The Executive Guide to **Data Loss Prevention**

From CSO Magazine and CSOonline.com

CONTENTS

Over the last few years, you've heard a lot from information executives, consultants and vendors about data loss prevention, an emerging discipline that aims to keep business-critical, private information from falling into the wrong hands. If it's all left you scratching your head, there's a reason. Businesses are looking for a way to prevent the loss of data, conceptually, while vendors are offering the acronym-friendly Data Loss Prevention (DLP). The disconnect between the two things has led to a fair amount of confusion.

There are subtle but critical differences between the prevention of data loss, a business imperative, and DLP, the product set. DLP tools, implemented correctly with the right processes in place, can indeed help prevent the loss of data. Buying and installing DLP, however, isn't as simple as some marketers would like you to believe, nor is it ever a goof-proof process. This executive guide, based on research done by *CSO* Magazine and CSOonline.com, is intended to help you make sense of DLP, the tools, while figuring out the best way to actually help your organization from losing data. Now doesn't that sound like something worth your time?

What Is Data Loss Prevention, Really?

LOOSELY PUT, DLP is a set of products and processes that help businesses protect information. It's not a stand-alone product like a firewall or an e-mail server, though. Instead, it's a group of technologies that pull together several important aspects of information security. A DLP system might prevent data loss by identifying content, tracking activity and blocking sensitive data from being moved. And here's the good news: While DLP the acronym has been around only a few years, many of the underlying technologies and processes that comprise it are battle tested. Roughly, DLP consists of the following:

1. A Way to Classify Data

Data classification dates back to the first time someone scrawled "top secret" at the top of a document, and it's the requisite for all your loss-prevention efforts. If your organization hasn't identified what information to guard most closely, then how can any technology prevent that information from falling into the wrong hands? The key is to develop a system that has a chance of working. Nick Selby, CEO/cofounder of Cambridge Infosec Associates, says that lumping data into too few or too many buckets is a recipe for failure. "The magic number tends to be three or four buckets—public, internal use only, classified, and so on," he says.

2. A Way to Encrypt Data

No matter what any vendor tells you, encryption does not equal DLP, but it is a critical component—as it is in any instance where you're trying to protect data at rest, in use and in motion. Again, understanding how your business works and setting appropriate policies is crucial. "It could be as simple as enforcing a policy," says Richard Stiennon, chief research analyst at IT-Harvest, offering an example of such a policy for an e-mail system: "When you see spreadsheets as attachments, encrypt them."

3. A Way to Detect and Block Data from Leaving Secure Areas

This is the technical version of a guard watching what's leaving the network and why. Sean Steele, senior security consultant at InfoLock Technologies, says the key is to have systems in place that provide real-time (or close to real-time) monitoring and blocking capabilities of the three ways data might leave secure areas: outbound at the network perimeter; at rest, on servers or storage devices; and while being used by human beings at the network's endpoints and servers.

4. E-mail Integration

E-mail is an easy target for data thieves, whether they're sending e-mails with links to computer-hijacking malware or sending e-mails from the inside with proprietary company data. Partnerships between security vendors and e-mail gateway providers are an essential piece of the DLP puzzle. Fortunately, Stiennon says, "Most DLP vendors formed partnerships with e-mail gateways early on."

5. Device Management

Finally, there's the gadget problem. Given the mobility of workers and their computing devices—from laptops to smartphones to USB sticks—security tools that help the IT shop control what can and can't be done with mobile devices are a key ingredient of DLP.

Looked at in another manner, the tools can be classified in three groups. Network-based tools sit at the edge of the network, monitor data flowing through the network and in some cases filter or block data movement. Host-based tools require an agent to be installed on individual PCs and servers, monitor static data on these systems and, in some cases, block or control actions that users can take. Finally, there are a growing number of systems that combine both of these capabilities.

The People Problem

NOT A BAD checklist, right? But information management is never as easy as just buying some security technologies and installing them. User awareness is a key to keeping sensitive data safe from online predators. "DLP is a process first. The technology is simply an enabler for the automation of the process," says Rick Lawhorn, a Richmond, Va.-based chief security officer. "The process needs to include education and awareness training and cover human resources, records management and compliance. The objective is to continuously train data owners and data custodians (the employees) on the company policies to reduce instances of non-compliance."

Here are several things you're trying to prevent employees from doing, either accidentally or on purpose:

Sending sensitive e-mails outside the organization. IT administrators have had success detecting and blocking mali-

cious e-mail, but users continue to let sensitive data outside the company walls by hitting "send" at inappropriate moments—like when they've just copied and pasted customer information or intellectual property details into a message box. Many times the e-mail is meant for recipients inside the company, but the user might include outside addresses in the message without thinking. Policies should be clear on the type of content that users can and cannot send out, with the "no" list including such things as customer credit-card numbers, details on the company's intellectual property and the medical records of fellow employees.

