Develop a Successful Data Loss Prevention Strategy

Published: 31 January 2017 - Brian Reed

Summary

An enterprise strategy for DLP requires security and risk management leaders to identify sensitive data, build use cases for appropriate data handling, develop policies and workflows to address requirements, and integrate with other security technologies.

Overview

Key Challenges

- Organizations are at risk when data loss prevention (DLP) is deployed without guidance from business owners.
- Organizations failing to respond appropriately to sensitive data access events is the single most significant factor in DLP deployments failing to meet expectations.
- DLP product selection is meaningless without a well-defined data security strategy that accounts for the expected outcomes of data flows.

Recommendations

Security and risk management leaders overseeing application and data security:

- Work with appropriate business owners to drive a DLP strategy by applying well-defined requirements, and highlighting sensitive data types, data repositories, expected data flows, policies and workflow.
- Inventory existing security technologies that integrate with DLP products before engaging vendors by looking specifically at security information and event management (SIEM) technology, user and entity behavior analytics (UEBA), and cloud access security brokers (CASBs).
- Determine the appropriate DLP strategy for your organization's needs. Organizations looking to satisfy regulatory compliance should utilize outbound email DLP. Organizations with intellectual property requirements should utilize endpoint DLP.
- Mandate that DLP investments include budget and resources for handling events and administration of the DLP system. DLP managed services could be an attractive option for resource-constrained organizations.

Strategic Planning Assumptions

By 2022, 60% of organizations will involve line-of-business owners when crafting their DLP strategy, up from 15% today.

By 2022, 20% of organizations with integrated DLP will have a well-defined data security governance program in place, up from near zero today.

Introduction

DLP allows the dynamic application of a data handling policy based on the active inspection of content. This includes information contained within an object such as a file, email, packet, application or data store, while at rest (in storage), in use (during an operation) or in transit (across a network). It is also the ability to dynamically apply a remediation policy, such as log, report, classify, relocate, tag, redact, encrypt and/or apply enterprise digital rights management (EDRM).

Used by security and risk management leaders to its full capability, DLP is a nontransparent control, which means it is intentionally visible to the end user with the primary value proposition of changing user behavior. This is very different from transparent controls like firewalls and intrusion detection systems, the operations of which are often unseen by end users.

Nontransparent controls represent a cultural shift for many organizations and present many challenges to success in the implementation of DLP controls.

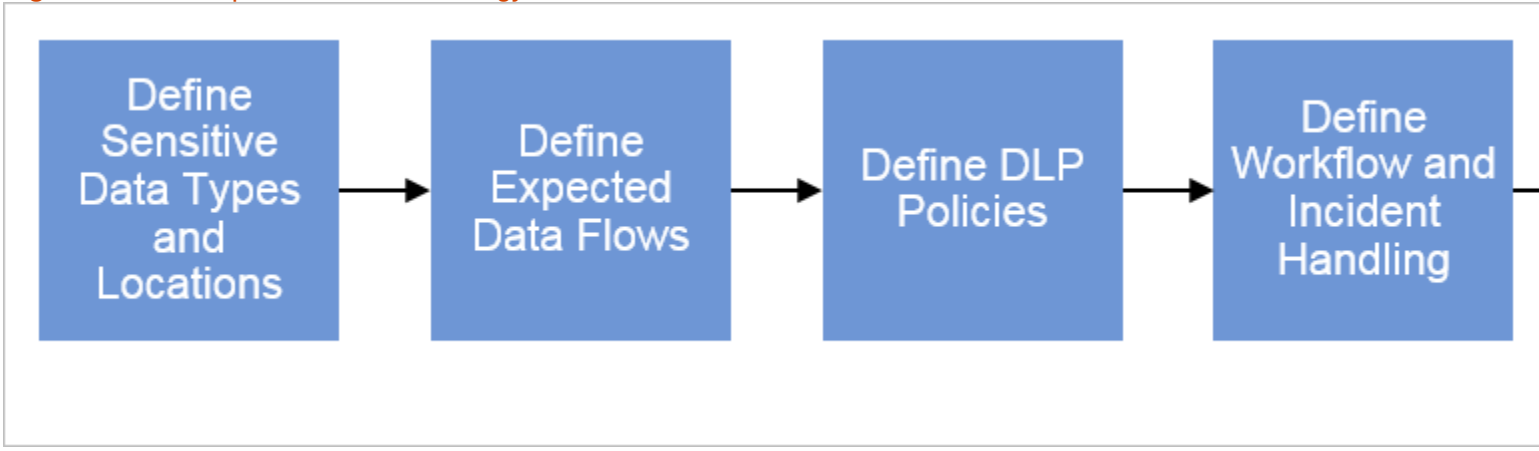
DLP is available as stand-alone products, although DLP capabilities can also be found in a wide variety of other products, as noted in "How to Choose Between Enterprise DLP and Integrated DLP Approaches."There is a danger of adopting ad hoc, siloed implementations that will be difficult to monitor, manage and maintain. Integrated DLP is not just a "checkbox" capability. Events generated by stand-alone and integrated DLP solutions have to be correlated, seen in context, and worked through validation and resolution. DLP starts with a well-defined process that is only *supported* by technology. This process must be articulated fully in order to realize any gains that DLP products or features may provide.

