Securing Your Company's Confidential Data

Data loss prevention tools are gaining interest, according to a recent global survey. This paper examines how they work and how best to use them.

EXECUTIVE SUMMARY

Companies face a proliferation of confidential data — for example, employee information, customer transactions, partnership contracts, intellectual property. At the same time, with employees accessing that data from mobile devices and through sophisticated collaboration tools, companies must find ways to protect it, whether it's in storage or being transmitted across networks.

New data loss prevention (DLP) solutions help to identify, manage, and audit such data, and recent surveys show increased interest among executives for this technology. But in addition to understanding where data resides, who should have access to it, and how it should be protected, CSOs must understand how DLP solutions work in conjunction with intelligently crafted enterprise-wide security policies.

In this white paper, we'll look at the advantages of DLP, the obstacles to avoid in its deployment, and what to look for in such a system.

THE NEW WORLD OF DATA LOSS PREVENTION

Data volume is on the rise. Companies are collecting and storing more information than ever—about employees, customers, transactions, partners and assets. And this data is being accessed and shared in new ways such as through mobile devices and collaboration technologies. It's becoming increasingly important for companies to protect their information, whether it's in storage or being transmitted across networks.

New data loss prevention (DLP) solutions help to identify, manage and audit such data, and recent surveys show increased interest among executives for this technology. But in addition to understanding where data resides, who should have access to it and how it should be protected, CSOs must understand how DLP solutions work in conjunction with intelligently crafted enterprise-wide security policies.

In this white paper, we'll discuss the advantages of DLP, what to look for in a DLP system, and the obstacles to avoid when deploying one.

THE NEW WORLD OF DATA LOSS PREVENTION

All data is not created equal. Prudent financial and risk management has always dictated that companies apply stricter security to confidential data. But the parameters of what constitutes confidential data are expanding and as a result companies—business units and IT departments alike—face new challenges when it comes to understanding, locating and protecting that data.

Confidential data—the kind new DLP applications target—is no longer limited to financial records. Whether because of increased governmental or industry regulation, companies now must protect customer transaction data, client records, employee information and other material. As more organizations outsource business processes and even R&D efforts to international firms, they must protect contracts, partnership agreements and intellectual property.

When contracts involve international entities, companies must understand and accommodate regional regulations, such as HIPAA in the U.S. or the EU Data Privacy Directive. They must also protect data where it is stored (data at rest) and when it is transmitted (data in transit). Because many organizations now allow employees to access data through mobile devices, the latter is especially crucial.

Finally, executives are finding that auditing their security processes has become increasingly important. Besides securing data, they must be able to *prove* that they have secured data. But recent surveys show that although corporations understand this imperative, they face challenges in three fundamental areas:

- Locating their most crucial data
- Understanding who accesses the data, why, and how frequently
- Ensuring their most crucial data is secure

Meeting these challenges requires developing policies to protect data and ensure appropriate access. The policies must also be flexible and intelligent enough to identify and remediate problems to accurately accommodate new data as systems are updated.

AN INCREASING COMMITMENT TO DLP

CSOs are well aware of the challenges their companies face. In 2009, PricewaterhouseCoopers, in conjunction with *CIO* and *CSO* magazines, surveyed more than 7,000 C-suite executives regarding their use of DLP; the results show a deep understanding of the value it brings to their organization. Almost half of respondents (44 percent) said they had deployed a DLP solution, compared to only 27 percent who said they had in a similar survey conducted in 2008. At the same time, 73 percent said it was "important" to consider investing further in DLP tools.

DLP solutions have a straightforward purpose: they help companies identify confidential data— Social Security numbers, financial information, business-critical information—and set up parameters to protect it. But it's not necessarily a simple process. For example, certain data may only be accessed by certain users, or can only be transmitted when it's encrypted, or cannot be transferred to portable storage devices.

"DLP provides the answer to a key IT question," says Mark Lobel, a principal in PricewaterhouseCoopers' Advisory Services group. "Where are specific pieces of data in my environment and are they protected? It's the first real opportunity that information security professionals have had to implement a data classification policy."

Deploying DLP solutions provides a higher level of automation and reliability, Lobel says. "Prior to DLP, this kind of classification and protection was all done by people and processes. You trained them and hoped they did it properly. But there was no way to audit it. With DLP solutions, you can conclusively know the answers."

Not surprisingly, according to the survey, the industries most likely to adopt DLP solutions over the next year are highly concerned about security, copyright protection, intellectual property, customer data, or some combination thereof. They include:

- Capital markets
- Entertainment
- Life sciences/biotechnology
- Insurance

Companies of all sizes have already discovered the benefits of DLP: while more than half of businesses with $10 billion or

How Symantec Data Loss Prevention Protects Your Confidential Data

Symantec's DLP solution tackles the key issues of monitoring, protection and prevention, both on the network and at any endpoint locations. It delivers a unified method of discovering, monitoring and protecting confidential data wherever it is stored or used.

You can gain visibility into where confidential data is stored throughout the enterprise (by user, department or policy); identify broken business processes transmitting confidential data (such as an FTP server sending non-encrypted customer information to a partner); proactively and automatically protect stored confidential data; and provide automated immediate end-user notification when data security policies are violated.

Here's a look at each of its seven modules:

Network Discover finds confidential data wherever it is stored, whether in file servers, databases, document and records management, e-mail, or Web applications.

