Table of Contents

Objective ................................................................. 3
Background ................................................................. 3
McAfee Solution Services Methodology ................................ 3
The Data Security Program ............................................... 4
Strategize: Discovery and Risk Assessment ............................ 4
Plan: Data Classification and Policy Architecture .................. 5
Design, Implement, Operate, and Optimize: DLP Solution Integration .................................................. 8
Summary ........................................................................ 12
About McAfee, Inc ......................................................... 12
Best Practices Guide

Objective

All companies risk the loss of sensitive data as confidential or proprietary information escapes through unauthorized channels. Data losses translate to billions in dollar losses every year, in the form of damaged brand equity, fines for regulatory violations, and opportunity costs resulting from stolen intellectual property. Given the high stakes involved, enterprises must implement strong and well-designed safeguards for sensitive data.

This guide provides a road map for creating an effective enterprise data loss prevention (DLP) program. It outlines the necessary steps for managing data usage, from initial risk assessment and planning, to data classification and policy architecture, to deployment and maintenance of automated loss prevention tools. The guide incorporates proven best practices to deliver not only a comprehensive technical solution, but also a best-of-breed enterprise data loss prevention model.

Background

Protecting sensitive information from unauthorized disclosure has become a major concern for companies worldwide. High-profile cases have highlighted the critical need to protect core assets, intellectual property, and sensitive data. Regulatory and legislative requirements such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), International Traffic in Arms Regulations (ITAR), Payment Card Industry Data Security Standard (PCI DSS), and SB1386 are other major drivers for deploying data loss prevention solutions.

Typical data theft security systems provide fair protection against external threats by using perimeter defenses such as firewalls and intrusion detection or prevention. However, these systems are not designed to prevent internal information theft. Additional security measures that protect internal information tend to limit data access only to authorized personnel—but though such legitimate access does not entitle the user to remove that data from the enterprise, existing solutions do not adequately protect against this risk.

DLP solutions work in this space, safeguarding data where other security solutions have proven ineffective. McAfee® Solution Services and McAfee SecurityAlliance™ expand the classic security approach with a program focused on DLP. By transferring their knowledge in this document, these teams aim to guide organizations to scope a proper DLP solution in advance, execute plans smoothly, and maintain momentum as needs evolve.

McAfee Solution Services Methodology

A complete life cycle for DLP incorporates best practices, operational improvements, and appropriate application of tools. Reflecting real-world business pressures, the program considers comprehensive data protection within the context of maximizing return on investment.
The McAfee Solution Services Methodology for DLP aligns these factors in a six-step life cycle that can be adapted to fit the needs of most enterprises.

1. **Strategize: Discovery and risk assessment.** Identify business requirements or problems to solve with strategic objectives and program elements. Establish priorities and scope.

2. **Plan: Data classification and policy architecture.** Translate objectives into specific DLP solution requirements that meet business and security priorities. Optimize data classification processes, such as definition and refinement of data classes, and data handling policies at the organizational level. Select an appropriate DLP solution.

3. **Design: Build the DLP solution for the target environment.** Design the implementation roadmap by addressing high-priority risks first. Accurately scope and scale the program, then procure hardware, DLP software, storage, and databases.

4. **Implement: Install, configure, and deploy the DLP solution.** Pilot initial components, and then expand policies and coverage in a well-paced rollout.

5. **Operate: Establish a structure for DLP administrators to monitor and react to DLP activity.** An initial monitoring phase leads to an enhancement phase where policies are refined.

6. **Optimize: Streamline and enhance DLP processes.** Refine policies and reaction rules to reduce false positives and noise.

**The Data Security Program**

Effective defenses against data loss require a strong data security program with three distinct components:

1. Discovery and risk assessment

2. Data classification and policy architecture

3. DLP solution integration

**Strategize: Discovery and Risk Assessment**

The first phase of the data security program is to create program strategy and define program goals. This process normally entails formal discovery and risk assessment to identify and prioritize process and control gaps. The strategy phase establishes implementation details and goals to close these gaps. It establishes a dollar value that quantifies the risk of data loss. Here we define program scope and set expectations for implementation and product selection. Time invested in this phase will save time and expense during deployment, increasing the likelihood of success.

