Why DLP is more important than ever before

Although data protection has always been of primary concern of all organizations, a host of factors have made DLP an even more important tool in the data protection arsenal.

For example, the volume of data that organizations must manage has grown dramatically due to both the use of mobile devices as work tools and the proliferation of data accessed from the cloud. Imagine the amount of data just one worker can create or access in one week, between using a desktop PC, a smartphone and a tablet, and tapping into both onsite servers and the cloud.

Additionally, much more of today's data is unstructured, such as e-mail, images, maps, social media messages, PDF files, web pages and GPS data, just to name a few. Unstructured data is notoriously difficult to manage and secure, but DLP tools can handle it. For example, a DLP tool would enable an agency to block an e-mail from being sent if it includes a Social Security number. Such a tool also could prevent someone from downloading a schematic of a military base.

"Unstructured data is to information what liquid mercury is to the traditional thermometer; when it escapes from its centralized container, it is easily dispersed and travels far and fast to every nook and cranny of the extended organization," says Derek Brink, vice president and research fellow for IT security at Aberdeen Group.

"To the extent that the sensitive information used in collaboration is in unstructured formats, it also needs to be protected and managed," Brink explains. "That's where DLP comes in – and it can be an opportunity for IT security to act as a vitally important enabler for supporting the strategic objectives of the organization."

The true cost of a data breach

NOBODY WOULD DENY that data breaches are costly, both in terms of reputation and actual dollars. But if you add it all up, how much does a data breach really cost an organization?

According to the 2011 Cost of Data Breach Study published by Ponemon Institute and sponsored by Symantec, the organizational cost of a data breach is approximately $5.5 million. Here are some additional highlights:

- The cost to detect the breach and determine how it happened: $433,000
- The cost to notify victims of a data breach: $560,000
- The cost of a single compromised record: $194

There are intangible costs as well. According to the National Computer Security Association (NCSA), for example, it takes 21 days and $19,000 to recreate just 20 megabytes of lost accounting data, and 42 days and $98,000 to recreate just 20 megabytes of engineering data.

WHAT IS DLP AND WHY DO YOU NEED IT?

A decade ago, security was about providing defense-in-depth and protecting the perimeter. But today, as technology has improved and organizations have become more aware of what it takes to protect their information, security has become truly data-centric.

That's where data loss protection (DLP) comes in. When used properly, DLP can help organizations keep close tabs on when, where and how data moves in and out of their networks. It works by allowing organizations to set specific rules, at a very granular level, about data access, downloading and copying.

DLP can monitor two basic environments: the endpoint and the network. Products that focus on the endpoint — that is, on notebooks, desktop computers or servers, or in databases — are designed to protect data at rest. Rules are set to protect data from being downloaded onto thumb drives or other types of removable media. Some of these tools also can remove or encrypt sensitive data. The system even can be set up to alert an administrator if a rule is violated.

DLP products that focus on the network are designed to constantly scan network traffic for violations specified by the organization. These tools examine all data that traverses the network and can block access to data based on the permissions and policies set by the organization.

Government and DLP

Although data security has long been an important issue in government, it has taken on much greater importance in recent years. The sense of urgency has been heightened by several high-profile data breaches resulting in the exposure of personal information of tens of millions of military personnel, veterans and private citizens.

"WE'RE TALKING ABOUT SOME OF THE MOST SENSITIVE DATA THAT EXISTS..."

Government manages numerous types of sensitive data, depending on the agency and its mission. Most agencies must protect intellectual property, while many deal with personally identifiable information. Some are focused on protecting the data of large, regulated corporations that must share financial data with the government, while others work with data related to national security.

"We're talking about some of the most sensitive data that exists, and that requires making sure there is a high layer defense in place to protect that data," says Emily Mossberg, national data protection practice leader for Deloitte and Touche. Mossberg says a DLP solution is one of the key components of protecting that sensitive data.

To make matters worse,

government data seems to be a particularly enticing target for hackers. According to research from Symantec, 25 percent of targeted attacks are geared toward government, by far the greatest percentage of any sector.

Technology such as DLP is clearly part of the solution, and government leaders realize that. During 2012, a Senate subcommittee worked hard to pass the Cybersecurity Act of 2012, which aimed to improve the methods and tools that agencies use to ensure that sensitive information is properly protected.