Endpoint Discover scans for confidential data stored on user devices or in remote locations, including laptops, desktops and workstations.

Network Monitor inspects network communications such as e-mail, IM, Web, FTP, P2P, and generic TCP, for confidential data in violation of data security policies.

Network Protect guards stored confidential data by removing it from its stored location.

Network Prevent stops network communications from being sent in violation of data security policies by either removing them or routing them to an encryption gateway.

Endpoint Prevent monitors confidential data downloaded to local drives; copied to USB or other removable media devices; burned to CDs/DVDs; transferred over network communications; or printed or faxed electronically.

Enforce Platform manages all universal DLP policies in a centralized platform for detection, incident remediation workflow and automation, reporting, system management, and security.

more in annual revenue use DLP solutions, so do 39 percent of companies with up to $25 million in annual revenue. Further, companies who have deployed DLP solutions report these applications significantly reduced the financial impact of data breaches. They averaged just $975,000 in losses as the result of a data breach or security loss, while companies without DLP averaged $1.7 million in losses per event, some 77 percent more.

Even so, Lobel recommends CSOs not look at DLP as an automated panacea. As with all enterprise software, it needs to be implemented properly. "Like any other monitoring technology, DLP solutions can overwhelm you with information that may not be of value," he says. They can also reveal a massive to-do list. "I've seen financial services firms scan their networks and find so many problems, they had to play catch-up for a long time to bring data in line with their data classification policy."

Lobel also notes that DLP solutions must be tuned properly, because they have the potential to collect too much sensitive information. He cites the case of one IT person who got fired because he classified certain information improperly and ended up collecting sensitive personal data that should have been handled only by the legal department. "If a company has union employees, there are clear lines about what you can and can't do in regards to collecting information and monitoring those employees," Lobel adds.

THE MANAGEMENT CONUNDRUM

While executives expressed confidence in the importance of DLP solutions, they were less sure about their ability to locate confidential data. Six out of 10 respondents admit that their company doesn't yet have an accurate inventory of where just one kind of confidential data—personal information about employees and customers—is collected, transmitted or stored. This leads to risk management challenges.

At a minimum, companies must be able to tackle confidential data from six key perspectives:

- Identify
- Locate
- Protect
- Archive/Delete
- Access/Storage
- Audit

Let's look at each of these individually, along with how DLP systems accommodate them.

Identification. There is no blanket rule about which information needs strong protection. A design firm may consider its computer-aided design drawings intellectual property because they represent the output of key employees and thus a competitive advantage, while a contract manufacturer may consider the terms of its contracts a trade secret. Ultimately, any type of information that is critical to either business success or risk management should be part of a DLP program.

Location and Use. Once confidential data is defined, it must be located. This is about more than just servers—companies should be aware of all potential locations. Is confidential data stored on employee laptops or desktops? Is it being sent over e-mail or on instant messages?

Protection. The heart of what DLP solutions do is ensure that confidential data doesn't break through the boundaries companies have set for it. Information solely used by the human resources department, for example, must be protected from inappropriate access by other departments. Confidential data cannot appear in e-mail or attachments going to external addresses, unless it's clearly delineated that the destination is approved by IT policies.

Archiving and Deletion. Just as with identification, there is no blanket rule for how long companies must keep data. Professional services firms frequently subscribe to governmental regulations, while other businesses follow industry guidelines. A DLP solution must be cognizant of these rules, regulations and guidelines, and alert IT for disposition on an automated basis. Once data is archived, companies must follow the same protection mechanisms to ensure it isn't transferred or transmitted inappropriately.

Access and Storage. CSOs must know not only who uses data, but also who is responsible for it. Understanding how data should be stored and secured is crucial—protecting confidential data while providing access to those who need it and maintain it is a real tightrope walk.

Auditing. Auditing enables companies to conform to regulatory agency requirements. It can also help identify who within a company is not following proper protocol, giving companies a way to identify transgressors and understand where training and education need to be improved.

DEVELOPING A UNIFIED SECURITY POLICY

Deploying a DLP solution won't automatically accommodate all of these facets. You must also develop a security policy that takes into account the needs of your company (from both a financial and regulatory standpoint), your employees (from a productivity standpoint), and your IT department (from a management standpoint).

Developing such a policy requires an understanding of business needs—security must support, not hinder, business goals—and a high level of collaboration between IT and business units. IT needs an enterprise-wide view to create appropriate policies around who needs access to which data, and why.

Because of the proliferation of mobile computing, organizations must take an information-centric perspective—one that accommodates data whether it's stored or transmitted. For instance, data that needs to be encrypted must maintain that state when it's sent across the network, not just when it's at rest.

Finally, from a management standpoint, a DLP solution requires a centralized view that can accommodate computing devices, networks and storage systems, no matter which vendor produced them. Only through such a centralized view can you define policies, implement them properly, and provide consistent monitoring and reporting.

By combining an enterprise-wide view with strong, consistent policies, CSOs can accommodate both the increasing amount of confidential data and its expanding boundaries. Because DLP solutions enable an automated, process-oriented way of identifying and managing confidential data, they are a crucial component of simplifying this important effort.

FURTHER RESOURCES

Symantec Data Loss Prevention Product Family

http://www.symantec.com/business/products/family.jsp?familyid=data-loss-prevention

Data Loss Prevention: Anatomy of a Breach

http://eval.symantec.com/flashdemos/other/anatomy_of_a_breach/