A FRESH LOOK AT DLP

Data leakage prevention systems get new respect thanks to technical advancements and new implementation best practices.

Keeping hackers outside digital boundaries is only half the battle IT managers face in securing their organizations. The other half — equally important — is to keep valuable information inside the organization, a difficult task given all the ways data can leak out in violation of security policies.

After all, many of today’s most sophisticated cyber thieves keep a low profile. They can, for example, breach organizational defenses by planting stealthy malware designed to find valuable data such as credit card numbers and quietly send it to an outside command and control server. Unfortunately, even trusted staff members sometimes put valuable data at risk by breaking internal policies and regulatory rules in the crush of daily operations. For example, a user preparing for a meeting may carelessly attach a confidential presentation to a group email distribution list.

Because of risks such as these, some IT managers are taking a closer look at data leakage prevention technology. (DLP, which also commonly used to refer to “data loss prevention.”) “DLP has been around for a little over 10 years, and now it’s mainstream,” says Linda Park, senior product marketing manager at Symantec.

Acceptance is growing as both the technology and the best practices for using it have matured. Early on, DLP had a reputation for being difficult to implement. “Some people were trying to watch so much data, DLP became unusable,” says Chris Morales, practice manager for architecture and infrastructure at NSS Labs, an independent information security research and advisory company. “The most successful implementations I saw just focused on compliance, which simplified everything.”

DLP veterans say a focused approach for choosing and using the technology can overcome early disappointments and keep organizations both secure and compliant.

DLP in Action

At the core of modern DLP solutions are sophisticated content identification technologies that accurately distinguish highly sensitive information from routine, unregulated data. “Sensitive content may be credit card and Social Security numbers, financial information or intellectual property,” says Rob Sadowski, director of technology solutions at RSA, the security division of EMC. “DLP finds where this data resides across the organization and monitors what people are doing with it, including whether someone is trying to send it outside the organization.”

Depending on how security managers configure a DLP system, the technology may send an alert of a potential policy violation to managers or proactively block a transmission.

DLP comes in multiple, complementary varieties, depending on where security managers decide to install the technology. Network-based DLP solutions monitor information transmitted over internal networks. This option can spot when sensitive information is about to leave an organization via email, instant message and upload to an FTP server. Endpoint DLP installs software agents on notebook computers or other end-user devices to monitor data streams. Mobile DLP looks at activity occurring on tablets and smartphones to ensure compliance and security. Discovery or storage system DLP scours data stores.
for confidential information throughout a data center and can help pinpoint specific data in response to a compliance audit or legal action. Because each of these variations homes in on different areas, large organizations may opt for a combination of DLP alternatives or choose a comprehensive solution that addresses all of these areas.

"Security regulations may not explicitly call out each of these channels as areas that need protection, but closely monitoring all of them is implied in the rules," Park says. "There are a multitude of ways that sensitive information can be disclosed, whether accidentally or intentionally."

### A Range of Choices

The latest version of Symantec Data Loss Prevention includes a new remediation portal through which managers can centrally review and remediate network file policy violations. An enhanced endpoint agent discovers data stored on the latest version of the Mac OS and monitors and prevents events on Microsoft Windows 8.1. It also monitors virtual desktops and applications hosted by Citrix XenApp, VMware View and Microsoft Hyper-V. "We've invested a lot of resources to achieve broad coverage of many types of communications channels, including web applications and proprietary protocols," Park says.

The Websense Data Security Suite combines modules for protecting information flows across networks and endpoints, along with a data discovery component. "With our solution, organizations can apply the same security and compliance policies for all of these areas," says Robert Slocum, product marketing manager for data security at Websense. "Using a consistent policy across the board makes it easier to demonstrate compliance to auditors."

The Websense suite includes optical character recognition (OCR) technology. "If someone in a hospital grabs a screen shot of a patient record and sends it to a doctor not affiliated with the organization, our OCR technology would recognize that as protected information and send an alert or block the transmission," says Bob Hansmann, director of product marketing at Websense. In RSA's Data Loss Prevention platform, a centralized console lets administrators manage modules for protecting data centers, networks and endpoints. To simplify compliance, the package comes with more than 170 standard policies covering a range of international rules.

It also includes a built-in incident-tracking workflow process that logs and monitors policy violations and maintains an audit trail of incidents.

McAfee Total Protection for DLP protects intellectual property and ensures compliance by safeguarding sensitive data on networks, in storage systems or on endpoint devices. It provides centralized management and reporting tools. A policy orchestration module makes it possible for multiple stakeholders throughout an organization to collaborate on incident workflow and case management without requiring IT involvement.

### 4 STEPS TO DLP SUCCESS

The right tools can promote security and compliance, but for full DLP success, organizations must implement and manage the technology effectively. Experts say these four steps can help.

1. **Identify your most critical information.** "It’s not realistic to say you’re going to protect all of your information," says Chris Morales of NSS Labs. "So begin with an assessment to understand what data really matters."

2. **Use predefined policy templates that come with many DLP solutions.** Also known as data identifiers, these resources jumpstart classification of standard data types, such as credit card numbers and protected health information. "Organizations can leverage these templates right out of the box to get DLP up and running quickly," says Linda Park of Symantec. "Then, as necessary, they can create custom profiles that look for information unique to the organization or its operations."

3. **Roll out DLP slowly.** Instead of a massive deployment, a better approach is to plan a series of small projects that introduce the technology to departments that handle critical information. Park recommends four roll-out phases: monitoring the flow of confidential data, remediating any problem areas that become exposed, notifying users when they violate policies and blocking information before it leaves the organization in violation of established policies. "By first gaining visibility into where critical data is stored and how people are using it, organizations can pinpoint and prioritize their highest risks," Park explains.

4. **Focus on enabling existing organizational activities, not restricting them in the name of security and compliance.** "The old joke used to be that IT security professionals are the ‘You can’t do that’ people," says Robert Slocum of Websense. Instead of adding to users' burdens, a successful DLP solution will enable security personnel to enforce the policies that are already in place, he adds.

To learn more about DLP, watch CDW’s webinar “Protecting a Valuable Asset: Your Data” at [CDW.com/DLPWebinar](http://CDW.com/DLPWebinar).