"WE WILL HELP USHER IN A NEW GENERATION OF CYBER TOOLS FOR THE FEDERAL GOVERNMENT..."

"We will help usher in a new generation of cyber tools for the federal government so that government agencies…can be better prepared to face the cyber challenges of the 21st century," says Sen. Tom Carper (D-Del.), co-author of the bill, in a statement at a July hearing on the bill.

THE NEED FOR MOBILE DLP

The fast growth of tablets, smartphones and other mobile devices throughout government has changed the security equation in a big way, especially given the growing adoption of bring-your-own-device policies.

Although allowing workers to use mobile devices provides many benefits, including increased productivity and the ability to work offsite, it also increases risks. Without the appropriate security controls, staff members accessing sensitive data via a mobile device could inadvertently cause a serious security breach when sending an e-mail or connecting to the Internet or a social media account.

All trends indicate that mobile use will continue to rise, and risk will rise with it unless appropriate precautions are taken. One option is implementing DLP tools on mobile devices. These tools, generally offshoots of traditional DLP devices optimized for mobile environments, can standardize and execute granular security policy on devices while still allowing users to access the data they need.

Mobile DLP also can manage a secure content container on each mobile device, lock down sensitive information and control content based on type and context, dictating which actions users have for specific data, such as save, print, e-mail, copy/paste and e-mailing links.

Monitor, analyze, measure and control

A few years ago hackers broke into the servers of a federal agency, stealing tens of thousands of Social Security numbers and other personal information. As a result of that attack, the agency contracted to develop a "heat map" of the entire agency to pinpoint the exact location of sensitive data on both endpoint devices and storage, as well as throughout the network.

The solution, developed by CDW•G with technology from Symantec, uses data loss prevention (DLP) technology to detect data in violation of agency policies, such as patterns indicating that specific Social Security numbers and credit card numbers are at risk of exposure. It also detects the use of encryption, password file formats and evidence of hacking tools and attack planning.

Today, even agencies that have not experienced a cyber attack are looking at DLP tools to help them mitigate both accidental and intentional data disclosure by workers, identify unsecure business processes and improve mobile security. In other cases, agencies want to identify potentially sensitive information being sent by e-mail and notify senders that they might be doing something in violation of policy. Other agencies are working to improve the security of inter-agency data transfers.

"Historically, we have always protected the can but not the soup inside the can," explains Peter McDonald, Symantec's information and identity protection account executive for data loss prevention, encryption and authentication. "But protecting the boundaries is no longer a feasible security strategy. Agencies need to know where sensitive data resides across the environment, including on portable devices."

DLP is an important technology, even if you trust the people in your organization, emphasizes Matt Jach, a senior security engineer for data loss prevention for CDW•G.

"This isn't about trust; it's about managing the risk of the environment," he says. "Even a few anomalies can cause an agency a lot of concern and cost, so they need a proven technology like DLP. Otherwise, they are putting their agency at risk financially, operationally and in terms of credibility and compliance."

WHAT TO CHOOSE?

Although DLP is an important tool in agencies' security arsenals, it can be difficult to determine what tool to implement and how to integrate it with the rest of the infrastructure. CDW•G's method of working with agencies is designed to do just that. By understanding an agency's objectives, tolerance for risk, existing risk management framework, budget and timeframe, CDW•G can recommend the best combination of products and services.

"Once our team of account executives and field security engineers understand what an agency needs, we work together with them to define a solution that typically incorporates services and products," Jach adds.

CDW•G has a vast arsenal of products to offer agencies, due to its partnerships with a wide range of vendors. It also offers several services, from assessment, planning and design to installation, configuration, deployment and product training.

In the case of DLP, CDW's assessment service includes a full review of an agency's existing IT security environment, a detailed risk assessment, definition of product requirements, detailed vendor evaluations and proof of concept.

The detailed risk assessment is one of the most important services an agency should have, Jach says, because it reviews both data at rest and data in motion, such as e-mail, web traffic and FTP sites. This information is critical to finding the best solution for the agency.

"With the right tools and the right implementation, all organizations can improve their security infrastructures," he adds. •