Understanding the level of risk an organization faces must come first. This process discovers existing threats, then characterizes and quantifies risk exposure relative to data losses that each threat might enable. Since the process involves cross-functional participation and detailed analysis, this phase usually takes a few weeks for smaller businesses and up to several months for more complex regulated entities. Given the breadth of expertise required, many organizations tap experts in data loss risk assessment.

McAfee offers a data loss identification service that uses several techniques to assess risk:

**Internal assessment**—This approach includes a broad assessment of internal data security controls (such as database access) to identify sources of data leaks that might indicate insecure internal processes. Our team reviews public sources and the corporate Intranet to investigate if sensitive information is improperly made available. Also conducted is a data-centric audit of the access controls and processes around information flows within the organization.

**Assumed role assessment**—This process looks conceptually at users in the organization to highlight potential areas of risk. It views data from multiple user
perspectives and considers different departments that handle sensitive data, such as finance, human resources (HR), sales, and executive management.

Typical roles include:

- Regular user
- Process/system administrator
- Technical expert

For example, roles, responsibilities, and access controls could be analyzed for an enterprise resource planning (ERP) system administrator. If the administrator is able to access privileged financial information, the risk is that the administrator could send this non-public information to a third party to execute illegal stock trades. During the implementation of a DLP solution, this analysis can be reused to define policies to prevent such unauthorized data flows (such as via email).

**Technical assessment**—A major part of any data security assessment is the identification of both process gaps and technical deficiencies. A technical assessment involves a security penetration test in which vulnerabilities, misconfigurations, and weak technical security standards are identified. For completeness, tests should consider coverage of network, application, and physical channels, and cover loss avenues ranging from portable and mobile devices to network elements. McAfee Foundstone® Consulting Services and Foundstone vulnerability assessment tools are beneficial here.

**Risk assessment**—The final phase of data loss identification brings together the internal, assumed role, and technical assessments into a dollar value summary of organizational risk. Standard industry cost data and a validated cost assessment are applied to predict and quantify the impact of data loss. If a company has a leak involving intellectual property, for example, the assessment would associate a dollar value to a product line that might be jeopardized. By attaching a dollar value to each risk, the team can easily prioritize the requirements for a DLP solution. The summary of all data loss values provides a comprehensive monetary risk estimate that not only can reveal risk exposure but also justify investments and motivate participation by business units in the data security program.

Because of these assessments, an organization should be able to recognize its problems, prioritize the losses it needs to prevent, and confidently characterize the elements that are necessary for a robust DLP program. Thoughtful consideration in this phase will ensure clear, reasonable expectations for people, processes, and the DLP solution.

**Plan: Data Classification and Policy Architecture**

Accurate data classifications and useful policies form the core of an effective data security program. McAfee consultants have found that the process is best implemented when this phase is broken into several steps:

- Establish data sensitivity classifications by identifying the necessary classification levels and associated definitions
- Document data flows to create a catalog of the types and sources of data that will use the labels; consider the application sources, locations, and content types
- Apply labels to the data and enforce the data classification program with a strong DLP solution

**Data classification**

Data classification starts with the definition of sensitivity criteria. Use a multi-level scale, graduating from freely available public tiers to highly private protected tiers, adjusting the granularity and scope of this scale to meet organizational needs. While establishing data classification criteria is beyond the scope of this paper, most organizations find this five-point scale to be a good starting point:

<table>
<thead>
<tr>
<th>Classification Level</th>
<th>Data Description (Scope)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected</td>
<td>Information that cannot be shared and must be secured at all costs.</td>
</tr>
<tr>
<td>Restricted</td>
<td>Information that is shared only between selected members.</td>
</tr>
<tr>
<td>Confidential</td>
<td>Information that is available to authorized personnel and partners under a non-disclosure agreement (NDA) at the organizational level.</td>
</tr>
<tr>
<td>Internal</td>
<td>Information that is available only within the organization.</td>
</tr>
<tr>
<td>Public</td>
<td>Information that is freely available to all.</td>
</tr>
</tbody>
</table>

