JULY 2012

DATA LOSS PREVENTION

Refreshing data security to meet an evolving threat environment

800.808.4239 | CDWG.com/dlpguide

CDW·G REFERENCE GUIDE

A guide to the latest technology for people who get IT

CDW·G® PEOPLE WHO GET IT™

WHAT'S INSIDE:

800.808.4239 | CDWG.com/dlpguide

What is Data Loss Prevention?

Expert advice from People Who Get IT.

Visit CDWG.com/dlp for more information on data loss prevention.

What is a CDW·G Reference Guide?

At CDW·G, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology.

Our Reference Guides are designed to provide you with an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise. We hope you find this guide to be a useful resource.

Defining DLP

Focusing security on an organization's most valuable asset — data

The one constant in planning out security strategy is that it is always evolving. Changing threat environments, technology innovation and shifting organizational priorities drive IT departments to continuously reevaluate the most effective approaches to protecting assets and ensuring stable operations. IT staffs also need to meet new challenges associated with securing what today are often highly distributed and increasingly virtualized environments that stress a digital operations component.

IT security has been moving away from the more perimeter-focused strategies of the past that emphasized controls over specific systems and devices to a more holistic approach that promotes protection of an organization's most crucial asset: information. This swing toward a data-centric security view aims to limit loss and the compromise of data from theft, mishandling and other breaches through the use of data loss prevention (DLP) principles, products and practices.

As a concept, DLP is effective because it concentrates on identifying the most sensitive and valuable organizational information and then works to eliminate the gaps that could expose that data to both internal and external threats. DLP can be applied to data in all of its stages: at rest, in use and in motion. It provides an approach to security that is particularly relevant in today's environments, where data is so easily created, shared and transformed.

Information has always been important from an operational perspective. But now that so much of it is digitized and organizations are employing more open communications models (which have the potential to make the environment more porous), it is even more susceptible to threats. Whether data is compromised because of negligence or malicious intent, breaches are often more costly on levels that can go far beyond the financial.

Consider the allegedly unauthorized release by WikiLeaks of the redacted U.S. State Department diplomatic cables, and the effect that this act had on international relations in the weeks and months following the cables' publication.

These documents, first leaked to the press in 2010, made headlines again the following year when it was revealed that the cables were published with a key to decrypt the redacted sections. While no lives were lost as a result of the published reports about the breach, the embarrassment factor was high to both the U.S. State Department and its allies. The exposure sent a clear signal to public-sector organizations in particular about the urgency of having the right controls in place to protect confidential and other high-value data.

Process Equals Progress

One of the more important security challenges IT departments face is identifying the right protections for both the data and the organization's operating environment. The IT staff has to balance the absolute requirement to safeguard critical information with the constant pressure for easier access to data. This task is further complicated when already extended organizations become even more operationally distributed and mobile, with staff and contractors running their own personal mobile devices over the enterprise network.

DLP offers a way to minimize loss and leakage without limiting productivity. Increasingly, organizations look at security and DLP as more of a process than a set of point products stitched together to defend against threats. The central idea is that all the elements must be in place to safeguard data as it is created and modified, at rest and in transit.

Although DLP cannot entirely eliminate loss, its broad objective is a realistic one: minimize theft, loss and exposure of confidential and sensitive data without interfering with operational efficiency. The technology and practices to support this goal have come a long way. In the past, point products were often too intrusive, inaccurate or otherwise ineffective. While an organization may have invested in DLP products, it wasn't unusual to find them gathering dust on a shelf.

Today, IT security professionals consider DLP a process that starts with recognizing the need to prioritize data so it can execute security policies designed to protect that information. While a breach of any data is unacceptable, DLP can build in multiple levels of security to ensure that confidential, sensitive and high-value data is protected, while lower-value information is subject to fewer controls. The object of this multilevel strategy is to minimize data loss while providing end users with as much transparency as possible into policy and practices.

This defense-in-depth approach requires the IT department to go through a number of phases to meet DLP goals. The first step in this process is conducting an inventory to discover high-value data and how it is handled and stored. Using this data inventory, the IT staff can classify information based on its sensitivity and value to the organization. This helps the IT staff design and enforce policies that are consistent with regulatory requirements, organizational priorities and mandates.

By taking a methodical approach to DLP, organizations can ensure that sensitive, high-value data, such as personally identifiable information (PII), financial information or intellectual property (IP), receives protections such as encryption and password-protected access. At the same time, an organization can also assign fewer controls to lower-value information.

It is crucial that organizations communicate policy information to end users interacting with the protected data. This kind of communication about a multilayered DLP process can go a long way toward ensuring maximum transparency and minimal data loss.

DLP ACTION ITEMS: A Five-step Process for Deploying DLP

Action	Description	Benefit
Discover	Identify data stores and flows, including all end-user interactions.	This action inventories critical location and process data necessary to assign security controls.
Categorize	Classify information based on value, sensitivity and confidentiality.	This action establishes a baseline for security measures assigned to data according to regulatory, financial and other factors.
Consolidate	Aggregate data stores for easier manageability, and eliminate outdated files.	This action simplifies the security process and lowers storage costs.
Design	Create security policies that apply protections to data and how it is handled based on classification.	This action supports mission-critical objectives, industry mandates and government regulations.
Execute	Enforce policy-based controls, with an emphasis on end-user education.	This action ensures that most critical and sensitive data is handled with the highest level of protection.

Protecting Against Unknown Threats

Having a strategy that implements protections based on the value and sensitivity of the data is essential to effective DLP. There is strong evidence that prioritizing data security produces positive results. In the Ponemon Institute's 2011 annual report on the cost of data breaches, the research firm reported that the per-record cost of a data breach actually fell to $194 from the previous year's $214 per-record rate.

Losses from theft and other data compromises by the 49 enterprises surveyed across 14 industries averaged $5.5 million per organization, a sharp drop from the $7.2 million the previous year. In essence, much less high-value information was breached in 2011, bringing down both the per-record cost and overall losses for the year.

Although the overall costs of loss are still substantial, the improvement is a good sign that effective DLP practices are having a real effect. Yet even as organizations get a better handle on data protection, the losses are still great, and many unknowns still pose a threat.

The emphasis on data security and DLP comes at a time when organizations are seeing increased attacks from new types of threats. One such threat includes a new breed of cybercriminal, known by the term *hacktivists*.

These socially and politically

motivated cyberattackers are often more interested in embarrassing their targets than in achieving financial gain. In the 2012 release of Verizon's *Data Breach Investigations Report* (an annual analysis of 855 incidents involving data theft, loss and compromise), it is noted that hacktivists were responsible for 58 percent of the total of records breached in 2011, up from nearly zero during the previous year.

This finding corresponds with other recent research showing that hacktivists pose an increasing threat to organizations. Along with some nonprofit organizations, public-sector agencies and higher education research institutions are particularly attractive targets for hacktivists, as well as cyberterrorists and other more traditional cybercriminals.

The High Price of Data Loss

Although the Verizon report found that 98 percent of malicious breaches are perpetrated by external sources, a sizable amount of data loss can also be attributed to internal carelessness and naiveté. The most recent Ponemon Study reports that negligence is the cause of 39 percent of all data loss. This category includes everything from misplaced notebooks and USB drives to unencrypted e-mail, all containing sensitive or confidential information.

Whether the cause of a breach is malicious attack or simple inattention, the result is often (at the very least) embarrassing and expensive — and in the most extreme cases, devastating. The higher the data's value, the more damaging the loss.

