
Six Stages to a Painless DLP Migration



Forcepoint


Whitepaper

Table of Contents

02	Introduction
04	Stage 1 – Scope and Project Initiation
06	Stage 2 – Review Your Current Environment
08	Stage 3 – Installation and Configuration
09	Stage 4 – Migration
11	Stage 5 – Monitoring and Testing
13	Stage 6 – Knowledge Transfer
14	Are You Ready to Migrate?

“A DLP migration doesn’t have to be painful; with the right, product, the right partners and, crucially, the right plan, you can realize a successful transition in as little as 6 weeks.”

**– Abdul Pasha,
Director of Professional Services, Forcepoint**



Introduction

Two things we know for sure. Data will continue to grow, and it will always be at risk. IT organizations across multiple industries are challenged to maintain data security and integrity at a time of relentless cyberattacks, increased regulatory oversight, the prevalence of hybrid in-office and remote work environments, and demand for continuous data access across a multitude of devices and networks.

[Data Loss Prevention \(DLP\)](#) is a must. New risks and digital transformation are forcing companies to think differently about DLP today. Finding the right solution that seamlessly fits your needs and facilitates an easy migration might seem elusive, regardless of whether it's a replacement for a legacy DLP or your very first DLP deployment. IT professionals will put off leaving sub-par legacy DLP solutions because of nightmarish stories or previous frustrations about migrating to a different DLP solution. After all, it's not just deploying a new data security application. You're transitioning policies and incident response programs and processes into a new vendor's product and paradigm for data loss prevention. That's why many in IT think the risks outweigh the rewards of DLP migration and, therefore, continue struggling along with their current, frustrating DLP solution.

But a DLP migration doesn't have to be painful or frightening. If you have the right strategies and solution in place, you can overcome the common migration obstacles of multiple products, vendor consolidations and mergers, software updates, and evolving threats and regulations.

The key to a successful migration includes three elements: a product that fits your needs, an experienced team, and a proven migration strategy.

Finding a data security product that fits

As data security professionals, you need to streamline your work to accelerate security risk responses. Moreover, the DLP solution you choose must help you meet the demands of multiple regulations and maintain compliance with various internal and international policies that continue to evolve. Finding solutions with built-in automation and comprehensive reporting make it easy to not only enforce security policies but also catalog incidents and responses for simplified review and analysis.

Forcepoint DLP provides powerful safeguards to stop unwanted data exfiltration before it can happen, regardless of where data resides, both on-prem and in the cloud. Forcepoint offers 3X more pre-defined policies than major competitors with 1,600-plus templates of data security policies to help you quickly meet regulations across 83 countries and every major industry. DLP is a major part of our total security portfolio, and we continue to deliver innovations like the industry's first

risk-adaptive data protection to automate security response based on behavioral risk. With a strong foundation for mapping and expanding your own rule set, Forcepoint DLP delivers complete control over your sensitive data and intellectual property everywhere.

Forcepoint DLP advancements have been recognized with multiple industry awards including:

- A 9X Leader in the Gartner® Magic Quadrant for Enterprise Data Loss Prevention
- [Gartner's Customer Choice Award 2020](#)
- [Radicati Group 2021 DLP Market Quadrant Top Player](#)
- [Frost & Sullivan APAC 2021 DLP Company of the Year](#)

Trusting a partner to navigate you through the migration

The DLP software landscape is constantly changing whether through new introductions, mergers, acquisitions, or simple failure – all of which has a major impact on your service and support. Forcepoint and our global network of implementation and channel partners are committed to delivering effective DLP deployments to companies of all sizes and industries. Forcepoint and our partners directly provide the expertise, contract flexibility, and knowledge transfer to make each customer's DLP migration and deployment a complete success. Depending on your requirements, either Forcepoint or the partner will support each stage and deliver professional services. In every case, Forcepoint will be responsible for guiding you throughout the DLP migration. We want DLP to make every IT team successful and be heroes within their organizations by ensuring a reliable and secure environment.