**Documentation of data flows**

The next step maps out organizational data flows to pinpoint types of data in use and to ensure there are no gaps in the analysis. Since data is primarily used by and flows among three organizational entities, three overlapping views are used for classification:

- Organizational units
- Applications
- End users and clients
Depending on the strategy developed in the previous phase, and the degree of classification required, an organization might choose to implement one or more of the three classification views. The more views used, the stronger the classification scheme and the more complete the coverage of data types.

**Organizational units-based data classification**
To classify data at the organizational level, document the various divisions and entities within the enterprise and then expand this list to identify external organizations, such as partners, vendors, and even competitors. This list serves as a starting point for the flow of information within an enterprise. For example, one could start by identifying information flows between the HR and accounting departments:

1. Payroll information
2. HR departmental budgeting information
3. Pension and benefits plan information

Once identified, these information flows can be classified. In this example, the data sensitivity levels outlined earlier are applied:

- **Payroll information** should be restricted to selected organizational members within the payroll department: *Restricted*
- **HR departmental budgeting information** is confidential at the organizational level (e.g., this information may flow only between human resources and accounting): *Confidential*
- **Pension and benefits plan information (brochureware)** should be available to all internal organizational members: *Internal*

**Application-based data classification**
To classify data based on applications, build a comprehensive list of software, applications, and programs used by the organization. Using this list, identify both the data flows and the data sources for each application. For example, the client-facing personal banker at a financial institution may use an application with the following data flows and sources:

- **Data source**—Client personal information, such as credit card and account numbers or home addresses; information provided by the client
- **Data flow (out)**—Back-end relational database (storing client information)
- **Data source**—Customer opinion survey information
- **Data flow (out)**—Third-party survey company

Once the data sources and flows have been identified, classify the data sources:

- **Client personal information** should be restricted to selected organizational members (e.g., personal bankers whom the client works with): *Restricted*
- **Customer opinion survey information** is confidential and should only be shared with authorized partners (in this instance, the third-party survey company): *Confidential*

The data flows are attended to in the policy architecture sub-phase detailed shortly.

**End user- and client-based data classification**
Classification based on end users and clients is the most difficult aspect of any program. Within an enterprise, the end user and client group consists of the largest collection of data sources and flows. A good approach to classifying this domain is to begin with the enterprise’s pre-existing structure: the organizational chart. This top-down approach moves from the head of the organization down the chart, identifying the data access points for each individual.

For example, in assessing the vice president of engineering (IT) role, sensitive data access points might include:

- **Source code**
- **Business project plans**
- **Customer support database access**

After identifying the data points, they are classified:

- **Source code** must be restricted to appropriate entities within the development organization: *Restricted*
- **Business project plans** are confidential and must only be available to relevant partners and organizational entities: *Confidential*
- **Support database access** includes product defect information and sensitive customer information such as account status, systems in use, and contact phone numbers: *Confidential*
As we move through the organizational chart, analysis expands to and iterates through other members of the engineering organization:

- Senior managers
- Research staff
- Software developers
- Quality assurance analysts
- Consultants
- Administrative staff
- Customers
- Interns

This process is tedious and often lengthy, but experience shows a systematic and thorough approach creates a strong data classification program requiring less rework over time.

**Data security policy architecture**

After defining the appropriate classification labels, the organization must find its sensitive data and apply its classifications. The policy architecture sub-phase thoroughly catalogs the storage locations of data and labels any sensitive data with its relevant policy. Here the relationship among the environment (content, locations, and applications), the data, and the respective data security policies are defined to guide data usage.

To identify information sources, the analysis team comprehensively documents the data flows identified in the data classification sub-phase.