For example, files containing PII or sensitive financial information (data such as Social Security numbers, medical information, credit card account numbers or financial disclosures) are not only important to that individual, but also are governed in the United States by various state and federal regulations.

These include the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX) Act, which covers disclosures to the Securities and Exchange Commission. Organizations also must adhere to industry security standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

In the case of mishandled PII covered under HIPAA, the violator is subject to fines and litigation. For example, the University of California at Los Angeles settled a case with the federal Health and Human Services Department's Office for Civil Rights in 2011 for $865,000 when the agency demonstrated that staff members repeatedly accessed UCLA Hospital System patient data without authorization over a three-year period.

In 2006, the Department of Veterans Affairs suffered a widely publicized breach when a worker brought home a notebook, which was stolen when the VA worker's home was burglarized. The stolen notebook contained the names, Social Security numbers and dates of birth for more than 26 million veterans. While the thieves probably didn't have any knowledge of the information stored on the notebook, the data and the people it identified were compromised by the incident.

More recently, NASA experienced a series of breaches. In November 2011, interlopers with Chinese IP addresses hacked the agency's Jet Propulsion Laboratory. While the investigation is ongoing, it is known that the cybercriminals were able to tap into accounts to gain access to restricted files, remove data and install malware.

NASA Inspector General Paul Martin reported to Congress that in 2010 and 2011, NASA suffered more than 5,000 computer security breaches. These included the March 2011 theft of a NASA notebook containing the unencrypted controls for the International Space Station.

NASA spent more than $7 million on remediation as a result of these incidents. But given that at least some of the security breaches may have been initiated by foreign intelligence agencies and nonstate cybercriminals, it is difficult to put an actual price on the losses.

All of these incidents reveal the importance of data security. As embarrassing and costly as these breaches are, the potential losses for attacks on confidential data are far more serious. Today, it's a requirement for governments, educational institutions and private-sector organizations to have an effective DLP strategy in place. ■

RALLYING STAKEHOLDER SUPPORT

DLP is more than just technology. To be effective, the organization needs both appropriate policies and execution. A comprehensive and effective DLP approach requires having key stakeholders on board from the outset. This support is critical, not just for funding purposes, but also to ensure support through policy development and enforcement.

For the IT group, this means educating directors and managers inside and outside the technology organization about the existing threat environment and the ramifications of loss to operations and budget. The IT team can identify potential vulnerabilities that could expose data to being compromised. It's also worth pointing out DLP's benefits beyond security, including greater transparency and insight into operational efficiencies and issues.

CHAPTER 2

The Data Protection Cycle

Securing data, from discovery to post-incident response

In an ideal world, an organization could protect all its data against theft, loss or compromise. The reality is that breaches are inevitable and resources are limited, so it falls upon the IT department to identify and address the organization's greatest risks to data security.

One way to assess which kind of DLP controls to apply is to place a value on the cost to the organization if a particular data file were to fall into the wrong hands. In other words, if the data were stolen or otherwise compromised, would the impact be overwhelming, disruptive or negligible?

For example, a defense contractor might look at computer-aided design files as valuable intellectual property that requires multilayer authentication and encryption to protect. In another scenario, basic password protection is more than adequate for a local government's e-mail system.

Although allocating protections may seem intuitive, there is still room for error. This is especially true for organizations that lack a clear understanding of what data they possess, which staff members and contractors have access to it and how this information is handled.

Without this baseline insight into data assets, it is impossible to successfully set, communicate and enforce effective data security policies. This necessity for transparency extends to contractors who may be in possession of sensitive data. Regrettably, there are many examples where a lack of clarity and insufficient controls have resulted in costly losses.

In 2011, backup tapes containing patient health records, credit card account numbers and other PII of 4.9 million active duty and retired Department of Defense personnel were stolen from the car of an employee of Science Applications International Corp. (SAIC), a contractor for military insurance provider TRICARE. Within weeks, TRICARE members affected by the breach reported fraudulent activity on their accounts, including unauthorized withdrawals from their personal bank accounts.

Although it is clear that such critical data should not have been left unencrypted in a contractor's car, sufficient protections were not in place prior to this incident. The SAIC/TRICARE case underscores the need for IT organizations to have a pragmatic and clearly communicated policy on the storage and transfer of confidential information.

Starting with Data Discovery

Deploying an effective DLP system starts with having an excellent grasp on the data that is being created, modified, shared and stored within the organization. The IT staff needs to focus on credit card account numbers, patient records, human resources files and intellectual property as it prepares a baseline of what kind of data it expects to discover that will require special security protections.

Regulatory compliance is one important indicator of how to prioritize security controls. Organizations can look at the effect of losing regulated information as a way of determining what kind of controls they should apply.

Is the information protected under federal regulations, such as the Personal Data Privacy Act of 2007? Do state laws or industry initiatives apply, such as the PCI DSS? Noncompliance with PCI DSS can subject an organization to severe penalties and leave it vulnerable to legal action.

Data discovery, the process of scanning databases, hard drives and other sources for confidential or sensitive information, can find regulated information and help categorize how that data is secured. At the same time, data discovery can support the overarching compliance process by documenting what data the organization creates, modifies and stores.

Classifying, documenting and then securing data appropriately can improve the compliance scope, further targeting where the most sensitive and confidential data is and then verifying that the appropriate controls are applied. This documentation should expedite and simplify the audit process, verifying that adequate controls are in place and proving that sensitive PII and confidential data are handled according to HIPAA and PCI DSS requirements.

Data discovery can also help organizations improve operational efficiencies in another important area. Knowing what information is stored where — and in how many locations — supplies IT management with the facts it needs to align data retention practices with regulatory demands and storage budgets.

Risk-benefit Analysis

Although the accuracy and effectiveness of the technologies used to support DLP and data discovery have improved in recent years, many organizations still struggle to perform a comprehensive risk assessment. IT organizations too often lack the resources to identify vulnerabilities in their environment and the expertise to understand the best way to revise security policies to close these gaps.

Turning to a third-party provider for a risk assessment is a good option for many organizations. Service providers often have the experience and the right mix of technologies to help internal IT staffs identify and address areas of exposure. A third-party provider will typically start an assessment with a high-level discussion about the organization's objectives and issues and then move through the discovery and data classification process.

Risk assessments, whether conducted by a third party or the internal IT team, shed light on whether the organization's existing data security policies and practices are providing adequate protection, and where improvements and corrections are needed. This inventory gives the IT department the insight it needs to refine policies and readjust security controls to minimize data loss and compromise.

A third-party risk assessment offers specific information on how an organization should prioritize its security spending and how this investment will help support operational stability.

Data Identification Tools

The central goal of data discovery and classification for DLP purposes is to find what data the organization actually possesses, who is using it and how it is handled throughout its lifecycle. Analysis engines used for data discovery seek out information on data in two phases: at rest (stored information) or in transit (traversing the network).

Scanning servers, databases, hard drives and network devices provides the IT organization with an outline to use to find out who is using what data, and what, if any, protections are applied. At a high level, data discovery offers a fairly detailed perspective on organizational processes by showing how information is created, transferred, modified, stored, accessed and then altered again.

DLP solutions use two primary methods to flag sensitive or confidential data for special controls: pattern matching and tagging.

For pattern matching, the DLP system relies on common characteristics, such as 16-digit numbers linked to a name, or a six-digit expiration date signifying an item that requires special security protections, such as encryption or user authentication for access. To discover this data, the DLP tool can either use data culled from a database dump or log on to systems to parse database and file structures. The solution then reports on the found data, including any version changes and who is modifying the files.

Tagging requires IT administrators to create a database of sensitive documents or other data stores. To spot tagged data in transit or use, the DLP solution can use one of two methods.

