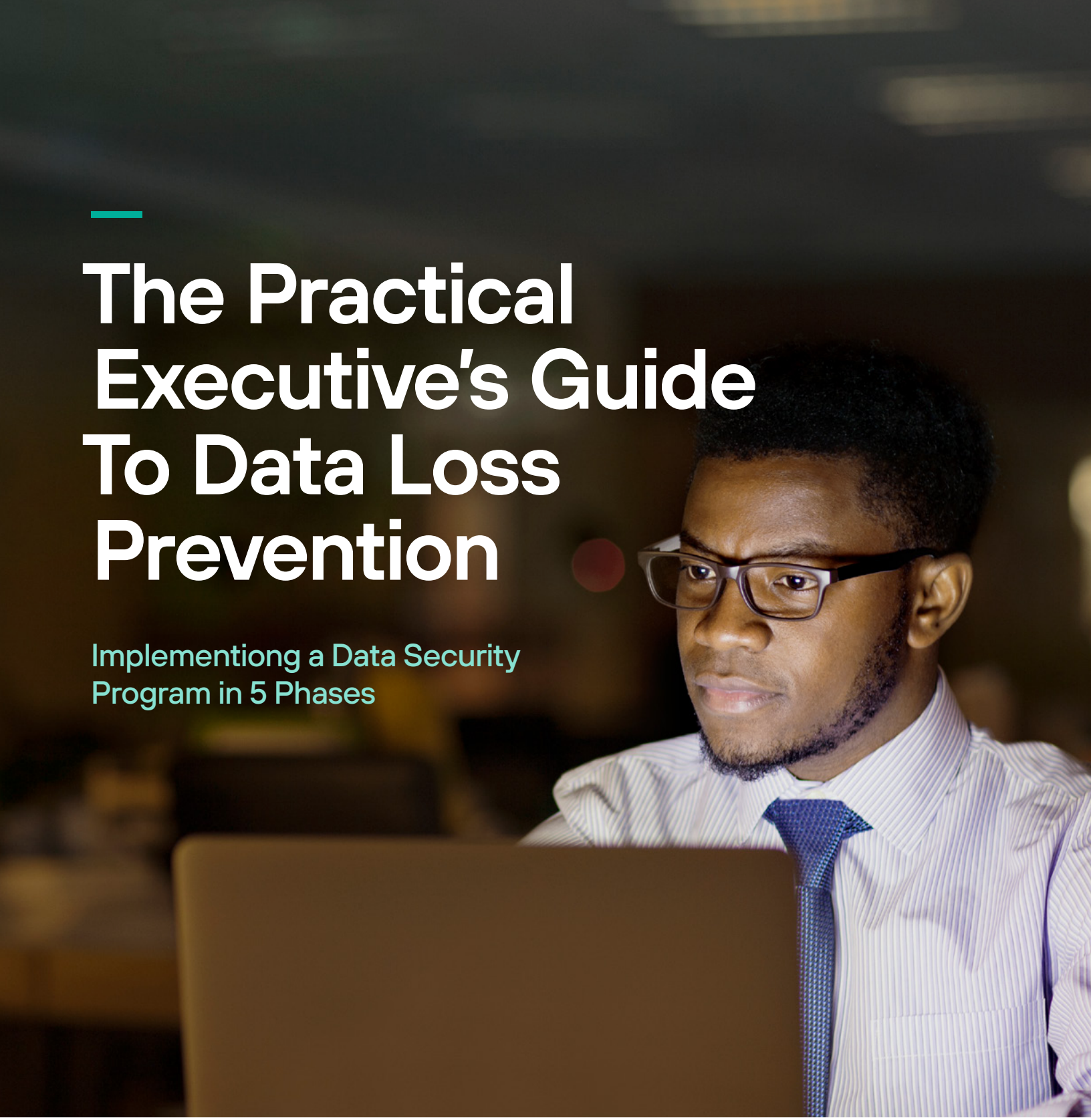


The Practical Executive's Guide To Data Loss Prevention

Implementiong a Data Security Program in 5 Phases

Forcepoint

Whitepaper

Table of Contents

The Problem

There has been much confusion in the marketplace regarding data loss prevention (DLP) controls. There are numerous contributing factors, most notably a general lack of understanding in the vendor community about how data security works or what communicates risk to a business. Impractical processes were established, operational bottlenecks ensued, and the ongoing threat of data loss and theft persisted. An organization's poor experiences may be directly related to the lack of clarity in program goals, insufficient planning, and poor implementation.