Information is stored in four different databases: SER1765, SER1766, SER1853, and SER1854 (see Figure 1). (The web self-service application uses one of the same servers as the HR system.) This information must be properly labeled with its sensitivity classification stamp:

- Labeling can occur in many ways. The goal of the label is two-fold. First, it is often a legal requirement for many sensitive data types. Second, it educates viewers and users to help them comply with policies. One labeling technique would be to publish a banner at the application layer (OSI Layer 7) to all connecting programs that outlines the nature of the HR data as determined by the data classification process. Alternatively, the label could be placed in the template for an application, so that any data created by that application is automatically labeled.

- In addition to ensuring consistent application of labels, enforcement of labeled data based on source application, storage location, and content is an important part of data security. McAfee Data Loss Prevention (McAfee DLP) is a powerful enforcement mechanism that ensures data classification rules are observed throughout the enterprise. Classification rules are immediately enforced as per the DLP policy on, for example, new items created by an application or stored on a named file share.

- Security best practices demand appropriate role-based access control for all users. Automated DLP solutions like McAfee DLP go beyond these basics to provide host- and network-level control, including dynamic, proactive monitoring, and enforcement based on the data’s specific usage policy. A range of risky user activities can be controlled, including copy and paste across applications; storage to portable devices, CD-ROMs, and DVDs; email, web mail or web posting; and printing.

The hypothetical scenario below shows the results of the overall process, from risk assessment to data classification to policy architecture:

- **Risk assessment**—There are four databases to protect: SER1765, SER1766, SER1853, and SER1854. Should data from these systems exit the company through unauthorized channels, significant financial losses could result. Loss of HR data could result in legal charges, while loss of accounting data could result in a multitude of financial concerns such as:
A decrease in market capitalization due to the perception of inadequate organizational controls
- Estimated at 2 percent of the enterprise market capitalization

Loss of confidential project information to competitors through budget information
- Estimated at $40 million in lost revenue opportunities

Divulgence of confidential operational procedures through financial records
- Estimated at $30 million in lost competitive advantages

Total losses, including legal costs, for this hypothetical scenario and company are estimated to be $150 to $170 million.

Data classification—A typical data security policy will define this data with the following classification:

- Payroll information should be restricted to selected organizational members within the HR and payroll departments: Restricted

- Accounting information should be restricted to selected organizational members within accounting and directly associated departments: Restricted

Policy architecture—Here, the data is labeled with the classifications developed above. For payroll information, the HR application accessing this data could label the data by publishing a banner at login to inform the user of the data classification as follows:

“Confidential. This data should be treated as company confidential. Personally identifiable information, including employee addresses and Social Security numbers, must be limited to members of the HR and payroll departments”

Design, Implement, Operate, and Optimize: DLP Solution Integration

After defining procedures and controls in the strategy and planning phases, a data security program must move forward with measures to ensure these processes are adhered to and enforced throughout the organization. Traditionally, organizations have worried about preventing unauthorized access by outsiders. Security products such as firewalls, intrusion prevention systems, and host-based anti-virus have all been part of a defense-in-depth security approach aimed at the external threat.

These are important tools, but they do little to defend against accidental or deliberate data misuse by authorized insiders, such as the inappropriate transfer of confidential data via email, USB drive, or posting on the web. In this space, DLP solutions play an important role in enforcing a company’s data security policy. The following case study focuses on the design and implementation of DLP security measures using McAfee DLP.

Getting started

The deployment process often begins with a pilot at a department or group level that starts with the most easily defined data classification and policy controls. Alternatively, some organizations create a test network with a representative user community and policy (derived from the planning phase). These approaches can be used in combination or iteratively to scale up protection to more of the enterprise.

Many organizations monitor activities for weeks or months to understand data usage. Evidence and metrics on data use and policy violations usually streamline decision-making for governance committees. Enforcement (such as blocking unauthorized activity) may be implemented as part of the pilot phase or it may be part of a subsequent iteration of the enterprise rollout.