In the first, the DLP technology uses a technique called document fingerprinting. This technique applies an algorithm to match files in transit that map to the tagged files flagged for special controls. In the second, the DLP solution keeps a full copy of the tagged documents in a database, creating an alert on files that match the pattern of tagged documents.

Data discovery and classification have an additional benefit beyond providing the structure for secure data handling and DLP. These processes can also help an organization understand where there is room for consolidation. During the discovery process, the IT staff often finds redundant data files and old data that can be consolidated. Not only is it easier to secure data that's unified in a single location (rather than files spread across multiple databases), but it also streamlines the management process and lowers storage costs.

CATALOGING RISK, FED STYLE

UNDERSTANDING THE FOUR MAJOR RISK CATEGORIES

Security Category	Exposure Risk
Top Secret	Loss would compromise national security
Secret	Loss would seriously damage national security
Confidential	Loss would damage national security
Unclassified	Loss would have no effect on national security

Categorizing Data

Data discovery yields information that is critical to helping organizations assess what information needs to have special security controls (such as encryption or limited-access credentials), and where that information is located. Federal agencies such as the CIA and the Defense, Energy and Homeland Security Departments categorize information based on its sensitivity to national security, specifying who can access what data and how that information should be protected.

Each data category *(see Cataloging Risk, Fed Style sidebar)* requires specific physical and logical security protections. For example, top secret data must be stored in vaults, while the requirements for confidential data are less stringent. Access to data is based on more than the user's role; personnel must achieve a security clearance through a background investigation that maps to the data they use.

Other organizations take a page from the agencies that deal in top secret data to establish data protections based on its sensitivity to the organization and whether that data is regulated by law or industry initiatives such as PCI DSS.

To help set these controls, data can be grouped together with the level of security required to protect it in mind. For example, organizations can catalog data according to the degree to which it needs to be kept private along the following lines:

- **Public data:** marketing information, contact data
- **Internal (but not high-value) information:** organizational charts, presentations, document templates
- **Sensitive data:** strategic plans, proposals, compensation information
- **Regulated data:** Social Security numbers, payment card records, healthcare information

\\\\ END USERS PLAY AN INTEGRAL ROLE IN THE SUCCESS OF ANY DLP STRATEGY BY SUPPORTING THE CONTROLS PUT IN PLACE.

Drafting and Communicating Policies

Having a standard way to categorize data according to security requirements will help to streamline the policy design and execution. Once the IT department completes the data discovery process, the organization can refine its security policies and practices.

How extensive required policy changes are depends largely on an organization's understanding, prior to the discovery process, of its own risk level. During the policy development phase, it is essential that the IT department draft balanced data protection guidelines that adequately protect data but don't disrupt productivity and general workflow.

The IT department needs to inform end users of any policy adjustments. End users play an integral role in the success of any DLP strategy by supporting the controls put in place. Policy communications can also deter both nefarious and general carelessness by reminding staff of the consequences of failing to handle data according to policy.

Although IT staff are often responsible for setting up the controls and executing policy from a technical standpoint, they should also involve executives and non-IT managers in both creating policy and then communicating the specifics to end users. Managers are the most effective ambassadors for outlining how sensitive information should be handled by their staff.

These policies can extend to multiple types of media. For example, IT and operational line managers might dictate that specific tape drives cannot be removed from the premises under any circumstances.

Data Protection Tools

At a high level, policies should employ a number of protections to limit data loss and compromise, starting with having a method in place for tracking both inbound and outbound communications, including those with outsourced staff and partners. An organization also should have the tools necessary to encrypt e-mail and other files that contain confidential data.

At the same time, the IT staff needs effective antimalware software that prevents data corruption. All types of organizations need policies that are consistent with regulations and industry mandates.

Organizations that possess intellectual property, which may or may not be easy to identify during the discovery process, should also make sure that the security of this valued resource is properly addressed. IT also needs to have mechanisms in place to enforce policies.

The good news about DLP today is that organizations have many choices in the types of protections they can apply to safeguard data. There are controls that provide good support for any of the many challenges faced, starting with multilayer firewalls that can block suspicious inbound traffic and filter outbound content to limit leakage.

Encryption, which uses one of a number of different algorithms to render plain text unreadable to anyone without a key to the code, is another of the more commonly applied data protection methods. There are a number of different applications for encryption available to address a range of scenarios.

Organizations can choose file-system encryption (which encrypts a single data file or folder) or full-disk encryption (which protects a whole disk volume). File-system encryption may be used by itself or in conjunction with full-disk encryption. Individual passages within a document can also be encrypted to redact confidential information.

The IT staff can also use encryption to secure data in transit. For example, an enterprise may dictate that remote users access data via a virtual private network (VPN) connection that encrypts data communications.

With a Secure Sockets Layer VPN (SSL VPN), users can access a single or multiple network services via a secure browser connection. Another option is an IP security (IPsec) VPN, which installs software on the client system to authenticate that user's identity before access to services and organizational data files is granted.

Secure Data Access

There are any number of methods the IT staff can use to grant or limit access to specific systems or files. These protections are as basic as requiring a password or as sophisticated as dual-factor authentication or biometric access controls that verify a user's identity.

CASE STUDY

SOFTWARE OFFERS FIRM PROTECTION

Learn how some federal agencies are addressing data risk with data loss prevention software solutions:

CDWG.com/dlpguidecs

An organization that is processing online financial transactions can use a certificate authority (CA) to grant Extended Validation SSL certificates that validate (for the user's benefit) that a website is secure. Extended Validation SSL certificates also encrypt data in transit, supporting a stronger trust model between an organization and its clients.

The IT staff can also apply a policy that requires multiple controls. For example, the organization can require remote users to log in to the intranet via an SSL VPN, then use dual-factor authentication to gain access to the enterprise resource planning (ERP) system, where file-system encryption is then required to protect specific financial data. For less critical information, such as marketing material or other public data, restrictions are often minimal and may not even require a password for access.

There are also a number of policies the IT department can enact with respect to how it manages ongoing data security through general maintenance and best practices. These include using automated patch management to find and fix any application vulnerabilities, ensuring browsers are up to date with the latest antimalware updates and verifying that the appropriate data filtering controls are in place.

The IT staff can also enact physical security controls to limit exposure and loss. An example of this would be requiring that any collocation facility that's used to store data meets ISO 27001 standards. And given the increasing use of mobile devices, an organization can also institute a policy outlining when to perform a remote wipe of a lost notebook or smartphone to prevent data compromise.

Reviewing Security Policies

A successful DLP strategy will include policy management as an ongoing practice. The IT staff and the larger organization need to take a close look at their operational processes to identify areas of inefficiency and potential vulnerabilities. Both organizationwide and IT managers also need to assess the efficacy of their security policies, consistently reviewing whether these mandates are appropriate for their organization.

Some of the questions the IT staff needs to revisit include the following:

- Are data security policies instituted consistently across the organization?
- Are security policies and practices impeding organizational productivity?
- How are these policies communicated to end users?
- What, if any penalties, are in place for noncompliance?
- Do data security policies support the compliance audit process? If not, where is there room for improvement?
- Can the IT staff document a reduction in security incidents through policy and practice changes?

It is important for the IT staff and the organization as a whole to look at its data security policies as a work in progress. This may mean more than just periodically reviewing mandates and controls.

Given the dynamic nature of most workplace environments today, the organization may need to inventory the content it is trying to protect. The good news on this front is that as data discovery technology and third-party expertise in risk assessment continue to improve, organizations will have many options from which to choose for maintaining a strong foundation for data security.