Falling for phishing attacks. E-mail filters can't stop every phishing attempt. URLs to malicious sites will still get through, and all it takes is one user to click on such a link to infect one or more machines with malware that finds and steals data. Attackers typically latch onto news events such as hurricanes or celebrity deaths to concoct bogus headlines that, once clicked, open the door to insidious websites designed to drop malware onto the user's machine. An awareness program can reduce the risk by constantly alerting employees to social engineering schemes that are making the rounds.

Sending sensitive information by instant messenger. Instant messaging (IM) programs like AOL Instant Messenger and Trillian have become routine applications in a today's mobile workforce. Along the way, attackers have found ways to send malicious links and attachments to users by creating imposter accounts that look like legitimate messages from colleagues. What's more, many IM clients can be downloaded for free and, once installed, may be beyond the control of enterprise IT shops. Again, user awareness training and policies are critical.

Sharing sensitive information on social networking sites. Attackers are increasingly setting their sights on such social networking sites as LinkedIn, Facebook and Twitter. The bad guys can use these sites to do all the nasty things they learned to do by e-mail and IM. On Facebook in particular, user's inboxes are stuffed with everything from virtual gifts to games to cause requests. The bad guys will send links that appear to be from legitimate friends, or trick legitimate friends into sending the bad links. If recipients open the link, they're inviting a piece of malware to infect their computer. User awareness programs must address the tricks attackers can employ on these sites.

Using insecure passwords. Because memories are short and log-ons are plentiful, employees may tend to use the same password for many accounts. A good user policy requires employees to use a different password for each work-related account with upper and lowercase letters and numbers, for example. Some programs also can be set to prevent users from reusing passwords during a certain time frame.

Snooping around in places they didn't need access anyway. Employees are often given access to more enterprise applications than they need to do their jobs. All it takes is one disgruntled employee with too much access to go in and steal enough sensitive data to put the company in serious jeopardy. The best defense here, security experts say, is to allow employees access only to applications and databases they need to do their jobs.

The Vendor Landscape

Given all the focus on data loss over the last half decade—and the regulatory actions that have followed—it's no surprise that the vendor landscape for DLP products is complex and undergoing rapid change. Any time established software and hardware companies don't have a technology that businesses are asking for, a common tactic is for them to begin buying up vendors who have what they need and bake it into their product lines. That's what has happened with DLP. Only a few years ago, multiple independent companies were selling various components of DLP. Now, a few large companies have made aggressive purchases to try to make themselves players in the DLP marketplace.

Of the companies Gartner considered DLP visionaries three years ago, only Code Green Networks remains an independent, privately held company (at least at the time of this writing). McAfee bought Reconnex, and RSA snatched up Tablus, which is now part of the RSA Data Loss Prevention Suite (from EMC, of course). Symantec acquired Vontu, one early leader, while Trustwave acquired Vericept, another. Websense—itself an early leader—did some acquiring of its own, with the acquisition of PortAuthority Technologies. Meanwhile, CA bought Orchestria and folded its DLP capabilities into its Security Management solutions.

A few niche players, including Proofpoint, Palisade Systems, and Fidelis Security Systems, are still independent and privately funded—but if history is any guide, they may not be for long.

As far as what they're selling, think broad, not narrow. Wayne Proctor, CISO at First Data USA, said the major trend he has observed in the DLP marketplace is for vendors to extend from monitoring content only in outgoing traffic to monitoring other sources of data (primarily data at rest and data on endpoints). "I don't view this as twisting the meaning of DLP, but just leveraging their content evaluation engines to offer additional services," he says. He added that some of the DLP vendors offer services that are not related to data leakage, such as tools that identify potential disgruntled employees and persons who are downloading software that is not approved for usage on a company network.

What DLP is, however, may matter less than the capabilities of whatever you're considering buying. "The term DLP has essentially become meaningless because of a variety of vendors who wanted to say they were offering it," says Rich Mogull, the respected founder of the security consultancy Securosis, who describes the acronym DLP as a buzzword created for marketing purposes. "Encryption and endpoint control vendors call what they do DLP. A firewall does some of what the concept entails. All of these tools are helpful in different areas of security, but they are not DLP."

So how can an IT security practitioner avoid confusion when exploring DLP options? Mogull offers this advice: "I don't care what someone calls what they are putting in front of me. Words can mean almost anything. I force the vendor to tell me in specific terms how their product does what it does. You say it prevents data loss? Great. Tell me exactly how. Oh, you encrypt. Oh, you monitor incoming content. Great." It's your responsibility to ask

probing questions.

