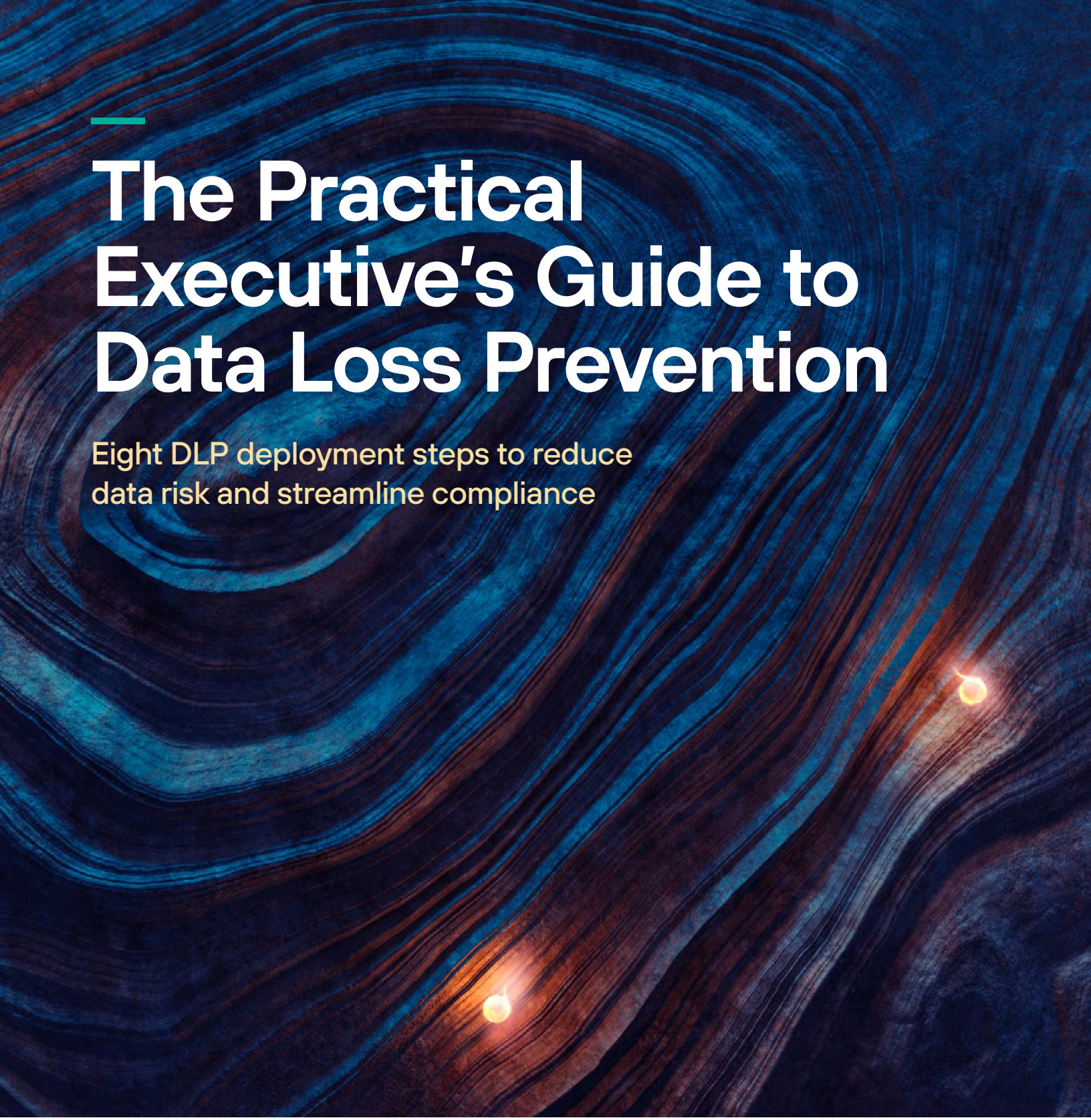


The Practical Executive's Guide to Data Loss Prevention

Eight DLP deployment steps to reduce data risk and streamline compliance

Forcepoint

Whitepaper

Table of Contents

It shouldn't come as a surprise that traditional approaches to cybersecurity are inadequate for confronting today's threat landscape. After all, the concept of the workplace itself has undergone a radical transformation, and employees now expect to be able to access business-critical company resources from anywhere.

How do you maintain control of your sensitive data when users work on unsecured Wi-Fi networks or open documents on unmanaged personal devices? What can you do to keep employees from sharing proprietary or protected information with generative AI tools for use in training Large Language Models (LLMs)? How can you guarantee ongoing compliance with increasingly stringent and fragmented regulations governing data use and privacy?

Meeting these modern challenges requires the assistance of a Data Loss Prevention (DLP) solution to ensure that sensitive data stays within your organization and to block the many vectors along which data can be exfiltrated to unauthorized parties.