As a result, organizations that want to protect their confidential data, secure access as well as their increasingly hybrid workforce, and comply with laws and regulations are often skeptical and unsure where to turn. Some have been burned by unsuccessful implementations.

The important thing to realize is that the technology behind DLP controls is not the most critical factor that determines your success—it's the methodology and execution strategy of your vendor that governs both your experience and results.

This whitepaper provides guidance and clarity on the following:

- → It explains the challenge of securing the hybrid workforce and context for putting data security at the heart of a secure access program.
- → It explains important distinctions and advises on how to assess a potential vendor.
- → It provides valuable insight into data-breach trends.
- → It offers an easy-to-follow five-phase process for implementing and executing a data security strategy in a manner that is practical, measurable, and risk-adaptive in nature; and finally,
- → It offers numerous "practical best practices" to avoid common pitfalls and eliminate most of the operational challenges that challenge DLP implementations.

"It's not the technology behind DLP controls that ultimately determines your success— it's the methodology and execution strategy of your vendor that governs both your experience and results."

A Starting Point

All DLP controls should fulfill the first two objectives in the following list.

1. They provide the ability to identify data.

- → **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)

2. They identify data as described or registered.

- → **Described:** Out-of-box classifiers and policy templates help identify types of data. This is helpful when looking for content such as personal identifiable information (PII).
- → **Registered:** Data is registered with the system to create a "fingerprint," which allows full or partial matching of specific information such as intellectual property (IP).

However, a more advanced DLP solution will also be equipped with the third capability.

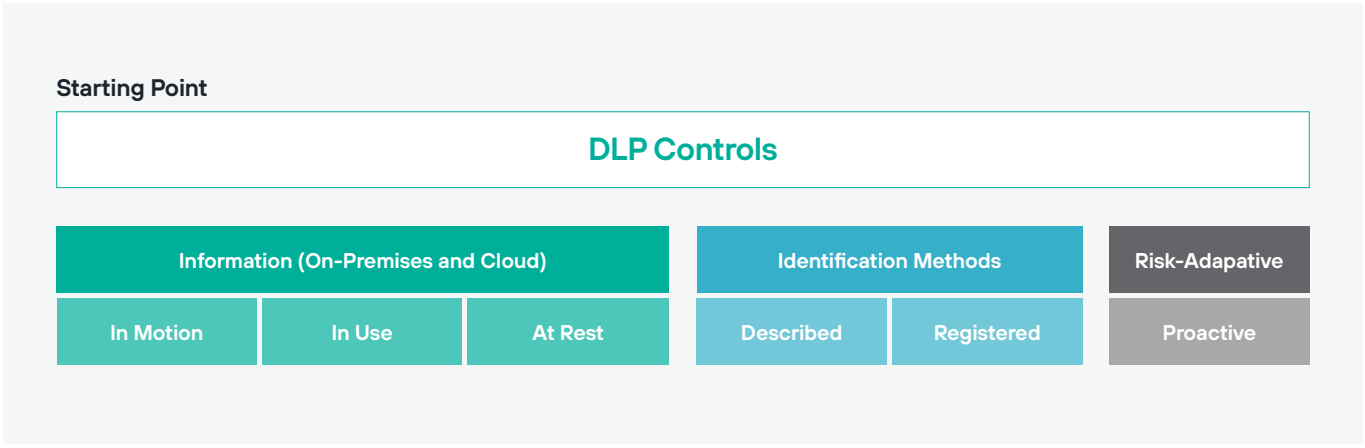
3. They take a risk-adaptive approach to DLP

- → Risk-adaptive DLP sets advanced data loss prevention solutions apart from the other DLP tool sets. Derived from Gartner's continuous adaptive risk and trust assements (CARTA) approach, risk-adaptive DLP adds flexibility and pro-activity to DLP. It autonomously adjusts and enforces DLP policy based on the risk an individual poses to an organization at any given point in time. Real-time enforcement is then able to predict and stop breaches before they occur. Productivity increases as users are less susceptible to intrusive security, while IT investigations are made easier by reducing false positives and incident risk ranking.