According to Gartner (where Mogull previously worked), these are some of the main criteria that will help you evaluate your options:

Channels. How many protocols does the product cover, and is it capable of decoding the protocol? The market has rapidly moved toward multiple-protocol decoders, Gartner says.

Blocking. Not all products perform blocking, and some block only on certain channels, though Gartner sees the market moving toward products that will block all channels.

E-mail. Most products block e-mail first and enable quarantining, rerouting, blocking, encryption and other more complex handling rules, Gartner says. Few products today monitor internal e-mail, but some provide Microsoft Exchange or Lotus Notes integration. Users should be cautious of products that monitor e-mail passively or block SMTP traffic by resetting TCP connections, which provides no feedback to the sender and can cause performance issues.

Detection techniques. Options include rule-based detection, document fingerprinting, database matching and statistical analysis. "If you're looking for things like Social Security numbers, that's not a hard thing to do, but when you start asking for other kinds of data, it gets harder," says Jon Oltsik, senior analyst at Enterprise Strategy Group. "Some products have more kinds of classifications than others—financial data, credit card data or whether people have hacking scripts on their desktop."

Implementation Tips from the Trenches

SEVERAL IT SECURITY practitioners said they achieved a reasonable DLP program once they stopped listening to vendors trying to sell so-called "DLP out of the box" products and focused instead on mixing security technologies with training programs to help users defend themselves—and, in turn, the companies they work for.

For Chuck McGann, manager of corporate information security services for the U.S. Postal Service, the key technologies were keyword pattern matching, auto quarantine for files that violate policy, the ability to specify and use certain combinations of data for matching, detection of specific data at rest and in transit, and robust reporting capability. That might sound like a tall order, but he was also able to determine that he didn't need to invest in additional encryption, or in access-control-list and data-in-transit-masking technology. It's just good business to make sure any product has built-in capabilities to detect what is most important to you.

For Michael Gabriel, CISO of Career Education Corp., another key component was being realistic about how much he would really be able to accomplish with user awareness. "Explaining everyone's role to them is much less of an issue if you can let technology minimize their role," he says. As part of its DLP program, his organization ended up installing an e-mail encryption system that detects confidential information using exact data matching and automatically encrypts information if it's being sent to an authorized recipient, so that the user doesn't have to remember to take that step.

The Enterprise Strategy Group's Jon Oltsik emphasizes the importance of testing DLP tools in your own environment before deciding which ones will work best for you. "Everyone talks about how their detection is better than others, but there's no way to tell which one works better without running a few products side by side it in your environment, on your data, with a couple of your rules." See which ones come up with the most alerts and which have the most false positives and negatives. "If you don't, you're really taking a risk, no matter how good the canned presentation is," he says.

Beware, too, of rushing in and preventing certain types of actions right away. Some products can block users from performing certain actions on sensitive data, such as copying, printing or e-mailing. However, users such as Randy Barr, chief security officer at WebEx Communications, would prefer to be notified when users do something that's against security policy rather than stop them outright. A majority of violations may occur initially because employees are unaware of regulatory rules or company policy, and are simply trying to perform essential job tasks. "I don't want to hinder them—I want to audit what they're doing," Barr says. "I wanted a tool that would provide awareness to employees and also log an alert to me."

Part of that user awareness ought to include informing employees that they're being monitored. Not only does this let them know what you're capable of doing, but it also teaches them what they need to do to protect sensitive data. After deploying a tool from Vericept, Sharon Finney, information security administrator at DeKalb Medical Center in DeKalb County, Ga., says the healthcare organization disclosed to employees that it fully monitors every piece of data that crosses the network, internally and externally, even requiring employees to sign a form saying they understand this.

Finally, in case this isn't already clear, be wary of anyone attempting to sell you DLP-in-a-box. Fortunately, there are signs that the vendor community is becoming more measured in its sales pitch of DLP. "There is a growing realization among vendors that they can go farther by addressing what exactly they can help with," says Selby, of Cambridge Infosec Associates. "It is less about 'we-can-do-everything' marketing and more about how 'we can help you with specific pieces of DLP.'"

This may be a natural outcome and a trend that continues as the market evolves. Once upon a time, the DLP landscape was dotted with vendors who wanted to convince you that their one small product did it all. Now, DLP solutions are being offered by larger companies with a whole lot more in their product line—and consequently, a lot more things to sell you that might help you prevent data loss, in the largest possible sense. As long as you do your homework, that's good news. ■