This guide will walk you through the process of deploying a DLP solution, whether you're implementing DLP for the first time, switching to a new vendor or migrating an on-prem service to the cloud. It focuses on placing DLP at the heart of your data security strategy and generating measurable outcomes with which to evaluate program success. Doing so will help you to prevent data breaches, streamline compliance and control security on all channels from a single management point.

Here are the eight steps to DLP deployment that we will follow:

1. Identify Goals and Use Cases
2. Create an Implementation Plan
3. Define DLP Policies and Incident Workflows
4. Deploy DLP for Monitoring
5. Move to Active Enforcement
6. Evaluate, Refine, Repeat
7. Extend Protection to Other Channels
8. Add Enhanced Capabilities

Data Security Strategy Fundamentals

Keeping your organization's data safe requires you to ask – and be able to answer – five key questions:

- → **What** is your sensitive data?
- → **Where** is your sensitive data?
- → **Who** can access your sensitive data?
- → **How** do they use your sensitive data?
- → **Why** can they access your sensitive data?

Your data security strategy should be based on the Principle of Least Privilege (PoLP), which states that users should only be able to access the information that they need to perform their jobs. Making this principle a reality requires understanding what types of data you have and where they reside.

We use four terms to denote the state of data within an organization. These are:

- → **Data-in-Motion** (traveling across the network)
- → **Data-in-Use** (being used at the endpoint)
- → **Data-at-Rest** (sitting idle in storage)
- → **Data-in-the-Cloud** (in use, in motion, at rest)

Data discovery and classification are necessary in order to locate all this data and understand how to describe it. If your organization already has one or more solutions in place to perform these activities, this can serve as a firm foundation for Data Loss Prevention. But this is also a step that you can take once you already have DLP deployed and protecting your sensitive data.

Don't listen to DLP vendors who tell you that you have to start with Data-at-Rest before extending DLP activities to other data types. A sound security strategy calls for taking quick action in response to immediate challenges while establishing a roadmap for the future. Let your organization's priorities dictate the starting point for your deployment. In this guide, we'll take the approach of getting DLP up and running, with an emphasis on a quick transition to active protection, before moving on to extend complete coverage and add enhanced capabilities. Following all steps will help you to achieve a mature data security posture that is efficient to maintain and easy to continuously improve.

Ensure that you have chosen the best DLP solution before beginning your deployment. If you need help deciding on a vendor, consult our Buyers Guide to DLP.

Step 1: Identify Goals and Use Cases

Your first order of business should be to agree on what you hope to achieve with your DLP deployment and what you will primarily use it for. A good place to start is by drawing up an information risk profile for your organization. This can include:

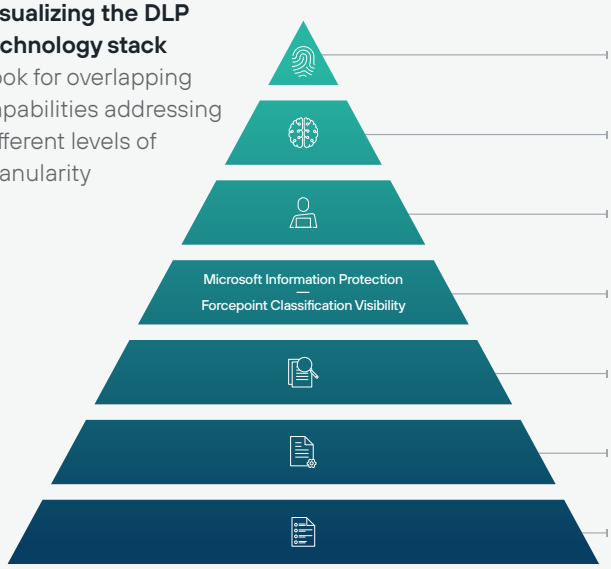
- → A statement of the potential consequences of inaction
- → A description of the types of data in scope (e.g., PII, IP, financial data)
- → Definitions of the network, endpoint and cloud channels where information can be lost or stolen
- → A list of existing security controls currently used for data protection (e.g., encryption)

Once you have this context, you can start listing your core use cases and goals, deciding on the key features of the deployment that will allow you to construct a detailed implementation plan. Here's what that conversation might look like:

- → Identify your core use cases
  - e.g., Securing critical IP, stopping data breaches, compliance
- → Derive short- and long-term goals
  - What business goals are driving the initiative?
    - Is it a compliance deadline?
    - Is it an expansion of remote or hybrid working?
  - What are the key dates?
- → Understand your security posture
  - Where will DLP fit into your security stack?
- → Identify your critical channels
  - Where do you want to start your deployment?

At the end of this step, you should have a broad outline in place of what your deployment should look like and how long it should take. Next, it's time to start filling in the specifics of what you want your implementation to look like.