A typical DLP deployment follows this sequence:

- Design and implement
  1. Pilot: set up
     Identify a pilot group and install and configure DLP software.
  2. Pilot: policy
     Establish an initial DLP policy using a subset of elements from the enterprise data security policy.
3. Validate: monitor

Monitor the deployment for areas where reaction rules should be refined.

4. Enterprise rollout: set up

Scale and expand the implementation by moving to production the DLP server and rolling out the DLP agents throughout the enterprise.

5. Enterprise deployment: enterprise policy

Build and deploy the DLP policies by iterating thoroughly through the enterprise data security policy.

- Operate and optimize

6. Enhance: monitor

Monitor the deployment for patterns in violations, trend lines, and opportunities for improvement.

7. Enhance: refine and verify

Refine policies based on identified opportunities and verify system and policy rollout.

8. Iterate

Monitor and repeat Step 6 throughout the process life cycle.

Design and implement

Pilot: set up

The McAfee DLP Installation Guide covers in full detail the deployment steps to be used in both set-up phases (pilot and enterprise rollout). The best practice guidelines to follow during this crucial design phase are outlined below:

- McAfee DLP server and clients should be segregated in a test network
- The test network should have its own Active Directory forest or domain (users and groups can be reused from existing Active Directory deployments, but a separate network helps avoid user disruption)
- The test sample set should represent a full spectrum of users. Diversity ensures accurate policy construction and validation
- Client sample size should range between 10 to 50 hosts; a size that is large enough to provide adequate information for the monitor phase but also small enough to remain manageable at this early stage in the deployment
- Administration suggestions:
  - Domain administrator or equivalent rights are useful to have handy as they facilitate troubleshooting and allow easy joins and removals of clients to and from the domain
  - Local administrator rights are required on each client to install the McAfee DLP agent. It is best to install the agent as a domain user who is a local administrator on the client system. The local administrator rights can later be revoked

Time frame: one to four weeks

Pilot: policy

The initial rule set creates the DLP solution’s translation of the enterprise’s data security policy, with its organization-specific data classification components. For example, if an enterprise’s data security policy limits the use of USB devices, this restriction could be implemented using McAfee DLP. To illustrate this process, consider a component of a hypothetical data security policy:

**Section 2.3: Client Information**

Client information is considered “Confidential” data. This data includes, but is not restricted to, credit card numbers, account information, and client personal data. This information is to be held in the strictest confidence, shared only on a need-to-know basis, and must not be transferred outside the organization. This information may not be duplicated, copied, or transferred by any means, electronic, mechanical or other, without the express written consent of Information Security.

Typically, client data is located in secure data warehouses and is accessed by specific end-user applications. This sensitive information also follows specific formats such as those implemented in credit card and Social Security numbers. These formats make it easier to define policies to monitor usage.
To implement controls for the above policy, the following rules might be set using McAfee DLP:

- **Tagging rules**
  - Content-based: Any content following certain credit card or Social Security numerical formats is tagged
  - Application-based: Any content resulting from certain end-user database access applications is tagged

- **Reaction rules**
  - USB: Block all USB devices except those authorized by Information Security
  - Email: Block tagged content from being transferred to an external email domain
  - Network: Block tagged content from being transferred on protocols like FTP

Here are some guidelines to follow in this pilot phase:

- Identify the most common and most important data security breach points within the organization
- Identify the easiest data security breach points to protect against, such as:
  - USB devices that are not the corporate standard or store data without encryption
  - Inappropriate (data loss/leak related) emails being sent to external domains
- Implement the reaction rules in monitor mode to avoid user disruption. Once the rules have been sufficiently fine-tuned, blocking functionality can be enabled.
- Work with five to 10 rules in this phase of the deployment, expanding the rule set further in Step 4 above
- It is best to concentrate on labeling rules, known in McAfee DLP as tagging rules, rather than over-engineering reaction rules in this initial, learning phase. After monitoring user behavior and easing the product into the environment, the reaction rule set can be expanded and tuned

**Validate: monitor**

This phase watches the pilot group and the policies deployed to ensure functionality and feasibility. For example, the pilot rule set is monitored to ensure the implemented policies are generating expected results.