To illustrate how the first two common capabilities work, a DLP control is told:

- → What to look for (e.g., credit card numbers)
- → The method for identifying the information (described/registered)
- → Where to look for it (e.g., network, endpoint, storage, cloud)

What happens after a DLP control identifies the information depends on a) the risk tolerance of the data owner, b) the response options available when data loss is detected, and c) if the solution is risk-adaptive.



From Vision to Implementation

Although all DLP controls provide similar capabilities, it's important to understand that not all vendors have the same vision for how DLP helps to address the problem of data loss. Therefore, your first step is to understand the methodology and execution strategy of each vendor that you are considering.

By asking a vendor, "What's your methodology?" you are really asking, "What's your vision for how this tool will help solve the problem of data loss?"

This is an important yet rarely asked question; the answer allows you to understand a vendor's vision, which in turn enables you to identify its unique capabilities and the direction its roadmap is likely to head. For decision makers, knowing why vendors do what they do is much more relative to your success and long-term happiness than knowing what they do.

A vendor's methodology also heavily influences its execution, or implementation, strategy. For example, if one vendor's methodology starts by assessing data-at-rest, and another's starts by assessing data-in-motion using risk-adaptive controls, then their execution strategies differ greatly. How a vendor executes DLP controls matters because it impacts both your total cost of ownership (TCO) and your expected time-to-value, which are crucial for making the right purchase decision and for properly setting expectations with stakeholders.

An important note: you should avoid applying one vendor's methodology to another's technology. The methodology defines and drives a vendor's technology roadmap, so by mixing the two aspects you risk investing in a technology that won't meet your long-term needs.

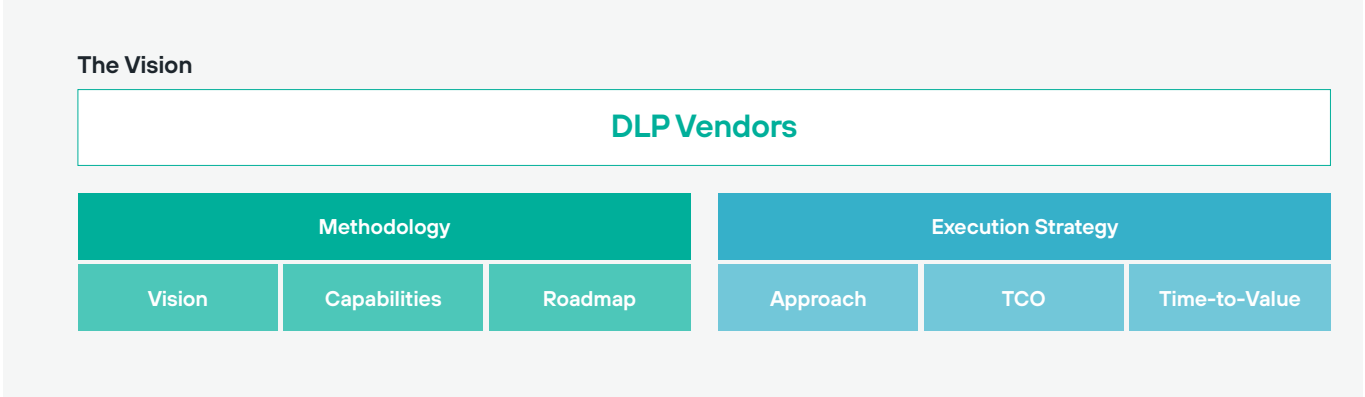
Measurable and Practical DLP

If you've attended a conference or read a paper on DLP best practices, you are probably familiar with the metaphor, "don't try to boil the ocean." It means that you can't execute a complete DLP program in one fell swoop. This is not a useful best practice because it doesn't help you figure out what to do and when. In some respects, "don't boil the ocean" sounds more like a warning than a best practice.