Visualizing the DLP technology stack
Look for overlapping capabilities addressing different levels of granularity



PreciseID Fingerprinting
Structured and unstructured data, can ingest directly from databases, documents, spreadsheets, etc. and provides high confidence detection for even small subsets of data leaving an organization

AI Classification
Applies cloud-based AI model, trained by LLM synthetic data and domain-specific GenAI with ML training

NLP Scripts
300+ predefined available in various languages. Intelligent data type detection based on described content with contextual helpers for accuracy

Classification & Visibility
Meta-Data (Files, Emails, etc), Supports and file labelling and classification tool that writes metadata tags to files.

File-Types
Over 900 file types detected based ontrue file type to identify all file types regardless of if they are renamed to avoid detection

Regular Expressions
Perl based regular expressions to provide wide, deep and accurate detection of content

Keyword Phrases
Over 1,000 pre-defined regulatory and compliance keyword, phrase and dictionary-based detection

The capabilities of your chosen DLP solution may not exactly match these, but it will apply a variety of techniques—true file-type detection, regular expressions, NLP scripts, fingerprinting and sifting through data. Make sure to compare lists of capabilities when deciding on a DLP solution.

Figure 1: DLP detection capabilities

Step 2: Create an Implementation Plan

Developing an implementation plan for your deployment starts with identifying the roles played in the project by different teams. Your list of key players and their functions might like something like this:

CORE TEAM	SKILLS REQUIRED
Project Manager / Business Analysts / Risk and Compliance Officers	Requirements gathering, documentation skills, conceptual knowledge of data protection
Architects / Senior Engineers	Familiar with local and global network structure, data flow and operational management
Network / Security / System Engineers	Install, configure, maintain solution and its components
Data Security SME	Rule construction, use cases, data element identification, policy tuning, etc.
Incident Investigators	Privacy and risk obligations related to investigations related to data exfiltration
Incident Handlers	Security event response and alerting
Data Security Event Escalation	Monitoring and ad-hoc escalation

Figure 2: Key team members and skills for your implementation plan

Once you've determined who is responsible for what, you can work out how the different phases of the deployment map onto your given timeframe. Use a format like this to clearly mark when you expect tasks to be completed, and refer back frequently to this project timeline to ensure that work is proceeding at the expected pace. Be prepared to revisit the timeline if the deployment process becomes blocked at any point.

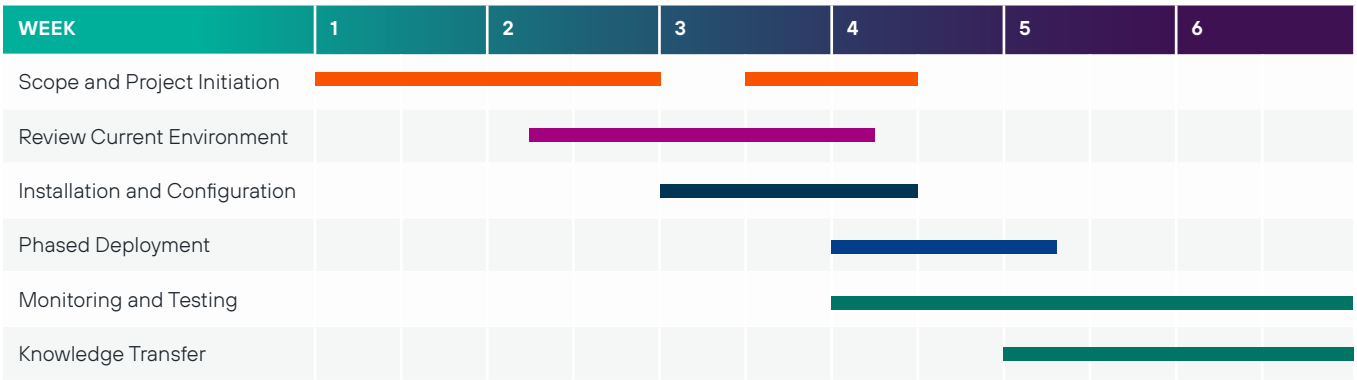


Figure 3: DLP deployment timeline

You should base your timeline on your assessment of your available resources and project needs. Each deployment will call for a different amount of time, but we have supported successful DLP SaaS deployments in as few as six weeks.

Step 3: Define DLP Policies and Incident Workflows

Once the project management fundamentals of your deployment are set up, it's time to figure out what exact policies your DLP solution will enforce. These determinations will be based upon your estimation of what impact there will be to your organization in the event that different types of data are lost, stolen or compromised.

Start with a simple whiteboarding exercise. Have your DLP implementation team meet with data owners and partners to determine the level of impact in the event that data is lost, stolen or compromised. You can describe impact using qualitative analysis, such as listing incident types along a scale of 1 to 5. This helps to prioritize incident response efforts and is used to determine the appropriate response time.