A proven set of migration paths and strategies

The last part, and possibly the most important, is the right strategy. Forcepoint has helped hundreds of customers move from existing DLP environments with a wealth of knowledge, experience, and dedication to data and operations. We have a proven track record for migrating DLP in a little as 6 weeks, without interrupting operations. We treat your data and our customers with respect, while we leverage industry best practices and our own experience to successfully and efficiently move you from the existing system to Forcepoint's industry-leading DLP.

"We treat your data with respect. After partnering with hundreds of customers and hundreds and thousands of hours working with them, we've created a framework on how to migrate successfully. At the end of the day, our job is to ensure our customer's data is protected and transparent to the end-user."

– **Abdul Pasha,**
Director of Professional Services, Forcepoint

And through lessons learned from thousands of hours of helping customers migrate to DLP, we've developed a six-stage strategy to help take the pain out of your next DLP migration. This is our best practices guide for working collaboratively with you and our channel partner to deliver the most efficient, successful migration.



Stage 1

Scope and Project Initiation

Measure twice. Cut once. This rule applies to carpentry and DLP migration. Everything starts with the scope. When we talk to clients about DLP migration, we start by understanding your priorities and goals – long and short term. Are you working on a deadline or a renewal? Are you racing to a compliance deadline? Is a merger or acquisition activity requiring consolidation of and expansion of your programs?

We look at what makes for quick wins to help you build integrity and trust within your business. And our collective effort can look at your use case goals to help establish a timeline. Pinpointing focus areas is key in this stage, whether you're prioritizing endpoint or network security, or want to start with data discovery.

Once we know all of this, we start aligning resources on your end and ours and begin confirming prerequisites to accomplishing your goals. If you don't have a clear idea of what your goals and timeliness look like, we can help you there too.

Are you planning to rip and replace the existing DLP or expanding your DLP reach or capability? We recommend a phased approach to match your current DLP capability with your new solution before adding and layering on new functionality. Start with a reverse timeline and examine your internal resources and business expectations. This should help you move directly to a deployment that implements your existing rules and policies. Forcepoint can help you start from scratch and build a blueprint for the program, including

recommended policies, incident response, timelines, beta testing, and reporting processes that will meet your short-term and long-term goals.

Once the blueprint is in place, we work with you to match up personnel with the required skills for the core team, as described in Figure 1. This roster and approach can work for either small or large organizations. In smaller organizations, we're agile enough to work with teams that crossover multiple functions: some people may wear multiple hats within the core team. Larger enterprises may have several specialists covering one of the areas on the core team. For global organizations, we have teams of network security engineers who speak multiple languages. We partner with customers to put together the right team of people based on their resources, so that all the skills required are brought together for a successful deployment. Working across diverse organizations ensures there are no blind spots in the implementation plan.

CORE TEAM	SKILLS REQUIRED
Project Manager / Business Analyst / Risk & 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
DLP SME	Rule condition, use-case, 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
DLP Event Escalation	Monitoring and ad-hoc escalation

Figure 1. Matching DLP Migration Stakeholders and Skillsets

With resources and skills matched, we'll create a project initiation plan that can compress or expand like an accordion to fit your needs and resources, working back from the established deployment date. The following example shows a conservative 16-week plan of activities. However, Forcepoint has successfully supported the migration of 100,000 endpoints in as little as 6 weeks! This timeline will help you know exactly when something will happen and help communicate the overall project to your management teams. Note below that the first stage covers the longest period—hence, measure twice, cut once. Let's take our time and get this right.



Create a Project Implementation Plan

- Work backwards from end of existing contract.
- 16 weeks is a conservative baseline.
- A successful implementation can be achieved in as little as 6 weeks.