The technical aspects of the deployment, such as attaching the policy to specific groups and collecting evidence, can also be fine-tuned as needed. If particular tagging or reaction rules are not triggered over an extended period, consider revisiting the technical implementation or refining the rule for accuracy. Additionally, organizations may wish to enable additional Reaction Rules during this phase, after monitoring activity and determining remediation measures.

**Time frame: two to eight weeks**

**Enterprise deployment: rollout**

After monitoring the pilot and refining the deployment, an enterprise agent rollout begins. Depending on the size of the organization, the deployment pace may vary. The table below outlines a sample schedule:

<table>
<thead>
<tr>
<th>Week #</th>
<th>Total Nodes Deployed (TND)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>10–50</td>
</tr>
<tr>
<td>4</td>
<td>250</td>
</tr>
<tr>
<td>6</td>
<td>500</td>
</tr>
<tr>
<td>8</td>
<td>2,000</td>
</tr>
<tr>
<td>10</td>
<td>10,000</td>
</tr>
<tr>
<td>12</td>
<td>25,000</td>
</tr>
<tr>
<td>13</td>
<td>50,000</td>
</tr>
<tr>
<td>14</td>
<td>75,000</td>
</tr>
<tr>
<td>N</td>
<td>TNDN-1 + 25,000</td>
</tr>
</tbody>
</table>

Some areas of consideration for the rollout include:

- Build a deployment group schedule, preferably mapped to Active Directory containers. For example, during Week 2, the IT department will be the focus, followed by finance in Week 4
- Determine which group to deploy to first by balancing urgency with complexity—allowing simplicity (the least complex) to prevail, even if it results in delaying an “urgent” group. This prioritization helps ensure a smooth rollout. Glitches can be fixed without disrupting critical systems. For example: A bank’s capital markets group has a regulatory need to deploy a DLP solution, but since this is a complex task, a rollout here would happen only after a few simpler deployments (in back-office groups like
IT and finance) have been completed. Once a few such deployment groups have been covered and the lessons learned have built confidence, the frontline capital markets group can be the next focus. Because this wait would be approximately two to four weeks, the delay would be acceptable in most circumstances.

- Avoid creating a new policy for a new group. Use the policy validated in the previous phase to limit complexity and to ensure a focus on the agent rollout. The enterprise policies will be further developed in the next phase, once the agent rollout is complete.

- Monitor McAfee DLP events to ensure policies are functioning as expected. Also, build a sustainable process to regularly monitor events and identify anomalies.

- Educate users on the product and the processes built around it. Make sure that the user community is familiar with the process to obtain an agent bypass (a release code that allows a one-time data transfer) and the consequences for breaching data security policy. As part of this education, the product can be deployed in a “monitor and notify” mode for a short period to assist in building this knowledgebase among the user communities. Users are often unaware of data classification and data security procedures; building this knowledge can be stronger than any technical security measure.

- Administration suggestions:

  - Monitor the McAfee DLP Server performance, namely the Microsoft® SQL Server, to ensure optimal performance. Server RAM may need to be adjusted to meet Microsoft SQL Server requirements.

  - The Event Collector Service (McAfee DLP Server) can be set up in a distributed manner to assist in supporting multiple sites and locations. Each Event Collector Service can point to a centralized Microsoft SQL Server to allow for centralized data management. Bandwidth and network topology must be assessed prior to establishing such a distributed architecture.

  - For every 25,000 nodes, one full-time employee is needed to monitor events, to investigate anomalies, and for administrative activities.

Time frame: one to six months

**Enterprise deployment: enterprise policy**

After rolling out the DLP product, the enterprise policy becomes the focus. As in Step 2, the data security policy translates into tangible security controls for the McAfee DLP solution. Here we iterate through the corporate data security policy and implement DLP-specific controls. However, the translation at this stage is much broader than that of Step 2. To illustrate this, consider another example of a hypothetical data security policy:

**Section 3.1: Protected Data**

All data classified as “Protected” shall remain the sole property of the company unless otherwise authorized by Information Security. All Protected content is prohibited from being transmitted, copied, or otherwise duplicated by any means, electronic, mechanical or other.