Analysis

Follow a Five-Step DLP Product Strategy for Your Organization

Regardless of whether your organization pursues an enterprise DLP or integrated DLP approach, the five-step process depicted in Figure 1 should be employed.

Figure 1. Five-Step DLP Product Strategy Process



Source: Gartner (January 2017)

By following the five-step DLP strategy process introduced above, security and risk management leaders can generate the necessary thinking within their organizations to be successful with implementations beyond just getting the technology to function. They should then approach DLP vendors with a set of independently developed, organization-specific requirements.

Step No. 1: Define Sensitive Data Types and Locations

All organizations should start with a good sensitive data definition, because this will help identify gaps in coverage of the planned implementation. It will also influence the requirements for content-detection mechanisms. Security and risk management leaders should also identify and collaborate with data owners to form an understanding as to where appropriate authorized locations exist for sensitive data.

Data stored in authorized storage locations might include:

- File servers or shared drives that are properly defined for use by specific users or groups
- Cloud storage repositories that are managed by IT and integrate with IAM systems
- Source code management systems
- Enterprise content management systems

Data stored in unauthorized storage locations might include:

- Workstations with unauthorized client data in unapproved files or directory locations
- Storage area networks with files containing credit card data in clean areas deemed out of scope for Payment Card Industry (PCI) compliance
- Databases with Social Security numbers, Social Insurance numbers and other similar data types in a comment field

Each vendor has its own interface to describe sensitive data, and its own set of mechanisms for detecting sensitive data. By defining your sensitive data requirements before the organization contacts vendors, you will ensure that your organization's needs — and not the vendor's offerings — are driving the selection process.

Step No. 2: Define Expected Data Flows

Once your organization has defined sensitive data types and has agreed on appropriate locations for sensitive data, you can begin to define expected data flows and what to do if data flows violate expectations. Some examples of useful data flow definitions may include the following:

- Data leaving the organization:
    - Blocking PII or employee data leaving the network over email (including personal email), unless the message body and all attachments are encrypted
    - Alerting and blocking any instances of file transfers where sensitive data is detected
    - Blocking the emailing of source code to recipients outside of the organization or to those without appropriate access privileges
- Sensitive data in use on a computer:
    - Disabling the transfer of sensitive data to removable media, such as a personal USB storage device or mobile device with mass storage enabled
    - Disabling the printing of unauthorized sensitive data
    - Copying sensitive data into unauthorized applications
    - Posting sensitive data to a company social media site, but not to unmanaged social media sites
    - Transferring sensitive data through web-based email not managed by the organization
    - Placing sensitive data on unsanctioned or unapproved cloud storage platforms

Step No. 3: Define DLP Policies

If you look for sensitive data, you will find it. Unfortunately, so will malicious insiders. Failing to appropriately respond to sensitive data detection events is the single most significant factor in DLP deployments failing to deliver value, because one of the primary value propositions is changing user behavior. Also, realize that many sensitive data detection events can't be effectively addressed through technology alone, and may have business or cultural ramifications on the organization. Security and risk management leaders should ensure that the company is prepared for the impact of effective sensitive data detection.

Some examples of policy actions that can be taken when sensitive data is discovered might include:

- Alert a DLP administrator that an action has occurred.
- Create an audit record to mark a data handling incident for later review.
- Encrypt a message automatically and send it on to its destination.
- Display a self-remediation box to a user for confirming an action or providing a business justification or override passphrase to allow business-approved actions.
- Quarantine a message for review by a DLP administrator or approved reviewer before release.
- Apply EDRM controls to a file.
- Move a file found in storage to a secure location, leaving a marker or breadcrumb behind for the owner with instructions to securely retrieve the data.

Most successful DLP deployments start with a well-defined scope of users and systems, and in monitoring mode with blocking or alerting set for only a handful of obviously wrong activities. In order to yield a set of policies that work with normal business flow, you should expect to implement policies iteratively, as no amount of planning will get this 100% right.

Step No. 4: Define Workflow and Incident Handling

Fundamentally, DLP is a capability to facilitate behavior change through visibility into unsecured business processes and poor data security practices. As such, the establishment of workflow to manage and address incidents is a critical part of success. Security and risk management leaders should determine how incidents will be managed to closure, including who they will be sent to, how they will be escalated, if exceptions are possible and how decisions will be made regarding resolution.