Incident Response Plan

Even with the best of efforts, no policy or practice can guarantee to entirely eliminate data theft and leakage. After all, as long as there are antagonists willing to invest considerable resources in creating more sophisticated hacking methods and finding vulnerabilities, there's always the potential for a breach.

It's critical that all organizations have a thorough incident response plan in place to deal with the immediate and long-term effect of a breach. This will not only help an organization deal more effectively with regulatory authorities, partners, customers and the general public, but it will also prescribe the appropriate steps to mitigate losses from a data compromise.

An incident response plan should identify who should be notified when data is compromised. Develop a comprehensive plan for general instances and a more specific plan for certain types of breaches that may require special handling.

The IT department will also need a post-incident plan to close the loop on any investigation. Was the source of the breach malicious? If so, was the attacker identified? Were arrests or prosecutions involved? What was the cost to the organization, both monetarily and in terms of public perception? Ultimately, the IT department will want to be in a position where it can prove it not only reacted well to the crisis and minimized losses, but also instituted changes based on lessons learned from the event. ■

A PARTNER IN RISK MANAGEMENT

Far too many organizations lack the internal resources or expertise to fully understand their security posture. This leaves them vulnerable to numerous unknown risks, which makes it more difficult to develop a truly effective data security strategy. IT solution providers with the appropriate skills can prove their worth to customers by giving organizations insight into their risk profile and helping them make a plan to address any security gaps.

CDW•G offers complimentary risk assessments to prequalified organizations. These start with a discussion to get a perspective on the customer's security concerns and priorities.

Following an initial consultation, CDW•G can offer an outsider's perspective on potential gaps in strategy and execution. CDW•G also offers remediation advice, as well as the budgetary justification for making a security investment that will improve the organization's risk profile.

CHAPTER 3

Network-based Solutions

Awareness at the network gateway is more crucial than ever to maintaining effective data security

Network connections still play a crucial role in data security, even though much is made in IT security circles about the clearly defined enterprise perimeter being an anachronism. The routers, switches and other devices that forward traffic between endpoints reveal vital information about data in transit and also offer an unwelcome route for data theft, loss or compromise.

Once the focal point of DLP solutions, network-based DLP still plays an important role in tracking traffic and defending against breaches. These solutions, which use techniques such as deep packet analysis to examine data in transit, are especially relevant to DLP strategies given the dominance of IP traffic today.

Network-based DLP technology scans traffic at network access points. It examines web, e-mail, File Transfer Protocol (FTP) and other applications, filtering inbound traffic and blocking malicious code, as well as scrutinizing outbound traffic for potential leaks. These solutions can filter out malware, block access to URLs containing inappropriate content and stop confidential data loss over IP connections.

Although there is clear value in filtering inbound network traffic to block malware or inappropriate content, the real benefit of these solutions comes in their ability to track traffic on the egress. After all, it is through outbound traffic that sensitive and confidential data can be funneled out of an organization.

Network-based DLP can prevent accidental leaks and misuse of sensitive files, blocking workers from transferring content that includes regulated or otherwise classified materials from e-mail accounts. In a similar vein, network DLP solutions can stop an end user from posting sensitive or confidential information to third-party sites. Network solutions can also stop deliberate theft, preventing the transfer of files via an FTP site that is initiated either by an internal user or backdoor programs started by a Trojan or other installed malware.

Types of Network-based Solutions

A complement to endpoint and storage-focused DLP, network-based solutions close the DLP loop by tracking traffic in transit and running interference to keep sensitive data from leaking. Network-based DLP solutions are typically appliances connected to an egress point via a network tap or a switch port analyzer (SPAN) that scan data in traffic, looking for policy violations. Some solutions that focus on monitoring particular traffic channels, such as the web or e-mail, collect data from a proxy server.

Network-based solutions include products such as Symantec Data Loss Prevention Network Protect, McAfee Total Protection for Data Loss Prevention and Websense Web Security Gateway.

The tactics vary for detecting and remediating a breach, but the majority of these solutions are part of a larger solution or they work with other technology to gather information from storage systems and endpoints. The most sophisticated of these solutions work with content analysis and data discovery tools to spot possible breaches before the network is attacked.

A network-based DLP solution may have the native ability to execute on a policy when a violation occurs, or it can work with separate enforcement tools to route sensitive data to a gateway for encryption. These separate enforcement products apply a model similar to Symantec's, communicating with a centralized management server that may have deeper content analysis capabilities and also a record of incident history.

Network-based solutions can execute on policy, stopping unauthorized traffic, quarantining an e-mail or a custom script, and routing sensitive data to an encryption gateway. Although each product applies different principles to detecting possible data breaches, most use either deep-packet inspection (which collects information on all traffic) or sampling (which collects a representative percentage of data). There are benefits and drawbacks to each approach.

Sampling has a minimal impact on network performance, but because only a percentage of data is gathered, there is a risk of missing a leak. Deep-packet inspection has a better chance of blocking sensitive content, but will slow network traffic.

How Network DLP Solutions Work

Network-based DLP solutions use one of two approaches in deciding whether data in transit can continue on its path, should be flagged for special handling or blocked entirely.

A content-neutral approach applies controls without regard for the particular data involved in a transaction. For example, a content-neutral solution could be used to ban downloads to USB drives to prevent accidental leakage or deliberate theft of sensitive materials.

Content-aware DLP technology uses a more sophisticated set of techniques to find data within a particular system, device, data store or e-mail and ensure that it is handled according to policy. These products capture data at rest or in motion and, using a form of file cracking, assess whether the data is sensitive in nature.

This may require drilling down into data embedded within a file — for example, an Excel spreadsheet integrated into a PowerPoint presentation. Content-aware DLP technology can act on policy in real time — logging, reporting, classifying, encrypting, moving and even enacting enterprise data rights management protection (*see* The *Multiple Attack Vectors sidebar*).

There are a number of methods that content-aware solutions use to analyze data. A rules-based approach is one of the more frequently used techniques for triggering an alert on sensitive information within a file. DLP solutions using a rules-based system for analyzing data look for predefined expressions that denote sensitive information.

For example, DLP solutions applying rules-based analysis might look through objects for nine-digit numbers that resemble Social Security numbers, or they may alert on a mix of numbers and letters that matches a medical billing code. Typically, solutions that use rules-based analysis also include more customized conventions, such as a name text search that looks for a name and address in close proximity to a 16-digit number, which indicates PII that may be regulated under state or federal law.

There are a number of reasons why a rules-based approach to network DLP is so popular. Rules can be processed quickly, speeding the identification of policy noncompliance. Most products that use rules-based systems come with some predefined templates that map to particular regulations or other sensitive data. This helps IT administrators expedite the configuration process.

Accuracy is the most significant downside to using a rules-based system for DLP analysis. Despite some reported improvement, this technique tends to produce a lot of false positives because of its broad-based analysis.

DLP solutions do use other forms of analysis to spot data policy noncompliance issues, including file categorization, which looks for content that is easily classified. File categorization uses an inventory of predefined rules and keywords that outline sensitive or classified content, such as healthcare data regulated by HIPAA or confidential diplomatic files.

Exact file matching, a method that flags content that contains a particular code, is often used to block leakage of media files where there is no text to examine.

Partial document matching, another DLP technique, takes a hash of a portion of a document to look for sensitive data. In this method, IT administrators can set policy to look for specific content that may have been copied into another file. For example, partial document matching might spot a paragraph from a scientific research paper copied into an instant message.

