data or blocking it altogether because the content in question is sensitive or subject to regulation. Obviously, blocking any of these processes from going forward is more favorable than allowing a data breach to occur. But if the numerous data breaches that have occurred in recent years tell us anything, it is that people will find workarounds when barriers prevent them from doing their jobs. When the ultimate goal is to keep data contained, and this is generally the case with DLP in its pure state, it becomes impossible or at least very difficult to realize the benefits that stem from the free flow of information. Indeed, when your priority is controlling the container, you're not thinking about the eventualities that could adversely affect your business.

The Answer: Policies Backed With Encryption & Enforced By DLP

Early adopters of DLP systems are confronting these same or similar issues. Crucial business processes get blocked or interrupted. Data and files that were once easily accessible to certain individuals or departments become inaccessible or difficult to access, forcing stakeholders to endure delays or find workarounds. Furthermore, non-compliant practices that may be unwise yet not outright illicit become grounds for intense scrutiny. For instance, workers taking laptops home over the weekend to catch up on projects get singled out as dire policy risks. The answer to these problems isn't more restrictions, it is to supplement existing DLP solutions with more options and greater flexibility in how at-risk data can be handled. Most importantly, organizations need to have the option of freely sharing information outside the network with the confidence that that information will remain secure even if it is lost or stolen. The only way to reach this goal is by incorporating strong data-centric encryption into the mix—that is, encryption that protects the data itself, not just the container.

When integrated with a DLP solution and the overall IT security infrastructure, encryption provides the organization with the capability to both secure information as needed to maintain policy compliance and also share that information with partners outside the enterprise. For instance, DLP systems with multi-protocol data scanning would enable the organization to enforce security policies around email, HTTP and FTP channels simultaneously. With email or FTP, the DLP system scans the content before it leaves the network, and if sensitive content were discovered, that file or email message (and any attachments) would be automatically encrypted. As a result, compliance policies are accurately and consistently applied and end users do not need to take any special actions to ensure that sensitive information is properly encrypted.

Consider also a case where executives in different offices need to provide input on a highly sensitive merger and acquisition contract on a collaboration system such as Lotus Quickr or Microsoft Sharepoint. Even behind the firewall, this kind of document would need to be sealed to prevent critical strategic information from leaking to competitors or the press. With encryption and DLP-enforced policies, the M&A contract file could be encrypted on the server itself and when in transit, and only decrypted for reading and editing when on the desktop of, for example, the CEO or CFO involved in the negotiations. In fact, with accurate screening and flexible encryption options, virtually any policy challenge or data leak scenario can be addressed, from enterprise database batch files and spreadsheets to more arcane threats posed by image, sound or video files. These kinds of capabilities are likely to take on growing importance as more and more organizations embrace collaborative systems and Web 2.0-type applications that greatly simplify the exchange and group sharing of the full range of digital media.

Screening + Encryption = Effective Security & Compliance

The combination of screening provided by the DLP solution plus encryption is key. Together, screening and encryption make for a combined approach that is more effective than either one alone. We've explored the shortcomings of DLP above, but encryption alone has certain limitations as well. Most encryption solutions are designed to be ad hoc – the creator of the file makes a decision, at the point of creation or point of sharing, to encrypt or not encrypt. Failing to make the right judgment call can be perilous, as can be seen with data breach incidents involving discarded IT systems or lost laptops. It is often the case that owners of these systems don't even realize that the sensitive information was present. With automated screening and encryption, even the most obscure files and data at rest on long-forgotten servers can be easily discovered and secured. Moreover, organizations embracing this approach can take advantage of a full range of rules and policies to accommodate virtually any business process or rights-management scenario.

Senior executives and managers charged with regulatory compliance responsibilities are often leery of implementing encryption on a widespread basis because it opens up the possibility of interrupting internal work processes or even abuse. What if, for instance, an IT security manager who managed file encryption for many years leaves the company without providing a record of who has access to which files? Crucial information could be lost. By the same token, what if a company began routinely encrypting all financial data, and granted access rights only to the CFO and the senior financial staff? Such a move would likely disrupt operations across the organization as the finance department fielded constant calls from the marketing, legal and planning functions for access to information they needed to do their jobs.

IA combined DLP and encryption approach obviates these kinds of problems because both functions are easily integrated with collaboration servers or digital rights management systems to ensure the right people always have access to the information they need. When a sensitive file is identified by the DLP system on some obscure server or ancient mainframe, it can immediately be encrypted with rights automatically granted to, for example, the director of compliance, the administrator of the particular system and the CEO. The beauty here is that if a certain individual leaves the company, the file would still be accessible—yet always secure. These capabilities are vitally important in light of resource limitations and compliance priorities as well. Imagine that an initial scan of a several shared servers and enterprise data stores turned up hundreds of potential compliance risks or vulnerabilities. With the DLP system serving as policy engine, it would be easy to encrypt sensitive files in place, or provide for automatic encryption should someone attempt to copy or transmit suspect files or sets of data. Potential impact would be minimized, while security would be ensured until a more thorough review and mitigation program could be enacted.

Conclusion

Many early DLP implementations quickly ran into problems because the simple reality of doing business in the 21st century is that innumerable processes and practices today rely on the free flow of digital information. Sealing off information into a container behind the firewall has a negative impact on productivity, or precludes certain processes altogether. Combining accurate data screening with strong encryption offers the most effective approach to maintaining information security and policy compliance in today's digital business environment.

08N030602