Unfortunately, many published best practices aren't always practical. Lack of resources, financial or otherwise, and other organizational issues often leave best practices un-followed—and therefore effectively useless. Equally, many guidelines may err too far on the side of caution; data must be kept secure but accessible—overly intrusive, fixed policies can become a roadblock to productivity and a risk to businesses. There's far greater value in practical best practices, which take into consideration the cost, benefits, and effort of following them, and can be measured to determine whether you and your organization can or should adopt them.

In order for your DLP control to be measurable and practical in managing and mitigating risk of data loss, there are two key pieces of information that you have to know and understand:

1. To be measurable, you have to know and apply the risk formula for data loss. Although similar to other risk models, the risk formula for data loss does have one substantial difference, which we explain below.
2. To be practical, you must understand where you are most likely to experience a high-impact data breach and use the 80/20 rule to focus your attention and resources.



The Risk Formula for Data Loss

The basic risk formula that most of us are familiar with is:

Risk = Impact x Likelihood

The challenge with most risk models is determining the likelihood, or probability, that a threat will happen. This probability is crucial for determining whether to spend money on a threat-prevention solution, or to forego such an investment and accept the risk.

The difference with the risk formula for data loss is that you are not dealing with the unknown. It acknowledges the fact that data loss is inevitable and usually unintentional. Most importantly, the risk formula allows risk to be measured and mitigated to a level that your organization is comfortable with.

Therefore, the metric used for tracking reduction in data risk and ROI of DLP controls is the rate of occurrence (RO).

Risk = Impact x Rate of Occurrence (RO)

The RO indicates how often, over a set period of time, data is being used or transmitted in a manner that puts it at risk of being lost, stolen, or compromised. The RO is measured before and after the execution of DLP controls to demonstrate by how much risk was reduced.

For example, if you start with an RO of 100 incidents in a two-week period, and are able to reduce that amount to 50 incidents in a two-week period after implementing DLP controls, then you have reduced the likelihood of a data-loss incident (data breach) by 50%.

Risk-adaptive solutions are especially effective at minimizing the RO. This is because they are far more accurate in identifying true data risk in the context of a user's broader interactions. They greatly reduce false positive incidents and thus provide an advantage over traditional DLP, not only minimizing risk, but presenting it more accurately.

The 80/20 Rule of DLP

In addition to identifying RO, it's important to discover where your organization is most likely to experience a high-impact data breach. To do this, you need to study the latest breach trends and then use the 80/20 rule to determine where to start your DLP efforts. A recent study has made this information readily available.

According to a 2021 study by the Ponemon Institute, compromised credentials are the most common initial attack vector, making up 20% of breaches, followed by phishing at 17%.[1]

To truly have an effective program for protecting against data loss, you have to feel confident about your ability to detect and respond to data movement through web, email, cloud, and removable media.

This is where a risk-adaptive DLP solution can provide an advantage. Traditional DLP solutions often struggle to identify items such as broken business processes or irregular activity, both of which can lead to significant data loss. Risk-adaptive DLP understands the behavior of individual users and compares them to an observed baseline to quickly and autonomously tighten DLP controls when activity is not in line with the end user's job function or normal behavior. This proactive approach can reduce risk for accidental data loss and exposure.

[1] Cost of a Data Breach Report 2021, produced by the Ponemon Institute on behalf of IBM.

The Forcepoint DLP Methodology and Execution Strategy

Considering the latest data breach trends and applying the risk formula for data loss are first steps towards the creation of a data loss prevention strategy. The most effective DLP methodology focuses on understanding user intent to prevent data loss before it occurs. Execution should focus on providing the best time-to-value for demonstrating a measurable reduction of risk.