CHANNELS	LEVEL 1 LOW	LEVEL 2 LOW-MEDIUM	LEVEL 3 MEDIUM	LEVEL 4 MEDIUM-HIGH	LEVEL 5 HIGH	NOTES
Web	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	Proxy to Block
Secure Web	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	SSL Inspection
Email	Encrypt	Drop Email Attachments	Quarantine	Quarantine	Block	Encryption
FTP	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	Proxy to Block
Network Printer	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	Install DLP Printer Agent
Cloud Applications	Audit	Audit / Notify	Quarantine with Note	Quarantine	Block	TBD
Custom	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	TBD

Figure 4: DLP policy examples

You should also work up an incident workflow plan to determine the course of events that are triggered by a given security incident. For low-severity incidents, apply automation whenever possible; this typically includes notifying users and managers of risky behavior. It may also include employee coaching to facilitate self-remediation of risk. Higher-impact incidents require intervention from an incident analyst, who will investigate and determine the type of threat (e.g., accidental, intentional or malicious). The incident analyst forwards the incident and their analysis to the program manager – typically the head of security or compliance – who then determines what actions to take and which teams to include.

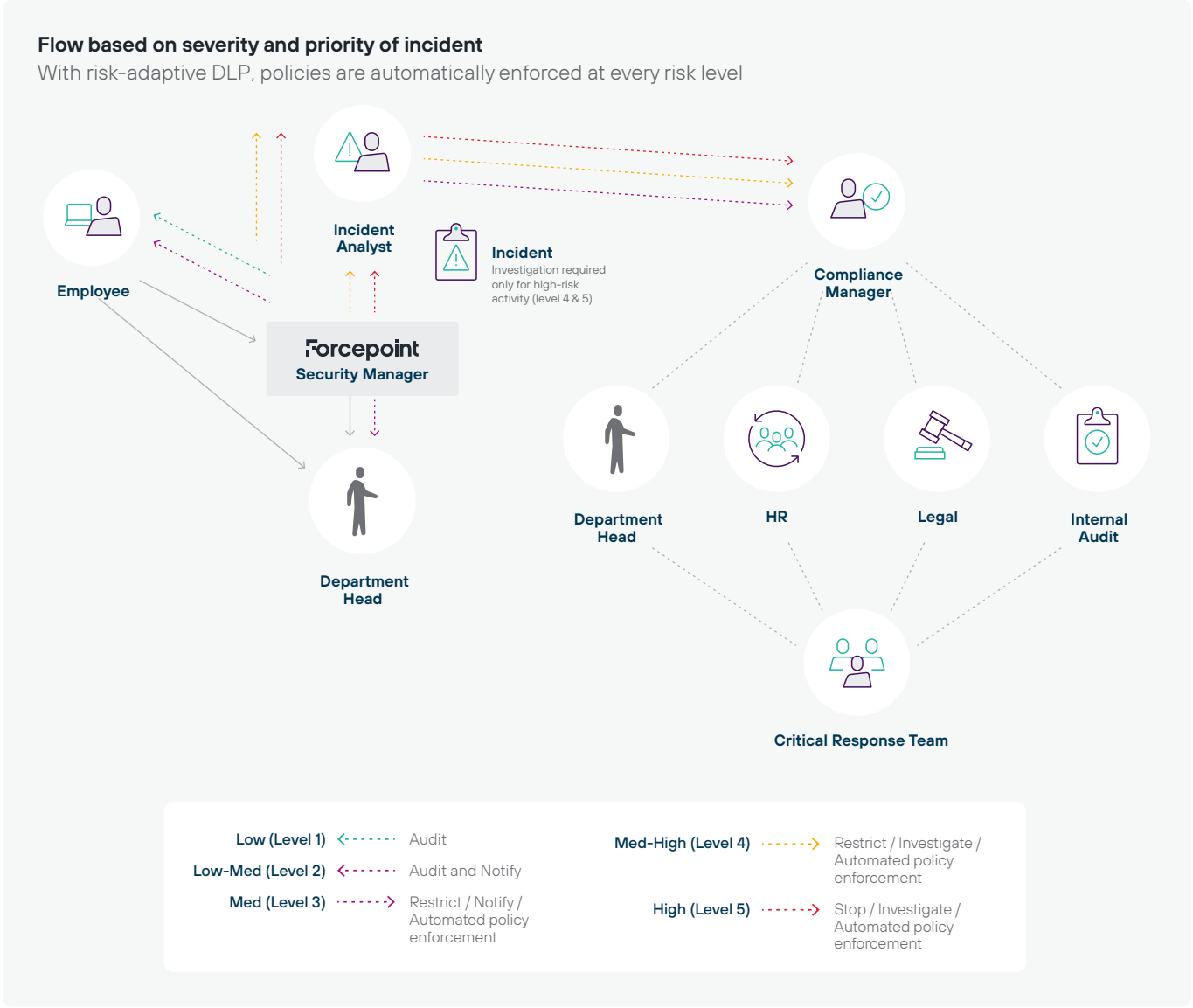


Figure 5: DLP incident workflow

Once you have these documents, you can use them as the basis for DLP policies to be entered during the next phase: DLP deployment.