In a typical data security policy we would find several such guidelines. In this phase, we iterate through each such instance, rather than a subset as done in Step 2 (pilot: policy). Controls for this example might look like these:

- **Tagging rules**
  - Content-based: Any content with “Protected” disclaimers in the file is automatically tagged.
  - Location-based: Any content from a particular location (XYZ file share) is tagged.

- **Reaction rules**
  - USB: Block all USB devices except those authorized by Information Security.
  - Email: Block tagged content from being transferred to an external email domain.
  - Network: Block tagged content from being transferred on protocols like FTP.

Each section of a corporate data security policy is reviewed with an eye for policy enforcement using DLP. Once several components of the data security policy have been transformed into McAfee DLP rules, policy deployment begins.

Any new policy should be deployed first to the pilot group outlined in Step 1. Once deployed to this group, monitor user activity and events to ensure expected results. After this monitoring phase, the policy can be rolled out in a
controlled manner throughout the enterprise. The rollout schedule can follow that of the agent rollout in Step 4, although timelines are usually shortened. In addition, an enterprise may choose to deploy different policies to different user communities depending on corporate need. Such segmentation is part of this phase. The key to this process is iteration—implementing more components of the data security policy into McAfee DLP rules and following the prescribed rollout schedule. This iteration continues until the entire data security policy has been translated into rules for the McAfee DLP solution. Lastly, all rules deployed in this phase, as done in earlier phases, are deployed in monitor mode.

Time frame: one to four months

Operate and optimize

The last phases of a McAfee DLP deployment are to maintain project momentum and quality. DLP policies are regularly monitored and verified to ensure an accurate match with the company’s data security program. This monitoring and verification continuously iterates throughout the life cycle of a McAfee DLP implementation. The enterprise constantly refines its DLP policies in these phases as part of a sound data security program.

In these phases, monitor the deployment for patterns and opportunities to tighten up the DLP policies. The following example illustrates the types of enhancements that might be made:

- Enhance: monitor

  There is a content-based rule set for Social Security numbers that identifies nine-digit numbers and blocks email transfers of any such content. Monitoring DLP event patterns reveals an unexpected number of false positives: legitimate nine-digit inventory numbers are tripping the rules. If true positives (genuine leaks) are compared to false positives, it becomes clear that genuine leaks also included a customer’s first and last name.

- Enhance: refine and verify

  This insight would allow refinement of the policy by adding an additional filter in the content-based tagging rule. The Social Security number rule is expanded to include a nine-digit number plus a customer’s first and last name. Monitoring would then resume verifying that the change reduces the false positives.

- Iterate

  A new opportunity would be identified and analyzed. Thus far, all DLP reaction rules have been implemented in monitor mode to allow for a seamless and low-risk process. Once the rules have been sufficiently fine tuned, blocking functionality can be implemented with DLP on a rule-by-rule basis.

Summary

A strong DLP program brings together a well-planned approach such as the McAfee Solution Services Methodology described in this paper. In this approach, we move through a six-step life cycle, building a solid foundation for the program during the strategy and planning phases. Following this, we expand the program by integrating a powerful DLP solution to enforce the corporate data security policy. Among the most crucial program components, McAfee’s DLP solution empowers an organization to control its data, educate its users, and proactively secure its intellectual property.

Proceeding through the life cycle, this paper builds a robust implementation methodology for McAfee DLP. Using the Solution Services Methodology, the DLP solution is designed, implemented, operated, and optimized. Enriched with real-world examples and technical insights, this guide offers a roadmap through the DLP implementation process, from initial scoping to optimization steps, using techniques proven by McAfee experts to assist organizations in achieving a strong data security posture.

About McAfee, Inc.

McAfee, Inc., the leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world. With its unmatched security expertise and commitment to innovation, McAfee empowers businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security.