Time-to-Value

Time-to-value is the difference in time between implementing DLP controls and seeing measurable results in risk reduction. Because the user forms the greatest point of data risk, whether from an accidental or malicious insider or as the target of external attack vectors, you get the best time-to-value with DLP that is focused on data-in-motion and data-at-rest using risk-adaptive technology in the background.

You might be scratching your head if you've been told by other vendors or thought leaders to first focus your DLP controls on Data-at-Rest. They often say, "If you don't know what you have and where it is located, then you can't expect to protect it." But this is not true; in fact, DLP controls are designed to do so. Either the other vendors and experts don't understand how to properly assess and address risk, or they are simply repeating what others say because it seems to be working for them.

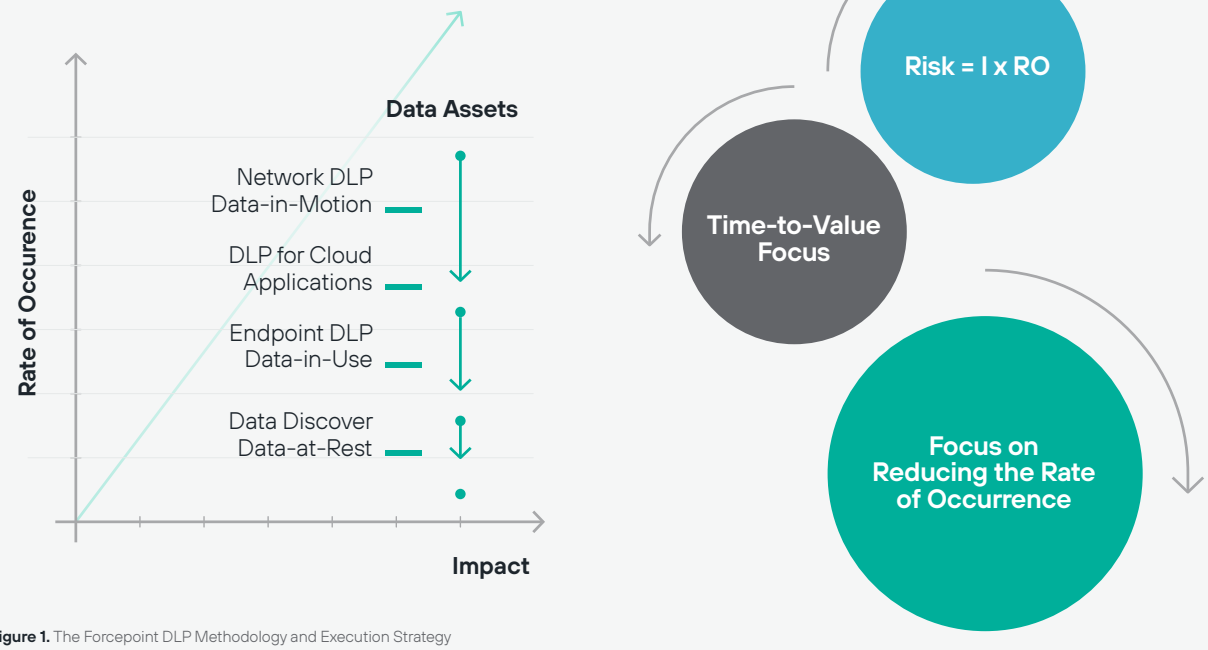


Figure 1. The Forcepoint DLP Methodology and Execution Strategy

Why should you challenge a recommendation to start with data-at-rest? Consider the following questions:

1. Do you know any organization that has successfully identified and secured all sensitive data, especially with accelerated cloud adoption?
2. Do you have any idea how much time it will take to scan, identify, and secure every file containing sensitive information?
3. Do you know how much risk will be reduced as a result?

The problem with focusing on data-at-rest at the outset is that it focuses on implied risk, not actual risk, and therefore it cannot be measured in the context of risk reduction. Implied risk means that other conditions have to be met before a negative consequence can happen. In the context of data loss, those conditions are:

- → Someone or something with malicious intent has to be on your network or accessing your cloud environments.
- → They have to be looking for your sensitive data.
- → They have to find it.
- → They have to move it.