Step 4: Deploy DLP for Monitoring

Now comes the actual deployment of your Data Loss Prevention solution. Before it is actively applied, DLP should be run passively so that you understand the effects of your policies in case policy inaccuracies cause excessive blocking of otherwise safe activities. As you gain more insight into data movement and usage within your organization, you can adjust the controls to apply enforcement for higher-risk users or incidents.

If you've planned properly and achieved buy-in from the proper stakeholders, deploying your DLP solution should go smoothly. A typical deployment should follow this workflow relatively closely, and you can use it to confirm that you don't leave out any important steps.

Installation

- → Lean on vendor technical support to ensure success
- → Perform connectivity testing on test users prior to rollout

Configuration

- → Set up policies, workflows and metrics
- → Stress-test using sample data from live customer traffic
- → Prioritize and resolve gaps with known workaround
- → Conduct technical User Acceptance Testing (UAT)

Cut over production traffic in phases

- → Perform after hours
- → Roll out by channel or region
- → Monitor for the next week to confirm the live environment is performing

Fine-tune and refine

- → Minimize unintentional incidents by adding exceptions or exclusions
- → Create different policy levels and custom reports based on use case needs
- → Create notifications and alerts for incidents and system health

This process will see you deploy a network DLP control, conduct an analysis and present key findings to the executive team. This should include recommendations for risk mitigation activities that can reduce the rate of occurrence of data at risk. Then capture the results and report them to the executive team.

Proceeding in phases is the best approach, although you may decide to structure your rollout in varying ways. You may start with a specific channel (e.g., endpoint), or proceed organizationally (by department) or geographically (by country or by region within larger countries); you may alternatively use a combination of these approaches. Proceeding by region allows you to take advantage of after-hours time slots for each phase of the deployment, minimizing disruption to your operations.

At this stage, the role of the DLP control is primarily to monitor, blocking only high-severity incidents (e.g., data being uploaded to known malicious destinations or a mass upload of unprotected records at risk in a single transaction).

Step 5: Move to Active Enforcement

Once you have finished fine-tuning your DLP policies and adding exceptions as needed, you are ready to shift to actively blocking threats.

Start with a gradual rollout of active blocking. You should prioritize the most critical data transfers and gradually expand to other areas in order to minimize the impact on business operations.

Continuously monitor the effectiveness of active blocking. Review blocked incidents and adjust policies as needed to ensure that legitimate activities are not hindered.

Once you have achieved active blocking of actions that violate your DLP policies, you should set up automation to speed up response times and simultaneously reduce the burden on admins to review incidents. Your DLP solution should allow you to automate policy enforcement, but you can go farther with capabilities to dynamically adjust enforcement to match user behavior.

A solution like Forcepoint Risk-Adaptive Protection enables a fully automated approach, providing a behavioral risk score for each user and tailoring security to the individual based on this scoring, which is adjusted dynamically based on the user's behavior over time. Tight integration with Forcepoint DLP allows the solution to adjust permissions according to risk score, reducing false positives and providing prioritized alerts. This triage system saves admins time and allows them to target real threats, simultaneously optimizing users' ability to get work done.

Actions that represent low risk are permitted while higher-risk activities generate automated responses that range from alerts to administrators or end users and coaching to encryption and complete blocking. This creates as little business friction as possible by stopping dangerous activity without impeding regular users and systems with overzealous blocking.

Calculating dynamic risk scores

This demonstrates how the system assigns a risk score between 0 and 100 based on different user actions