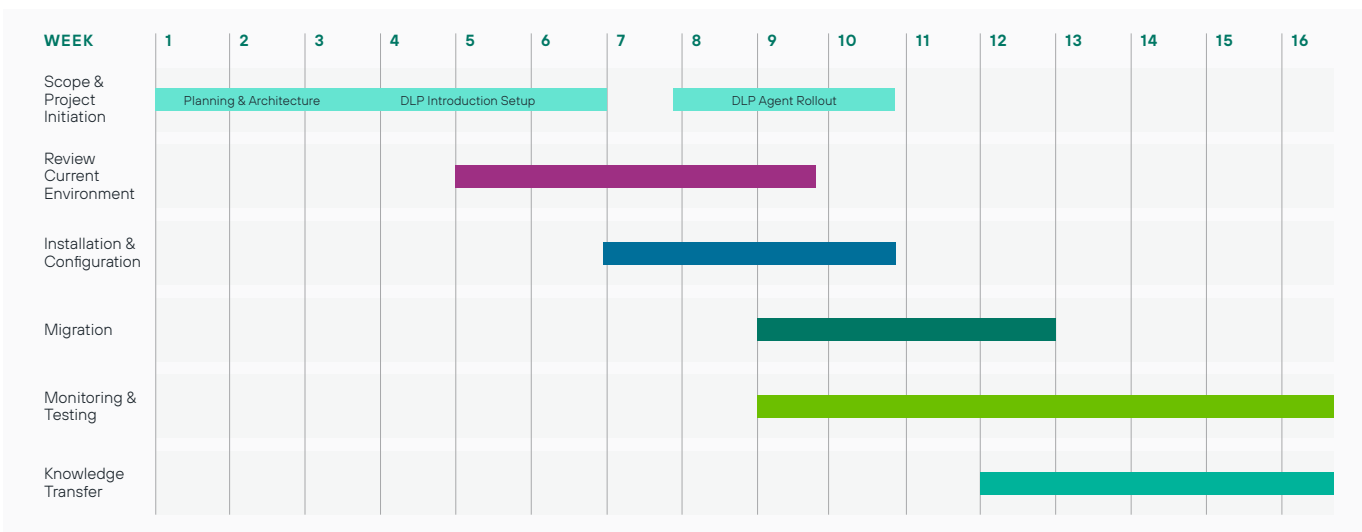


Figure 2. Example Implementation Plan Showing a 16-Week Timeline



Stage 2

Review Your Current Environment

This is also our chance to sit down with you and thoroughly understand your environment, short-term and long-term goals, issues, and resources. We need to understand your current environment perfectly as we begin designing an implementation plan and translate your needs and activities into a Forcepoint environment, like the example below where someone is migrating from Symantec to Forcepoint.

From here, we can dive into your architecture and how much of your data and operations are in the cloud or on-premises. In this phase, it's important to establish a clear and common language for the technology that everybody understands and help customers match the prior application environment to

the new Forcepoint capabilities and methodology. We'll start by asking you to run diagnostics that will help us understand your footprint. This could take us a couple of hours or weeks to collect the necessary data, depending on accessibility.

We will look at your email traffic so we can size your needs properly and explore your incidents so we can make sure you have enough database capacity. We want to know how much you are partitioning. How much are you archiving? What is your data retention rate? And we'll look at your policies and action plans, along with your false positives and pain points.