This is true for every organization, and leads us to the more important question: "How comfortable are you with your organization's ability to detect and respond when data is moving?"

There are three channels through which data loss occurs, where you detect and respond to actual risk:

- → Network Channel (e.g., email, web, remote access points, FTP)
- → Endpoint Channel (e.g., USB storage, printers)
- → Cloud Channels (e.g., Office 365, Box)

What About Data-at-Rest and Compliance?

Many regulations require you to scan your data stores for unprotected data-at-rest, so you might wonder why a DLP methodology and execution strategy wouldn't start there. But the truth is, auditors are more concerned with the fact that you are complying than whether you have complied.

So scanning for data-at-rest is important for compliance, but not the primary objective and value of your DLP control. Therefore, plan on using DLP for data discovery and compliance, but in a manner that is practical and sustainable for your organization.

Create policies for defensible deletion (destroying files you no longer need) to reduce risk and for long-term retention when mandated by law. The best place to start is to use DLP to automatically quarantine files that have not been accessed for at least six months. Assign permissions to your legal and compliance teams so they can make decisions based on data retention policies.

The Five Phases to DLP Success

The following five phases provide a process for implementing DLP controls that is practical for your business to follow and able to deliver measurable results. Whether you're early in your DLP maturity or well on your way, use these steps as a roadmap to success for traditional DLP applications or to augment your current data security approach with risk-adapative DLP.

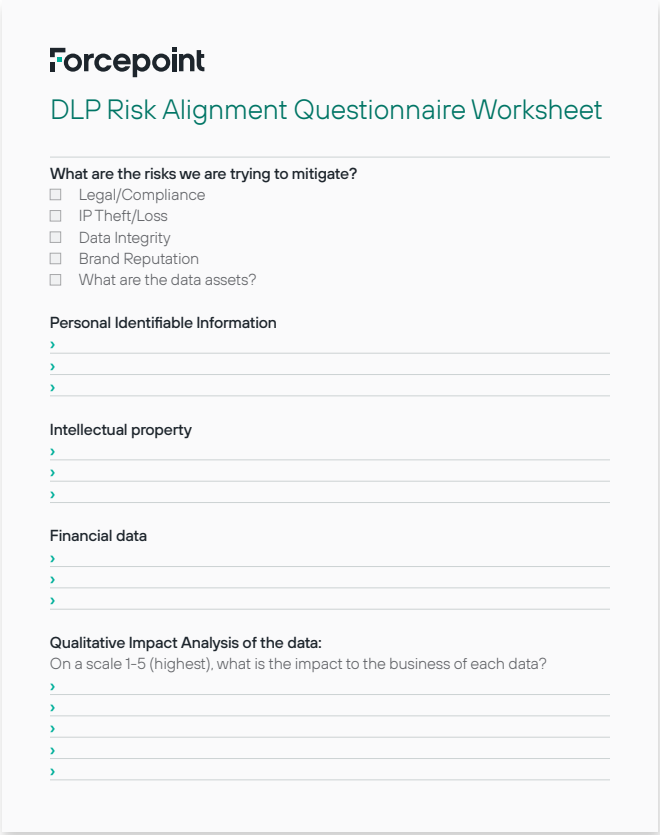
Phase 1:

Build an Information Risk Profile

Goal: Understand the scope of your data protection needs.
Overview: Create an initial information risk profile that includes:

- → 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).

1. **State the risk you want to mitigate**
2. **Start a list of data assets and group by type**
3. **Interview data owners to determine impact**
4. **List channels that can transmit information**



Forcepoint

DLP Risk Alignment Questionnaire Worksheet

What are the risks we are trying to mitigate?

- ☐ Legal/Compliance
- ☐ IP Theft/Loss
- ☐ Data Integrity
- ☐ Brand Reputation
- ☐ What are the data assets?

Personal Identifiable Information

›
›
›

Intellectual property

›
›
›

Financial data

›
›
›

Qualitative Impact Analysis of the data:
On a scale 1-5 (highest), what is the impact to the business of each data?