Integrating with Endpoint Solutions

As valuable as network-based DLP is in filtering content and blocking data leaks, the technology is only one part of a comprehensive data loss prevention process. To be truly effective, network-based DLP solutions need to work in tandem with systems that monitor network endpoints and storage.

Endpoint systems can catch the movement of data that a network-based DLP system may not. For example, an endpoint system can spot and block an illegal download of a file to a CD-ROM.

Endpoint DLP products that protect data at rest can also catch users who try to store sensitive data in the wrong location. Whether it's a careless error or deliberate action, such activity alerts the IT department to policy noncompliance.

For an extra layer of protection, organizations can also use discovery technology to disclose questionable activity, such as a file transfer of sensitive data. This information makes IT administrators more effective in preventing leaks that otherwise might go undetected.

In cases where access to classified data is limited, network-based DLP products used in tandem with identity management systems can verify that only authorized users tap into such data. Identity and access management solutions use a number of controls, ranging from simple passwords to biometrics, to authorize users to open, edit or transfer a file.

Technology providers are looking at ways to integrate DLP and identity management technology to simplify administration and to lessen data losses. IT solution providers can play an important role immediately, not just in terms of integrating the technologies into the organization, but also in helping define how identity management can be used in conjunction with DLP solutions to improve their effectiveness.

Cloud Computing Concerns

The growing adoption of cloud computing (a technology designed with the express purpose of making it easier to access and share content) is one of the chief challenges associated with DLP today. As defined by the National Institute of Standards and Technology, cloud computing requires broad network access. And to some wary IT administrators (and lawyers), it has all the makings of a massive data sieve.

However, the cost and flexibility that the cloud promises are too good for most organizations to ignore. So as more public- and private-sector organizations explore the cloud, expect to see more of an emphasis on network-based DLP technology by manufacturers. While IT administrators may worry about loss of control over data in an on-demand environment, network-based DLP solutions are actually very effective in supporting existing data-handling policies in the cloud.

Network-based DLP solutions have a perfect perspective from their location at the network's interconnection point to look out for unauthorized data movement. These solutions can stop sensitive data from being accidentally or deliberately transferred to a public cloud, or even a private cloud environment where the security standards may be more lax.

The effectiveness of network-based DLP technology in the cloud is further enhanced when it is used in association with other solutions, such as identity and access management, to set the right controls for secure data handling. It is critical that organizations define cloud security policies carefully and revisit these mandates frequently to ensure that sensitive and confidential content is protected. ■

MULTIPLE ATTACK VECTORS

Network-based DLP solutions promise to support overarching efforts to limit data loss and leakage. Unfortunately, though the very best technology can go a long way toward preventing many breaches, no one solution can guarantee that an organization will stop all theft or misuse.

Though recent reports on declines in the cost of breaches and the lower sensitivity of the data stolen are welcome improvement indicators, cybercriminals will always find new ways to attack. By the same token, organizations can also count on users to continue to lose notebooks and smartphones and engage in other forms of carelessness that put data at risk.

So how do cybercriminals steal or compromise information? In many cases, they actually capitalize on multiple entry points and vulnerabilities. According to the 2012 Verizon *Data Breach Investigations Report*, the top methods of attack included the following:

- **55%:** exploitation of default or guessable credentials
- **40%:** use of stolen credentials
- **29%:** brute-force attacks
- **25%:** exploitation of backdoor or command-and-control channels

Endpoint–based Solutions

Closing the loop on data loss starts and finishes at the endpoint

Classifying data and monitoring policy compliance on the network are just part of the DLP picture. Organizations also need ways to monitor activity and enforce policy on endpoints, which can include file systems, PCs, notebooks and other user devices. DLP efforts also need to include technology that can track data at rest, information stored in databases and other file systems.

By covering all of these data environments, an organization gets a better perspective on whether its data security strategy is adequate to keep ahead of both external threats and the kind of casual misuse that leads directly to costly data losses. With literally billions of external attacks reportedly launched each year and countless deliberate internal breaches, organizations need to pay attention to the endpoint.

Applying centralized data security policies, endpoint DLP products can discover, track, report on, and protect data at rest, in use or in motion. These solutions go a long way toward closing gaps in DLP deployments that formerly were focused almost exclusively on the network.

This is done first by discovering content that is created, modified and stored on end-user systems and servers, and then by extending the IT organization's ability to enforce policies on remote systems. Endpoint DLP products also give administrators insight into data transfers to portable storage devices which, without proper monitoring and controls, present a prime opportunity for data leaks.

Endpoint DLP products can prohibit classified data from being cut and pasted into other objects or faxed or printed. IT administrators can also set policies to automatically encrypt some data based on the specific content, or even based on the application.

Classes of Endpoint–based Products

Of course, the endpoint is more than just the location of a breach, accidental or otherwise. It can be the opening that cybercriminals use to gain entry to steal files from other locations on the network

\\\ ENDPOINT DLP SOLUTIONS CAN OFTEN **SPOT THREATS** THAT **ESCAPE THE RADAR** OF A NETWORK-BASED DLP.

or used as a launch pad for other attacks. To thwart external attacks, endpoint DLP solutions work with products that deflect viruses, malware and other nefarious content to be more effective against a diverse threat environment.

Today, the ability to block data from being moved to a CD ROM or other storage device is often handled as a function of broader threat protection suites, many of which work in conjunction with endpoint DLP products. But as concerns mount about illegal downloads — such as the 250,000 diplomatic cables allegedly stolen by a U.S. Army staffer and then distributed via WikiLeaks — more organizations are looking to endpoint DLP to fulfill the device security function.

So what functions can endpoint solutions handle today? At a high level, endpoint DLP solutions are agent-based products that scan files, folders, and databases in workstations, notebooks and mobile devices, flagging instances of data security noncompliance and stopping classified data from seeping through the endpoint.

Some of these solutions can also discover data and classify content according to its sensitivity. Separate products are available, often as part of the broader DLP suite, that also include discovery and classification software to scrutinize content on servers.

Endpoint DLP solutions are typically more context-sensitive than content-aware, zeroing in on which user is accessing what file, focusing in on specific types of data and tracking data flows. They can often spot threats that escape the radar of a network-based DLP, including situations where a keylogger-infected PC transmits stolen data to an external attacker.

These solutions dig deeper into content, applying sophisticated techniques to identify dangerous threats. Endpoint and server-focused

DLP products use methods such as database fingerprinting to focus on specific factors within a file to identify, track and protect sensitive data.

Using information culled either from a database dump or a live feed, database fingerprinting can follow an established policy that requires it to flag specific documents based on particular attributes, such as a specified number of digits or words.

Database fingerprinting can be fairly granular and customized. For instance, the device can be set to only flag payment card numbers tagged to the client database for special protections, but not 16-digit credit card numbers of workers making online purchases.

Some database fingerprinting technology can tailor its analysis based on multiple factors. For example, a patient name with a Social Security number and medical record number might be considered classified.

Although some solutions are stand-alone, endpoint products often are part of a large suite of DLP solutions that include technology for network DLP, discovery software and an inspection server that can handle deeper content analysis than an agent can in the field.

Products like Symantec Endpoint Protection and McAfee Endpoint Protection can tap into a common set of data security policies shared across all DLP technology, including network-based solutions. Having a unified policy approach reinforces consistency by making it easier to deploy rules in a production environment.

One concern about having endpoint-based solutions working so closely with network-based DLP is that the endpoint might issue a very different directive from its counterpart. For example, an endpoint might be inclined to encrypt a sensitive document, while a network-based product would likely quarantine the data.