Example Product Name Translation Guide: Symantec to Forcepoint DLP Components

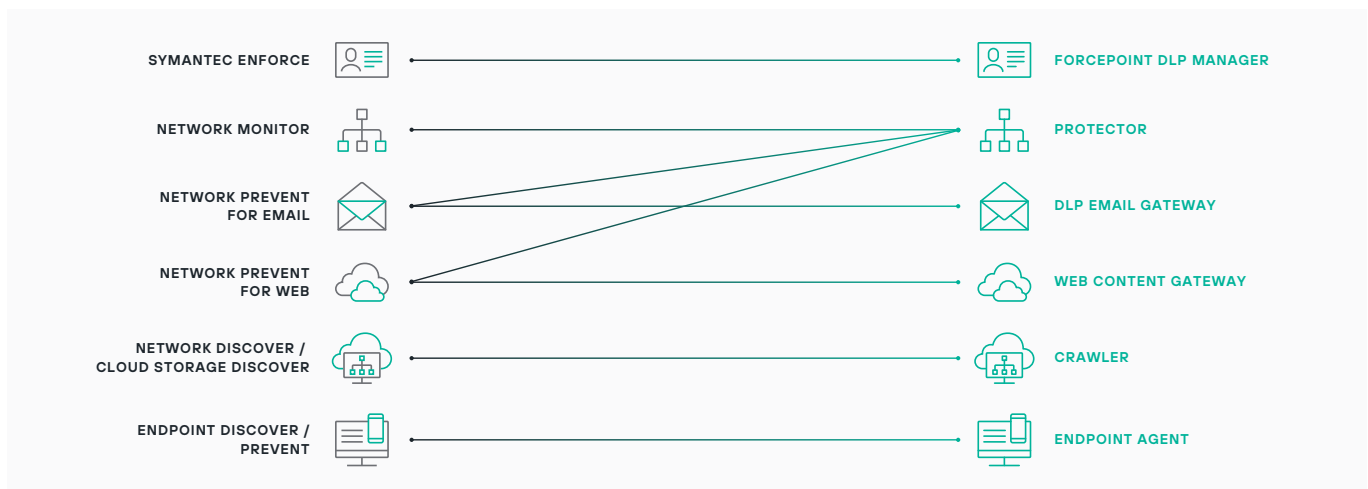


Figure 3. Mapping Legacy to Forcepoint DLP

You should know that migrating existing policies is not as simple as downloading them and uploading them as a file to your new solution – policies must be mapped and recreated. However, with over 1,600 policies out-of-the-box, Forcepoint provides the most extensive template library to help you save enormous amounts of time and money. We will help map your policies to ours. By using Forcepoint’s policy wizard, you can identify the most relevant policies for your regulated industry without having to create or customize your own. Forcepoint’s expertise and pre-defined templates offer you the opportunity to set the right policies quickly, review as you go along, and make improvements easily.

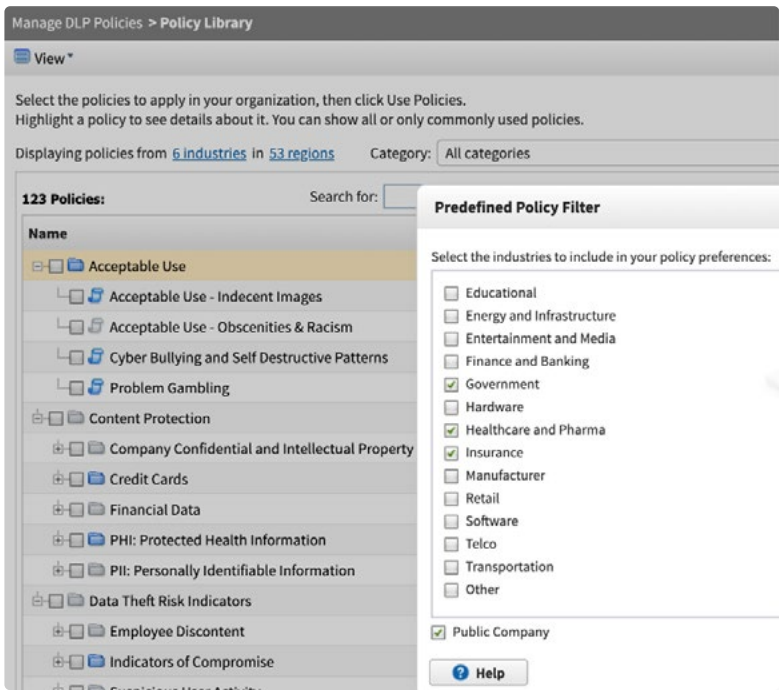
Our work goes beyond a lift-and-shift migration. We’ll hold whiteboard discussions to map out the security policies and incident management workflows. This is a review of your data, users, concerns, status, and ultimate business outcomes. It’s an opportunity to find gaps, learn more, and find ways to optimize your environment. We’ll then test the new proposed environment in our Forcepoint Go4Labs and create a mapping control report that clarifies what to do when data is used and in motion, the type of policy we’re enabling, and the preferred notification and action plan.