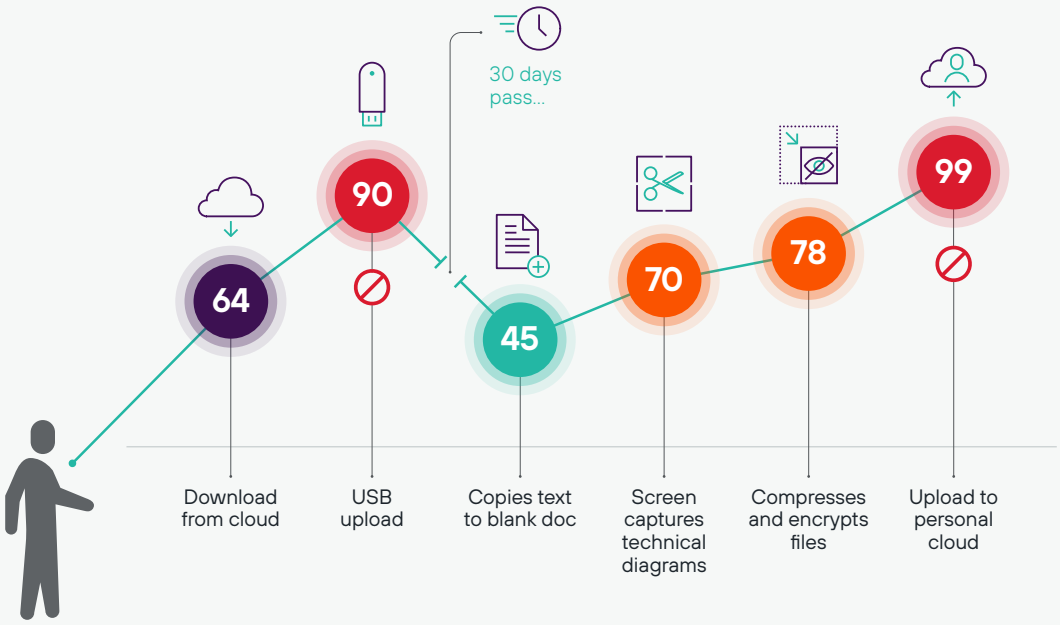


Figure 6: Example risk scores of activities across different channels

Step 6: Evaluate, Refine, Repeat

Now that your deployment is complete, you should take care to quantify the impact of DLP on your business operations in order to measure return on investment. You can derive this evidence from your incident tracking and create reports showing to what degree risks have decreased following your deployment and transition to active blocking. Here are a few tips to promote accurate and actionable results:

- **Group relative incidents together.** Common groups include severity, channel, data type and regulation. For larger organizations, additional sub-groups help to further clarify the risk according to geographic locations or subsidiaries.
- **Maintain consistency between risk-reduction phases.** To preserve the integrity of your results, the monitoring and risk-reduction periods need to be of equal length. In the beginning, we recommend two weeks to improve time-to-value and to simplify analysis. However, you are in the best position to determine what is most reasonable for your organization.
- **Distinguish automated from human response.** If using Risk-Adaptive Protection, you should provide a comparison of the incidents captured in audit-only mode (all incidents) versus incidents requiring investigation with graduated enforcement. The summary should show the number of incidents for each risk level 1-5, contrasted against those actually requiring investigation (risk levels 4-5).

Schedule cyclical reviews moving forward in which you continue to analyze this data, ensuring that risk levels remain low and taking time to fine-tune DLP policies if a gap is identified.

Finally, training employees is a critical ongoing component of your DLP operations. There are many ways to approach employee education, but some key places to start include:

- Setting up table-top exercises to demonstrate risk levels and mitigation options
- Providing training for administration and operations team
- Creating relevant online Knowledge Bases (KBs)
- Conducting awareness and product training for various stakeholders

Success requires an iterative approach to security that always seeks to improve and refine existing processes. No matter how strong your security posture is, there is something you can do to make it better.

Reducing the Likelihood of Data Loss Over Time

Set goals and measure the effectiveness of risk reduction over specific channels for 60 days, 90 days and beyond

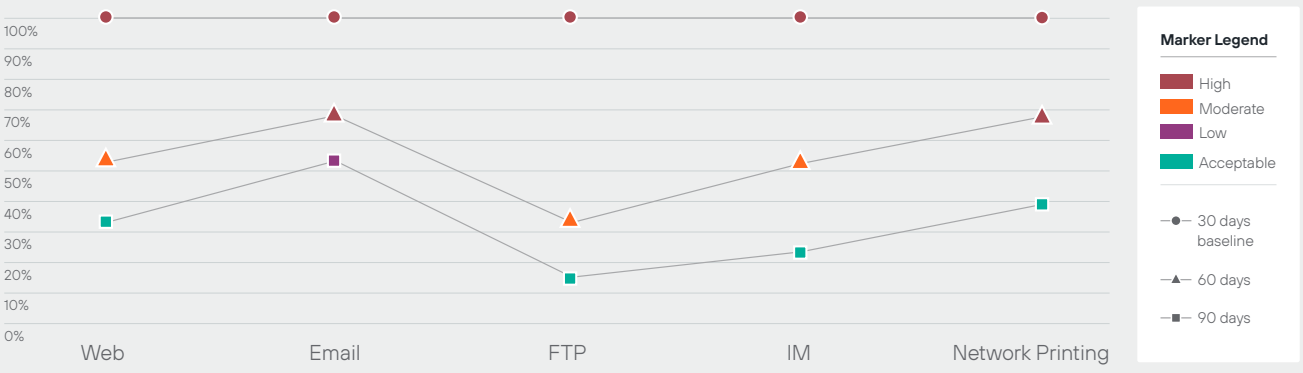


Figure 7: Incident tracking to measure risk reduction

Step 7: Extend Protection to Other Channels

Complete the organization-wide deployment of DLP capabilities by extending coverage to any remaining data types (e.g. Data-in-Use and Data-at-Rest) and channels (e.g., web, email, cloud SaaS apps and endpoints). You may have started with cloud by securing a few key apps, and now comes the opportunity to extend coverage to the rest.

Regardless of where you start, you should be able to use your existing DLP policies from one channel for enforcement over all other channels. This functionality is key to rapidly applying comprehensive protection to all your organization's ways of transmitting data. You can replicate your existing policies for the sake of speed and subsequently fine-tune if you find that different channels require different policies for any reason.