Coordinating DLP Policies

Regardless of the route an organization chooses (whether picking a discrete endpoint protection solution or an integrated DLP suite), it is important to coordinate policies across all devices and systems. IT departments can manage policies through their directory servers, making it easier to implement and support standard controls.

Organizations can modify policies based on evolving operating conditions, shifting priorities, changing regulatory requirements and technology conditions. Administrators may also choose to modify policies to address new operating models or different conditions in different parts of the organization.

For example, the IT department might require that sensitive data created at a remote site include more access controls than comparable information maintained at headquarters.

Some content analysis methods used by DLP systems are also often too resource-intensive for some endpoints. For example, partial document matching can require too much memory to make it a practical option for a notebook. As an alternative, an organization may opt to use a pattern-matching method to catch data files containing Social Security numbers before they are distributed.

While there is a higher rate of false positives using pattern matching, the IT staff can set the DLP system to monitoring mode so that users are alerted to a possible policy infraction. But they still have the option of sending the file if they want. Of course, the trade-off is a higher risk that regulated PII data may be compromised.

MOBILE SECURITY CONCERNS

The endpoint's impact on DLP solutions has become more complex as the number of mobile devices used for work purposes continues to expand at an astounding rate. Most organizations have to support a mix of mobile devices today, including notebooks, tablets and the influx of high-powered smartphones that have become integral to running organizations today.

The bring-your-own-device (BYOD) trend, which allows workers and contractors to use personal devices for work, only ratchets up concerns about new endpoint-related security risks.

Although it is challenging to load a CPU or memory-intensive agent onto a smartphone, some providers tap into a function integrated into these devices that makes it possible to initiate a virtual private network (VPN) tunnel from the smartphone to the DLP system. This allows the DLP system to peek into the data on the devices. A number of providers are also now offering tablet-specific data loss prevention solutions that can initiate functions such as remote data wipe.

However, none of this is enough to stave off the considerable risk associated with data literally walking around in someone's pocket. Nor do most of the DLP solutions have a way to address challenges in the near term, such as how to prevent a data leak via Bluetooth or some other channel that remains unguarded.

This brings up the importance of end-user education with regard to data security policies and enforcement. Endpoint DLP is by design a transparent process that requires end-user participation. End users must understand data security policies and their respective roles in complying with these mandates, and must demonstrate this understanding to their managers and the IT department to safeguard sensitive and confidential content.

The human resources department should have written documentation available to staff outlining general policies with respect to data handling. Another effective strategy is offering ongoing education, tailored to individual roles within the organization, on how these policies are instituted and enforced. Like the data they are developed to protect, policies are continuously evolving.

End-user education should include instruction on technology-related data handling, such as what to do when a file is quarantined or when the user receives an alert that the data contained in a file about to be transmitted is sensitive. Users also need to know what to do with nontechnical data, such as media or computer systems that need to remain at headquarters. Confidential information should only be shared with authorized users.

Encryption Solutions

Besides blocking and quarantining data, one of the most commonly used and effective methods of data security is encryption. Encryption software uses special algorithms to scramble data so that only those with the key to decrypt the content can see sensitive or confidential information.

Encryption is useful for protecting regulated or highly sensitive content, including PII data that must be protected to meet HIPAA or PCI DSS requirements. Endpoint DLP solutions are starting to include more file encryption capabilities or integrating other encryption software to protect data both at rest and in motion. Encryption is also an important component of many channel-specific DLP solutions, such as those focused on preventing data loss through e-mail systems.

Organizations can encrypt data found within a file, an entire file, an entire folder or even an entire drive. IT departments can also use encryption software to protect data transmitted over an insecure channel. Encrypting data in motion does come with a downside. With this approach, the content is masked to network-based DLP solutions, making it possible for encrypted data to be leaked by someone who can decrypt it once it is stolen.

Encryption software uses either a symmetrical model (where a common key is used to encrypt and decrypt data), or an asymmetrical approach (which uses separate keys). Each model comes with its advantages and disadvantages. Symmetrical encryption doesn't require much processing power from the CPU, but managing the keys can be a challenge. Asymmetrical encryption is CPU-intensive, but key management is more straightforward.

Endpoint DLP solutions can detect when a document contains data that should be encrypted and can alert the end user that an action is required. This is one of the many reasons why IT organizations need to educate users, so that they are aware of procedures that can be taken to avoid an interruption in their workflow. ■

PRODUCTIVITY IN THE BALANCE

Having the end user educated and involved is critical to the effectiveness of a DLP strategy. But getting staff buy-in isn't a given, particularly considering that endpoint DLP enforcement tools can be disruptive to normal workflow.

This is one of the many reasons why it is vital to have unit managers on board as an organization maps out its DLP policies and practices. These managers can help minimize the effect that controls such as blocking and encryption will have on productivity.

At the same time, line managers have the best perspective on where there is greatest tolerance for risk within their unit and where it is critical to use the most maximum-strength protection to secure the organization's data.

CASE STUDY

BYOD DLP

Bring-your-own-device programs are pushing some universities to look closer at how to improve endpoint security. Learn how they are using DLP solutions to address this concern:

CDWG.com/dlpguidecs2

CHAPTER 5

Channel-specific Solutions

Effectively targeting key communication methods with DLP

One major challenge organizations face today is developing a comprehensive DLP strategy that's both effective and practical. Although DLP technology has made impressive strides in recent years, deploying DLP into highly diverse and often geographically distributed organizations takes time and money. These systems are also very complicated.

Yet, in an era where one data breach headline in the news follows another, no one can afford to put DLP on the back burner. Deploying an effective data loss prevention strategy is an especially difficult proposition for organizations that may not have the budget or expertise to implement the required data security controls.

Many organizations seek to resolve this skills gap by turning to technology that targets commonly used and inherently insecure communication methods such as FTP, or web-based protocols such as Hypertext Transfer Protocol (HTTP) or e-mail. These are the channels most organizations focus on because they represent the most common avenues for data traffic.

Focusing on a widely used application such as e-mail is a practical way to reduce leakage without requiring the extensive investment in an enterprise DLP solution. Channel-specific products typically work with other security solutions to extend their native security capabilities, or are increasingly part of a broader security solution. When they are integrated into a broader solution, DLP features are packed into products such as an e-mail security gateway or a unified threat management (UTM) system.

By connecting channel-specific DLP efforts directly to complementary security functions (such as authentication or antimalware), these solutions can secure content and demonstrate compliance with government regulations or industry mandates.

For example, a secure e-mail gateway that includes DLP features, bundled with e-mail reputation analysis (which identifies and blocks threats based on the sender's status) and encryption, can provide a highly proactive defense.

It also offers documentation that proves compliance with HIPAA.

Because security investments are driven primarily by urgent security concerns or the need to comply with regulations, this direct link to compliance drives home the appeal of these channel-specific solutions. That these products also tend to require less intensive integration and management support further distinguishes them from endpoint- and network-based DLP solutions.

Channel-specific Product Classes

High profile data breaches such as the WikiLeaks case highlight how vulnerable organizations are to attack. The risks associated with exposure put the responsibility on the IT staff to demonstrate that it has adequate protections in place to minimize, if not eliminate, loss and leakage.

Unfortunately, the volatility of the current threat environment and often limited security expertise leave organizations outmatched and unprepared to manage the risks they face. Channel-specific DLP offers a more practical and effective alternative to the random approach that too many organizations use.

At a high level, channel-specific DLP offers an organization a way to address security on its most commonly used communication methods. Applying content analysis techniques that mirror those used by network-based and endpoint DLP technology, channel-specific products offer functions similar to network-focused DLP products, including discovery, classification, reporting and enforcement.