3x

Forcepoint has over 1,600 pre-defined classifiers.

3x more than other leading DLP solutions in the market. For comparison, Microsoft has only 204 classifiers.



→ Forcepoint covers a range of key industries and over 155 regions within 83 countries.

Figure 4. Pre-defined Policies by Industry



Stage 3

Installation and Configuration

Now that you've done the hard work of planning, you've simplified the important step of installation and configuration.

On top of that, we designed Forcepoint software to be self-installed in as little as a couple of hours. We'll develop and provide high-level and low-level installation and configuration documents that match your environment. Documentation is also available to your database and networking teams, or a certified third partner.

Initially, to avoid disrupting your business, you will not enact any blocking actions. Instead, you'll configure Forcepoint DLP for observation before actual enforcement is put in place.

We provide customized support to help teach you how to install, configure, and run the software guided by tech support professionals around the globe with instructions in multiple languages. And then we will test your installation for connectivity and end-to-end performance to ensure everything is working correctly.

1. **Develop high-level and low-level design documents**
2. **Install and configure DLP per approved design documents**
3. **Configure DLP for observation prior to enforcement**
4. **Perform connectivity testing on pilot users**

Stage 4

Migration

After installation, configuration, and testing for connectivity, you'll begin working to tune the new DLP software into your actual environment and start making progress to show the first value.

Establishing First Value

The first value reflects accomplishment against your short-term goals. This might include, as a use case, a goal of having 50,000 agents deployed or addressing concerns over your network or storage requirements. USB drives, for example, should be encrypted. So, start by installing agents and policies to ensure that happens. First value is really to make sure that you see the business result of the product as quickly

as possible. During this phase, include an active directory import, notification, and action plans, along with end-to-end environment incident reports.

Determining Incident Response

Next, replicate and map policies, workflows, and metrics based on your use cases. And conduct stress tests using sample data from live customer traffic to generate and gauge false positive incident rates.

Action Plan Details

Name: BLOCK ALL

Description: Block and audit incidents from all channels. If notifications are configured, generate notifications.

Data Loss Prevention | Discovery

Network Channels

Email: ESG-DLP-Email Quarar ?

Encrypt on release ?

Mobile email: Quarantine

FTP: Block

HTTP/HTTPS: Block

Chat: Always permitted

Plain text: Always permitted

Endpoint Channels

Email: Block

Application control: Block

Removable media: Permit

HTTP/HTTPS: Block

LAN: Block

Printing: Block

Cloud Channels

DLP Cloud Proxy ?

Help OK Cancel

→ Centralize DLP through multiple channels including network and endpoint.

→ Audit, permit (user coaching), mail encryption (USB and network email), quarantine/release (network email) and block.

Figure 5. Centralizing DLP Actions: Network and Endpoint

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	
Custom	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	TBD

*Additional granularity available with risk-adaptive DLP

Figure 6. Determining Incident Response Based on Severity and Channel

Resolving Gaps

Based on what you discover, prioritize and resolve gaps and fix issues around the endpoints, user experiences, or latency. Identify out-of-the-box policies and fingerprint options that match your requirements and save you time from creating or adjusting your own.

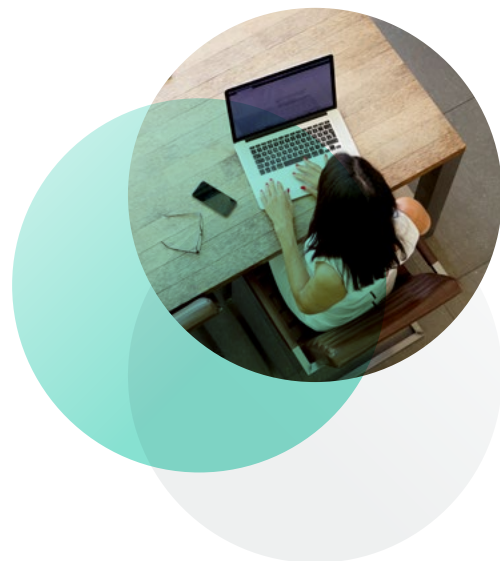
Identifying Approvals

Before rolling out the DLP environment, conduct User Acceptance Testing (UAT) and identify the standard policy that you use for approvals. Find out who needs to sign off and what acceptance testing looks like to meet your expectations. And identify a group of testers to ensure everything is working the way it should.