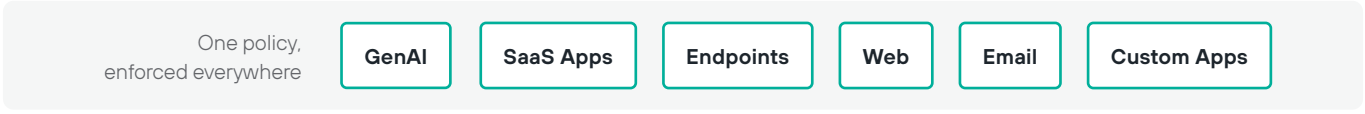


Figure 8: DLP policy enforcement across multiple channels

Applying security coverage to all channels can be conveniently handled through the adoption of tools for individual channels such as a Cloud Access Security Broker (CASB) and Secure Web Gateway (SWG); it can also be used to provide security for email transfers.

Once your DLP solution is actively and automatically enforcing policies across all data channels, the main portion of your deployment is complete. You should expect to maintain continual policy optimization in the future, especially as you incorporate more apps, physical locations, data types and so on into your organization. Consider further capabilities that will enhance the efficacy and accuracy of your data security program while lowering your exposure to data risk.

Step 8: Add Enhanced Capabilities

Powering up your data discovery and classification processes establishes a firm foundation for your ongoing DLP activities. By getting a clear handle on what your sensitive data is and where it resides, you can ensure that the correct policies are being enforced throughout the lifecycle of your data.

The best way to achieve this proactive approach is through the capabilities of a Data Security Posture Management (DSPM) solution. This can significantly enhance the effectiveness of your DLP solution by accurately discovering and classifying data, reducing false positives to free up admins to focus on remediating incidents, audits and workflow orchestration. DSPM reduces data risk by minimizing ROT ("redundant, trivial, outdated") data and ensuring data sovereignty. It checks whether files are over permissioned (e.g., sensitive documents accessible allowing public access) in order to enforce the Principle of Least Privilege (PoLP).

A DSPM solution should be able to generate reports to demonstrate compliance with regional and industry-specific regulations, speeding up the audit process. It can also provide a centralized view of your data across cloud and network storage locations, making it easy to implement and enforce data governance policies.

Implementing DSPM provides a firm foundation for your DLP activities, proactively establishing an environment in which DLP can do the most good and require the least intervention from admins. DLP can only be as good as its understanding of the data; the better your data classification and your overall data security posture, the more accurate your DLP will become.