DLP capabilities can be integrated into products such as Cisco Systems' IronPort e-mail security gateway or Trend Micro's ScanMail Suite for Microsoft Exchange. It's also possible to deliver channel-specific DLP features through the cloud via a software as a service (SaaS) model. Some of the early channel-specific offerings include solutions that combine additional features for web-based content security or hosted secure e-mail gateways.

For policy guidance, channel-specific products rely on centralized data security policies, often tied to Active Directory or some other directory service. These solutions scan inbound and outbound e-mail, web, FTP and other traffic, looking for policy noncompliance.

Unlike their network-based and endpoint DLP counterparts that typically use multiple content analysis methods, channel-specific solutions apply just one or two methods to assess whether sensitive data is handled appropriately.

Channel-specific solutions also tend to use simplistic techniques. For example, while an endpoint DLP product might use two or three complex methods, such as database fingerprinting, statistical analysis and categorization to evaluate how sensitive data is handled, channel-specific solutions apply straightforward techniques, such as digital fingerprinting.

Digital fingerprinting builds a hash file from a specific source. Then the DLP system can flag content whenever the data is cut, copied and pasted into an e-mail or downloaded onto a USB drive, and the system can alert IT administrators to block the data transmission.

Web-focused DLP technology analyzes data carried over HTTP and HTTPS for anomalies that indicate a vulnerability or suspicious activity. In the case of HTTP traffic, the DLP solution must be able to decrypt the content so it can peer inside and guarantee that the data is properly handled.

Channel-specific DLP has a number of inherent benefits. For starters, it is simple to deploy and manage. Unlike endpoint and storage-based DLP, which typically requires IT staff to distribute agents to each endpoint and server, channel-specific technology sits at the gateway and often incorporates other features, such as e-mail archiving.

By focusing on e-mail and web traffic, which carry a large percentage of content throughout the organization, channel-specific technology is well-positioned to track activity and enforce policy. Because of the broad use of these channels for data transmission, they are also popular entry points for cybercriminals.

Though the majority of stolen and compromised data is lifted from servers, e-mail and web traffic are often conduits for attack as well as routes out of the organization for cybercriminals carrying stolen data. Similarly, e-mail is the source of many accidental leaks.

Integrating e-mail and web-specific DLP with other preventive measures, such as antivirus and antispam software, is a particularly effective way to thwart attacks on those channels. Of course, the singular focus of channel-specific solutions has some clear shortcomings.

For example, while a secure e-mail gateway with integrated DLP capabilities will halt a message containing classified intellectual property data, it will entirely miss an FTP download containing the same high-value content.

Deployment Scenarios

Channel-specific technology is a particularly useful way to protect e-mail, which comprises many endpoints accessing content outside the firewall or through a webmail server.

E-mail–focused DLP helps IT teams better gauge how secure their webmail communications are while adding greater control over the data handled through the system. Many e-mail gateways and secure mail solutions automatically execute on policies, blocking personally identifiable information from being transmitted, and encrypting classified material that otherwise might have moved through the system without adequate protection.

These solutions also help address privacy requirements for secure electronic communications mandated by SOX or HIPAA, often by verifying that sensitive regulated information is handled according to policy. And unlike other DLP methods that may slow application transmission or put a drag on databases, channel-specific DLP usually has minimal effect on data flow performance

\\\\ **BY FOCUSING ON E-MAIL AND WEB TRAFFIC,** CHANNEL-SPECIFIC TECHNOLOGY IS WELL-POSITIONED TO **TRACK ACTIVITY AND ENFORCE POLICY.**

THE NEED FOR PHYSICAL SECURITY

Most IT organizations focus on logical security, but physical security is just as crucial. For every news story broadcast about stealthy cyberattacks, there are an equal number of costly breaches caused by a person literally walking off with a piece of intellectual property or sensitive content. In April 2012, it came to light that two contractors for the California Department of Child Support Services had lost several disk cartridges containing files on 800,000 children and adults.

Without repercussions for noncompliance, staff members will not be motivated when it comes to safe handling of data. That's why it is crucial for the IT department to enact concrete policies for sensitive data handling and promote effective physical security practices.

These controls should specify that all sensitive data be backed up multiple times with at least one remote copy, and that the transport of any media containing classified information be made using a secure vehicle.

and can actually help expedite the delivery of authorized content.

Channel-specific solutions can go a long way toward stopping both accidental data exposure and calculated theft. The web-centric focus of most channel-specific DLP solutions also hinders data loss through wikis, blogs and other web postings that use Web 2.0 applications. FTP and e-mail–specific DLP technology can stop the surreptitious backdoor data transfers that are a common method of cybertheft.

Integrating DLP with Social Media

Social media represents a sweeping change for the IT department. As workers engage in communication across a host of sites, such as Twitter, Facebook and LinkedIn, the technology staff is often steps behind in understanding the potential effect on data security.

Social media is playing a growing role in the communications operations of many organizations. But there is continued concern that either through negligence or ill intent, staff will transmit embarrassing, sensitive or valuable information to external sites that can be accessed by anyone.

There is a clear role that channel-specific technology can play in helping the IT organization monitor social media. DLP solutions can help IT staff gain visibility into worker social media activities.

DLP solutions offer some tools for addressing concerns around unapproved social media activity. At the most basic level, organizations can simply block users from accessing specific social media sites. Though this can keep staff from posting content to these sites from their work computers, the IT staff will need to take more steps to ensure that data isn't posted from a staff-owned device.

This kind of blunt-force defense isn't practical for most organizations because it interferes with normal workflow and also lacks nuance or depth to cover any number of other scenarios in which a user might leak data. Also, as more organizations start to use Twitter and Facebook for promotion and public relations, blocking these sites isn't practical.

While some web-specific DLP products can alert IT staff or managers to possible data policy violations, the technology clearly has far to go with respect to both automation and a full set of features.

Anecdotally, the medium itself is often where organizations first learn a breach has occurred. For example, the IT staff may not realize that a file has been illegally copied from a server by an external agent until it is posted on a social networking site.

Social media will certainly continue to grow, both in use and in its effect on data security, as more organizations seek it out as a marketing and communications tool. Mindful of social media's reach, organizations need to find creative ways to leverage social media while keeping users secure.

This requires a proactive approach that starts with educating users on policies and enforcement. Users need to understand what kind of material is appropriate to post. The IT organization should be clear about possible enforcement actions, including prosecution.

Although channel-specific technology may seem more limited than enterprise DLP solutions, these products offer a well-targeted approach to DLP for smaller, under-resourced organizations and can be useful in prioritizing responses and limiting damage. Whichever method or combination of products an organization uses, the goal remains the same: Prevent data loss without disrupting workflow and impeding productivity.

The strengths and weaknesses of these methods vary by approach and by individual product. Winnowing down the number of options, an organization can find a solution that works well for both its security and its operational requirements.

However, choosing and even deploying DLP is only half the story. Perhaps most important to an effective DLP strategy is having well-defined data policies in place and the kind of ongoing communication necessary to ensure that they are executed properly. Only then can an organization be entirely confident it has the tools and practices in place to stay ahead of threats. ■

TACTICAL ADVICE

ACHIEVING PCI DSS COMPLIANCE

Gain a better understanding of PCI DSS and how it ties into DLP efforts:

CDWG.com/dlpguideta

STATETECH

Achieving PCI DSS Compliance

This glossary serves as a quick reference to some of the essential terms touched on in this guide. Please note that acronyms are commonly used in the IT field and that variations exist.