Alerts regarding the presence of sensitive data also create a data propagation issue, because data is replicated in alerts and passed to various people through the workflow chain. Security and risk management leaders must decide who should have access to view the actual contents of alerts, and control access with delegated administration functions available in all DLP products. Privileged access management is a crucial element of DLP incident workflow.

Step No. 5: Integrate With Additional Security Technologies

While DLP is not a silver bullet to secure data, it does possess the content awareness that many technologies lack. Security and risk management leaders should evaluate ways in which they can integrate DLP resources with other existing security technologies within their organizations:

- If the organization uses SIEM technology or a managed SIEM service, security and risk management leaders should determine if there are event handlers and connectors to use DLP to serve as an additional point of event correlation.

- UEBA is another emerging technology that can serve as a strong analytical complement to DLP. UEBA factors in user activity, application usage, network access, location awareness and a number of additional contextual points to provide added value to DLP events. These products can use advanced analytics and machine learning capabilities to find and highlight DLP events of real interest. UEBA can analyze DLP events to help provide a better determination as to who the riskiest users are with access to specific sensitive data.
- CASB is another area where DLP integration has proven to be valuable. Many CASBs have their own data security policies and integrated DLP engines, and many also integrate with network DLP gateways via ICAP. Clients typically use the CASBs' DLP for an initial inspection of a cloud application session; however, depending on the user or data type, you could configure handoff via ICAP to a network DLP instance for further investigation. There are drawbacks and limitations to ICAP, and these could cause latency, network redundancies and a poor user experience.

Use Sample Policies, Reports and Templates Carefully

Security and risk management leaders should confirm vendor claims regarding the reliability and accuracy of vendor-supplied DLP policies, reports and templates. Verify each of these claims against your own sensitive data definition to ensure that a particular template will detect what you need to address for your DLP requirements.

Be sure to cover all representative departments or divisions in your organizations, as success with one department's data does not guarantee success with another one's.

Perform live testing with actual data in a controlled time frame of two to four weeks against your production environment. A common cause of debilitating false positives is the presence of data patterns in applications, and certain stored data formats that match sensitive data definitions.

When defining detection requirements for sensitive data, ensure that there are unique patterns that differentiate sensitive data of interest from all other data that is not of interest. If you cannot conceive of a pattern to differentiate data of interest from all other data — whether that pattern is text, nontext or a data attribute — you may not be able to use content-aware DLP to solve your problem.

Ensure Your DLP Strategy Corresponds to Business Requirements

The reasons your organization is looking at DLP must relate back to tangible business requirements. Typically, the three business requirement drivers for DLP are some combination of measuring regulatory compliance, protecting intellectual property, or obtaining greater visibility and control over the movement of data.

It is critical that data owners are involved with any DLP project, both initially and on an ongoing basis. It is also incumbent upon the data owners to be accountable for the ownership of their own data, just as it is equally important for information security to provide options for how to achieve success securing data. It is not the job of information security to determine the appropriate level of data security; instead, it must offer options and alternatives to the data owners, and educate them on the administrative capabilities of DLP technologies. Any DLP strategy requires the sponsorship and buy-in of relevant management within the organization.

Include System Administration and Event Handling in DLP Costs

Far too often, organizations only look at the capital expenditure of security technology and do not factor in the operational expenses of new technologies. DLP requires not only a clear strategy and solid implementation, but also ongoing administration to ensure proper handling of generated events. Without operationalizing a DLP system, DLP is simply an event generator.

Security and risk management leaders and DLP administrators must remain vigilant and proactive to ensure that generated events are indeed valid. If events are valid, they must be worked completely to resolution; if events are invalid, DLP policies might need to be tested and altered accordingly. Administration of any DLP system requires a well-defined and logical change control process, as well as an administrative workflow with clear steps and decision trees that help administrators quickly and accurately resolve DLP events when they occur. DLP system administration will require ongoing budget, resources and effort.

Resource-constrained organizations might also investigate using a managed service provider for their DLP system. Managed services might also be appropriate in the initial phases of a DLP deployment or in the short term in order to help lessen the knowledge gap and bring internal administrators up to speed on a new DLP system.

DLP managed services cannot decide which data is sensitive. This requires data definitions from your own organization. Without this cooperation, DLP managed services will ultimately fail. You cannot outsource responsibility for DLP; you can only outsource system management and some event handling. Organizations will need to invest in the time and resources to work with any DLP managed service provider in order to get optimal value from this approach.

Ref.: https://www.gartner.com/doc/reprints?id=1-3WPYERL&ct=170330&st=sg