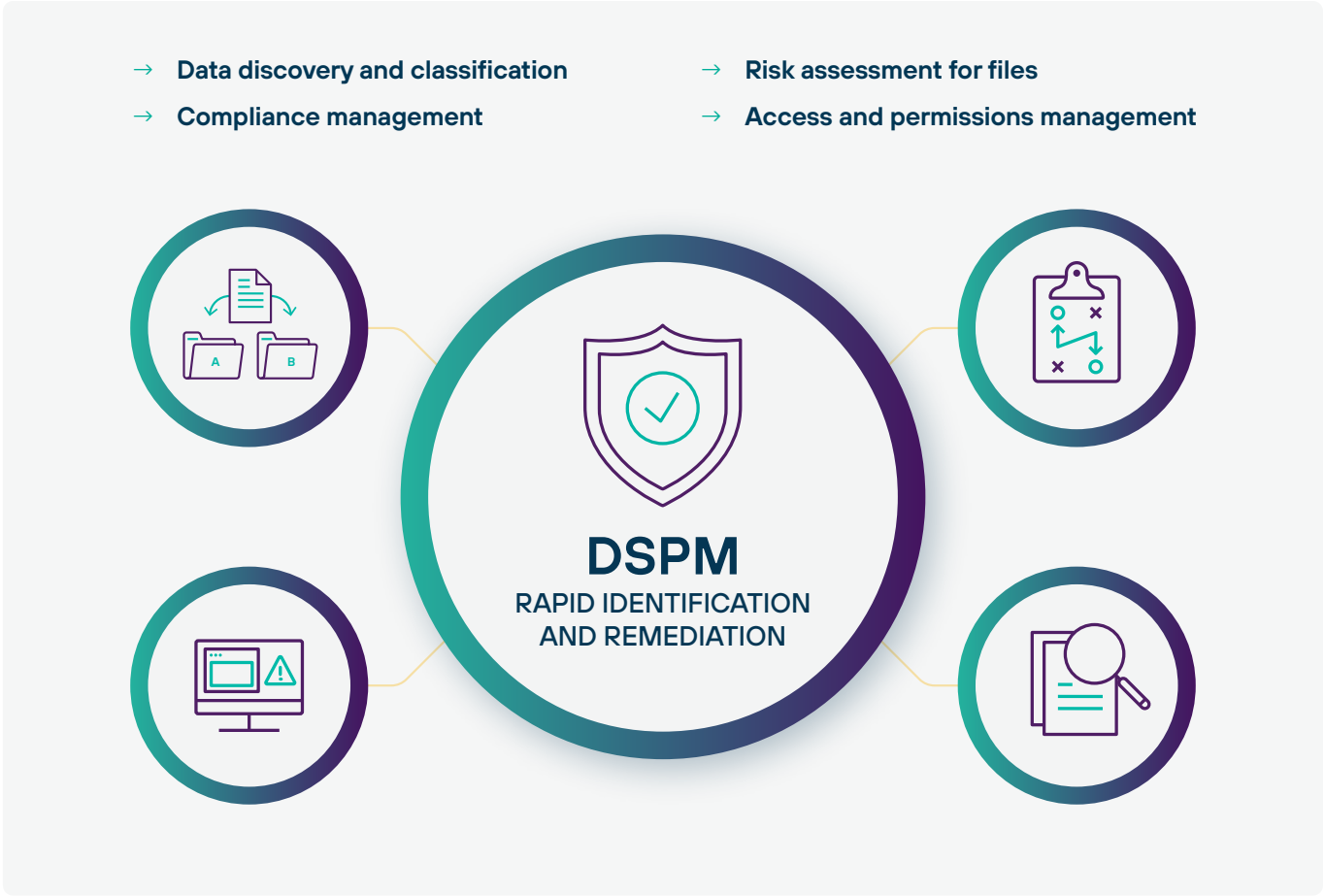


Figure 9: The core functionalities of DSPM

Conclusion: Protect Data Throughout Its Lifecycle

Risk to your data is risk to your business; taking a lifecycle approach to your data minimizes risk in both areas. This calls for you to continuously address all stages through which data passes, combining proactive and reactive processes to achieve total protection and unified visibility and control. We call this approach "Data Security Everywhere."

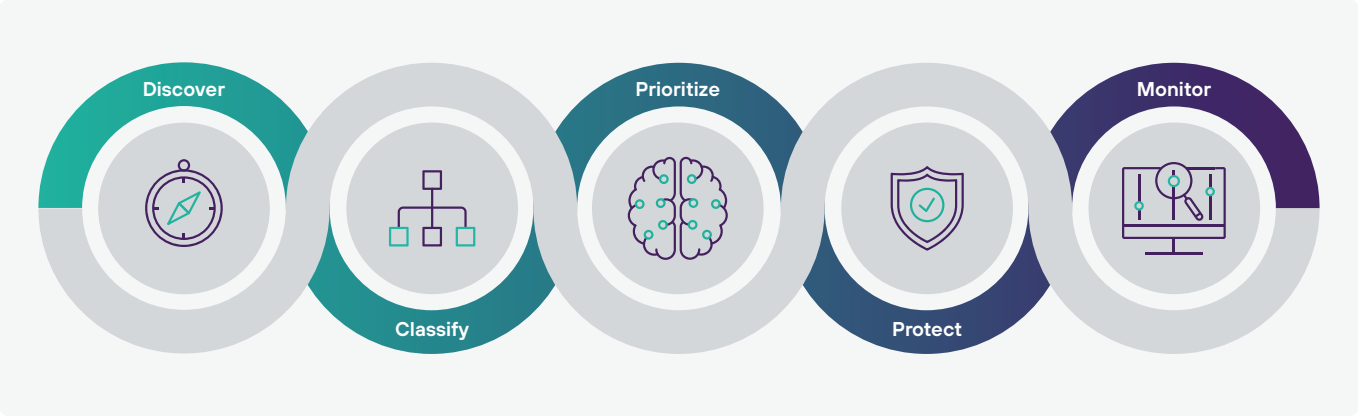


Figure 10: Visualizing the steps to Data Security Everywhere

Key tenets of Data Security Everywhere are:

- → **Discover** where your sensitive data resides, scanning rapidly at the organizational scale to identify data redundancies and other risks
- → **Classify** data with the greatest possible accuracy to make policies and reporting consistent and to give DLP the best ability to block data breaches
- → **Prioritize** where to focus data security efforts the most, also utilizing the ability to extend protection to additional channels or apps
- → **Protect** intellectual property and regulated data everywhere by preventing data exfiltration and maintaining compliance with regulatory requirements
- → **Monitor** risk to data to dynamically adapt policies, stopping insider threats and reducing time-consuming false positives

The combination of DLP (enhanced with Risk-Adaptive Protection) and DSPM is at the heart of a continuous strategy for minimizing data risk across the organization, providing a solid foundation for comprehensive data security wherever users and devices access the network.

We hope this guide has been helpful in planning and executing your DLP deployment. Visit forcepoint.com to find more DLP resources or to schedule a trial of one of our data security solutions

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on forcepoint.com, X and LinkedIn.

[Practical-Exec-Guide-to-DLP-Whitepaper-EN] 31Jan2025