Rolling out DLP

If everything meets expectations, begin migrating product traffic in phases by regions, offices, and departments as stated in your high-level design (HLD) and low-level design (LLD). Remember, do this in stages to avoid disrupting your business, whenever you're ready, on your schedule and after hours, and even while your prior DLP is running. No interruptions.

Monitor everything for the next week to confirm the live environment is performing as desired.



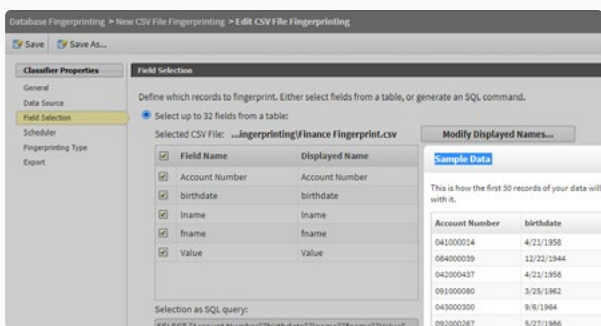


Stage 5

Monitoring and Testing

Once the migration is completed, monitoring and testing the DLP environment will help get it just right. This means minimizing unintentional incidents and reviewing and fine-tuning it to add exceptions or exclusions. Adjust policies and add additional fingerprinting to existing rules if needed.

or marketing. The more you learn about your data, the more accurate you can be. All layers of data identifiers and classifiers are important to the DLP configuration, inspection, and testing processes, especially the file metadata and other classification labels, regular expressions, hundreds of file types, and OCR-based text within images – all represent a huge portion of data identification work (see Figure 8).



Database fingerprinting is the most advanced inspection method, protecting the crown jewels of any organization's data. You can apply fingerprint both structured and unstructured data using hashing to provide exact matching for a wide range of highly important customer data.

Figure 7. Database Fingerprinting

The next step is incredibly important: create pre-defined custom reports based on use cases for your business, such as applications for specific departments like legal, development,

“The richness of data identification can improve through the additional monitoring and testing at this stage. You can get a much more precise data identification framework in place and a rich library of data to pull from that you can apply to your environment.”

— Kevin Oliveira,
Senior Manager of Product Marketing, Forcepoint

For example, if a user tries to manipulate a document or compress dozens of files at once, your policy should be able to inspect them. As you become more confident in your understanding of your data, you can refine your policies and criteria based on the various file classifiers, labels, tags, and headers. By optimizing reporting, we can also help you demonstrate the efficacy of the program, streamlining of policies, and reduction of false positives for senior leadership.