Glossary

Channel-specific DLP

These solutions monitor specific traffic channels such as HTTP, e-mail and FTP to ensure that classified and other sensitive information is handled according to policy. Some channel-specific DLP products can intervene if other appropriate controls aren't being applied.

Cloud computing

Cloud computing is an on-demand IT consumption model that, as defined by NIST, incorporates aspects of self-service, broad online accessibility, resource pooling, rapid elasticity and measured service.

Content-aware DLP

These systems rely on advanced techniques to find data within a particular system, device, data store, e-mail or other object to ensure that it is being handled according to policy. They capture data at rest or in motion and, using a form of file cracking, assess whether the data is sensitive in nature.

Content-neutral DLP

These solutions apply controls without regard for the particular data involved in a transaction. For example, a content-neutral solution can be used to block all downloads to USB drives to prevent accidental leakage or deliberate theft of sensitive materials.

Data classification

This process categorizes information based on its sensitivity and importance to the organization so that special controls can be instituted to secure the access to and the handling of that information. In many cases, the secure handling of such highly sensitive information is regulated by government or industry mandates.

Data discovery

This process scans databases, hard drives and other sources for confidential or sensitive data to find regulated or high-value information. The discovered data is then categorized based on whether any special security protections must be applied.

Data loss prevention (DLP)

DLP comprises a series of interlinked processes designed to minimize information theft, leakage and compromise. This is done by applying adequate controls to protect access to and the handling of data based on the value and sensitivity of the information. A comprehensive DLP strategy covers data discovery, information categorization, data consolidation, policy design and execution.

Database fingerprinting

Database fingerprinting uses a database or a live feed to look for exact matches to classified information that may have been cut, copied and pasted into a document.

Document fingerprinting

Document fingerprinting uses an algorithm to match files in transit that map to the tagged files flagged for special controls.

Document tagging

This process relies on information culled from databases or other data stores that hold sensitive documents, as specified by IT administrators. Document fingerprinting is one technique used to recognize tagged documents.

Encryption

Encryption is a process that relies on software using special algorithms to scramble data so that only those with the key to decrypt the content can see sensitive or confidential information.

Endpoint DLP

Endpoint DLP is technology that discovers, monitors, reports on and protects data at rest, in use or in motion.

File categorization

File categorization is a method for identifying high-value information that must be accessed or handled with special controls, as dictated by organizational policies. This discovery technique relies on an inventory of predefined rules and key words that outline sensitive or classified content.

Health Insurance Portability and Accountability Act (HIPAA)

Enacted in 1996, HIPAA outlines provisions (including administrative, physical and technical security controls) to ensure the protection and privacy of patient health information.

Identity and access management (IAM)

IAM is the security discipline that provides the authorization for sanctioned users to open and use protected information. Techniques used to protect access to information include passwords, tokens, biometrics and digital certificates.

Incident response plan

An incident response plan outlines the processes and procedures that need to be implemented in the event of a breach. These steps include details on who should be notified in the event that data is compromised, both general and specific project plan outlines, and a mechanism to account for losses related to a breach.

Intellectual property (IP)

IP refers to a set of distinctive inventions, discoveries, creative output and industrial designs that are given protected legal rights. These protections are governed through copyrights, trademarks, patents, trade secrets and industrial design rights.

Network-based DLP

This DLP solution scans traffic at network access points, examining web, e-mail and FTP applications; filtering inbound traffic; blocking malicious code and other suspicious inbound traffic; and scrutinizing outbound traffic for potential leaks or possibly compromised data.

Pattern matching

DLP systems use this technique to identify classified, sensitive or other high-value data by looking for common characteristics. For instance, 16-digit numbers that might be linked to a name, or a six-digit expiration date that might identify an item requiring security protections (such as encryption or user authentication) for access.

Payment Card Industry Data Security Standard (PCI DSS)

This industry standard defines specifications set by the Payment Card Industry Security Standards Council for the handling of cardholder information for major credit, debit and prepaid cards.

Personally identifiable information (PII)

This term refers to data that can be used alone or with other information to uniquely identify, locate or contact a single person.

Remote wipe

Sometimes referred to as a mobile kill switch, a remote wipe is a feature of mobile and portable devices that lets IT administrators disable the device and erase the content of its hard drive.

Rules-based analysis

This is a process used by content-aware DLP solutions to match data within a document that requires special protections. In this approach, a DLP system would refer to predefined rules for examining objects to identify sensitive information, such as the nine digits that represent a Social Security number.

Sarbanes–Oxley Act (SOX)

SOX is a federal law enacted in 2002 to outline controls that need to be applied to protect the integrity of financial data in publicly traded companies. Sarbanes–Oxley requires companies to secure access and apply specific protections to financial information.

Statistical analysis

This security approach is applied by content-aware DLP solutions using a combination of advanced mathematical techniques (including Bayesian analysis and machine learning) to identify sensitive content that requires special security controls.

WikiLeaks

An online source of leaked government and corporate documents, WikiLeaks is best known for the unauthorized release of redacted U.S. State Department diplomatic cables in 2010. These cables were published with a key that could decrypt the redacted sections.

Disclaimer

The terms and conditions of product sales are limited to those contained on CDW·G's website at CDWG.com. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given. For all products, services and offers, CDW·G® reserves the right to make adjustments due to changing market conditions, product/service discontinuation, manufacturer price changes, errors in advertisements and other extenuating circumstances. CDW®, CDW·G® and The Right Technology. Right Away.® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners. CDW and the Circle of Service logo are registered trademarks of CDW LLC. Intel Trademark Acknowledgement: Celeron, Celeron Inside, Centrino, Centrino Inside, Core Inside, Intel, Intel Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside Logo, Intel Viiv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Viiv Inside, vPro Inside, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. Intel's processor ratings are not a measure of system performance. For more information please see www.intel.com/go/rating. AMD Trademark Acknowledgement: AMD, the AMD Arrow, AMD Opteron, AMD Phenom, AMD Athlon, AMD Turion, AMD Sempron, AMD Geode, Cool 'n' Quiet and PowerNow! and combinations thereof are trademarks of Advanced Micro Devices, Inc. HP Smart Buy savings reflected in advertised price. Savings may vary based on channel and/or direct standard pricing. Available as open market purchases only. Call your CDW·G account manager for details. This document may not be reproduced or distributed for any reason. Federal law provides for severe and criminal penalties for the unauthorized reproduction and distribution of copyrighted materials. Criminal copyright infringement is investigated by the Federal Bureau of Investigation (FBI) and may constitute a felony with a maximum penalty of up to five (5) years in prison and/or a $250,000 fine. Title 17 U.S.C. Sections 501 and 506. This reference guide is designed to provide readers with information regarding data loss prevention. CDW·G makes no warranty as to the accuracy or completeness of the information contained in this reference guide nor specific application by readers in making decisions regarding data loss prevention strategy. Furthermore, CDW·G assumes no liability for compensatory, consequential or other damages arising out of or related to the use of this publication. The content contained in this publication represents the views of the authors and not necessarily those of the publisher.

Index

ABOUT THE CONTRIBUTOR

MATT JACH has been a Senior Security Engineer with CDW for the past twelve years. He currently leads an engineer team focused on conducting data loss prevention risk assessments for customers. He has also worked as an IT consultant in a variety of internal and customer-facing roles. His wide security experience includes conducting vulnerability assessments, assisting with various compliance and risk management initiatives, and developing strategies to safeguard critical data and infrastructure.

LOOK INSIDE FOR MORE INFORMATION ON:

- Conducting a risk-benefit analysis
- Strategies for securing data access
- Drafting data security policies
- Choosing the right network-, endpoint- or channel-specific solution