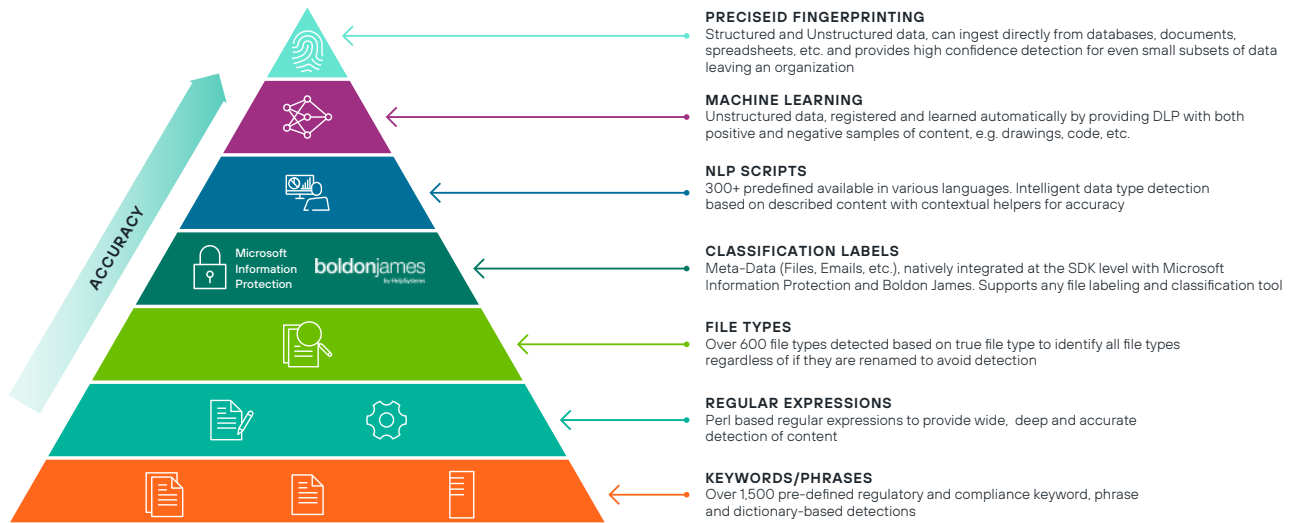


Figure 8. Data Classification

The rich data intelligence can help you train your new Forcepoint DLP system to deliver true positives and curtail false alerts. Reducing false positives is key to a successful end-user and IT security experience. The richness of data identification can improve through the additional monitoring and testing at this stage. You can get a much more precise data identification framework in place and a rich library of data to pull from that you can apply to your environment. After all, the goal of good DLP is to only step in when it's needed – and let people get on with their jobs when not. Monitoring and testing again and again allows you to minimize risk and maximize productivity. After that, it's time to backup and restore.

Before we leave this stage, sit around the table to confirm standard operating procedures with your stakeholders. Then, if an issue occurs, everyone knows their roles and responsibilities from DLP tools and program perspective. For example, if an incident occurs or if there's a policy violation, the security response team will know how to properly triage.



Stage 6

Knowledge Transfer

As you continue to monitor and test the DLP environment, we will transfer knowledge we gain from looking at customers' live data. Part of this knowledge is provided through training for administration and operation teams. We can create bespoke training and knowledge transfer documents to allow your team to own the solution.

Customers receive training and access to the Forcepoint knowledge base where they can learn procedures like how to open tickets and provide relevant information. We continue to train and pass on knowledge because we want you and your teams to quickly learn and comfortably use the Forcepoint DLP.

Forcepoint focuses on knowledge transfer from start to end, but really at the end, what we want to do is make sure you and your team are confident and at ease with the solution. You should also plan to train your own internal stakeholders,

partners, and employees to expand the knowledge sharing. Ultimately, it's everyone's responsibility to protect the organization's data and intellectual property.

At the end of this engagement, we will seek a project sign-off based on the statement of work and a survey to confirm the project is complete. Then, you're formally transferred to Forcepoint tech support for ongoing help.

Are You Ready to Migrate?

DLP migrations don't have to be as complicated, daunting, or nerve wracking as the first time. That should never be a reason to stay with a legacy platform that doesn't meet your needs. You don't have to settle. Doing DLP right can transform the product from being a business blocker to a business enabler and competitive edge.

Remember, a best-in-class DLP migration should give you peace-of-mind through the ability to:

- Identify clear project goals and use cases—both short-term and long.
- Identify your target migration date and then work backwards to plan a timeline.
- Plan a phased roll-out by region or department and in terms of maturity and scale. Aim to match your previous deployment features before layering more advanced functionality.
- Pick the right solution, partners, and strategy to suit your business.

With our vast experience of successful deployments and decades of innovation, Forcepoint provides a viable path away from your existing DLP software without the risks or headaches. Together with our partners, we can easily migrate from your existing DLP system to a world-class product that simplifies data security to make your life easier. Contact us to find out how to partner with a vendor 100% committed to protecting your data and users.



For more information, contact us to [set up a demo](#).



You can also watch a webinar on the [six-stage migration approach](#).

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.