›
›
›
›
›

Phase 2:

Map the Data Incident Severity and Response Chart

Goal: Determine data-loss incident response times according to the degree of severity.

Overview: Have your DLP implementation team meet with data owners to determine the level of impact in the event that data is lost, stolen, or compromised. Use qualitative analysis to describe impact, such as a scale of 1–5. This helps to prioritize incident response efforts, and is used to determine the appropriate response time.

Risk-adaptive DLP Option: Keep in mind, a DLP solution that takes a risk-adaptive approach is designed to prioritize high-risk activity, autonomously enforce controls based on risk, and reduce the time it takes to investigate an incident. The result is lower risk of impact and more proactive control of critical data.

The initial phases still apply, but will be augmented with risk-adaptive DLP.

1. **Start by discussing the types of data to protect**
2. **Align regulations with the data types identified**
3. **Determine how you will identify the data**
4. **Determine impact severity and incident response**

"GDPR breaches of personal data must be reported to the relevant supervisory authority within 72 hours of becoming aware of the breach."

Regulations			**Step 1:** Discuss General Data Types **Step 2:** Relative Regulations (Wizard Avail) **Step 3:** "ID" — Registered or Described **Step 4:** Quantity or % for High Medium Low		Impact Rating Legend		
Breach Notification	HIPPA	PCI/PCI-DSS			5, 4	3, 2	1
			Personal Identifiable Information	ID	High	Mod.	Low
			VIP PII	R	1	-	-
			PII	D	>100	>25	>2
			PHI	D	>100	>50	>2
			Financial Information	ID	High	Mod.	Low
			Credit Cards	D	>25	>5	>2
			Payroll Information	D	>25	>5	>2
			Intellectual Property	ID	High	Mod.	Low
			Project X	R	>25%	>10%	10%<
			Design Document	R	>25%	>10%	10%<
			User Name and Passwords	R	>25%	>10%	10%<

Step 1: Determine Incident Response Based on Severity and Channel

Goal: Define what happens in response to a data loss incident based on its severity and channel.

Overview: Your organization has a limited number of channels through which information flows. These channels become the monitoring checkpoints that the DLP controls use to detect and respond to data loss. List all of the available communication channels on your network, at the endpoint, and in the cloud (i.e., sanctioned cloud applications) on a worksheet. Then, apply a response (based on incident severity) using one of the response options available in the DLP controls for that channel.

You can also clarify any additional requirements that your organization has for delivering the desired response, such as encryption or SSL inspection. For example, removable media is one of the top three vectors for data loss; however, it is also a great tool for increasing productivity.

One option for mitigating the risk of data loss to Box or Google Drive is to automatically unshare files containing sensitive information that are transferred to cloud storage and shared externally.

Risk-adaptive DLP Option: A risk-adaptive DLP solution can provide organizations with granular enforcement controls across channels, giving the flexibility to adjust response based on the risk level of the user (e.g., audit-only for low-risk users vs. block for high-risk users). This allows users to effectively perform their job duties, without compromising data.

1. **Choose data or data type**
2. **Confirm channels to monitor**
3. **Determine response based on severity**
4. **Note additional requirements for desired response**

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-adapative DLP

Figure 2. DLP Channel Policy Mapping

Step 2: Establish an Incident Workflow

Goal: Ensure that procedures for identifying and responding to incidents are followed.

Overview: Refer to Figure 3. Incident Workflow diagram to view the process in which incidents are managed according to severity, and to see what happens once an incident is detected. 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 by 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.

Risk-adaptive DLP Option: If you choose to leverage an adaptive solution, investigation by an incident analyst is not required before action is taken. Incidents attributed to low-risk users may not pose a threat to the organization, and therefore should be permitted to keep from impacting productivity. However, these permitted actions would include safeguards such as requiring encryption when saving to USB or dropping attachments sent via email.

For higher-risk users and associated incidents, administrators can take a proactive approach by automatically blocking or restricting specific actions until the incident analyst can investigate.

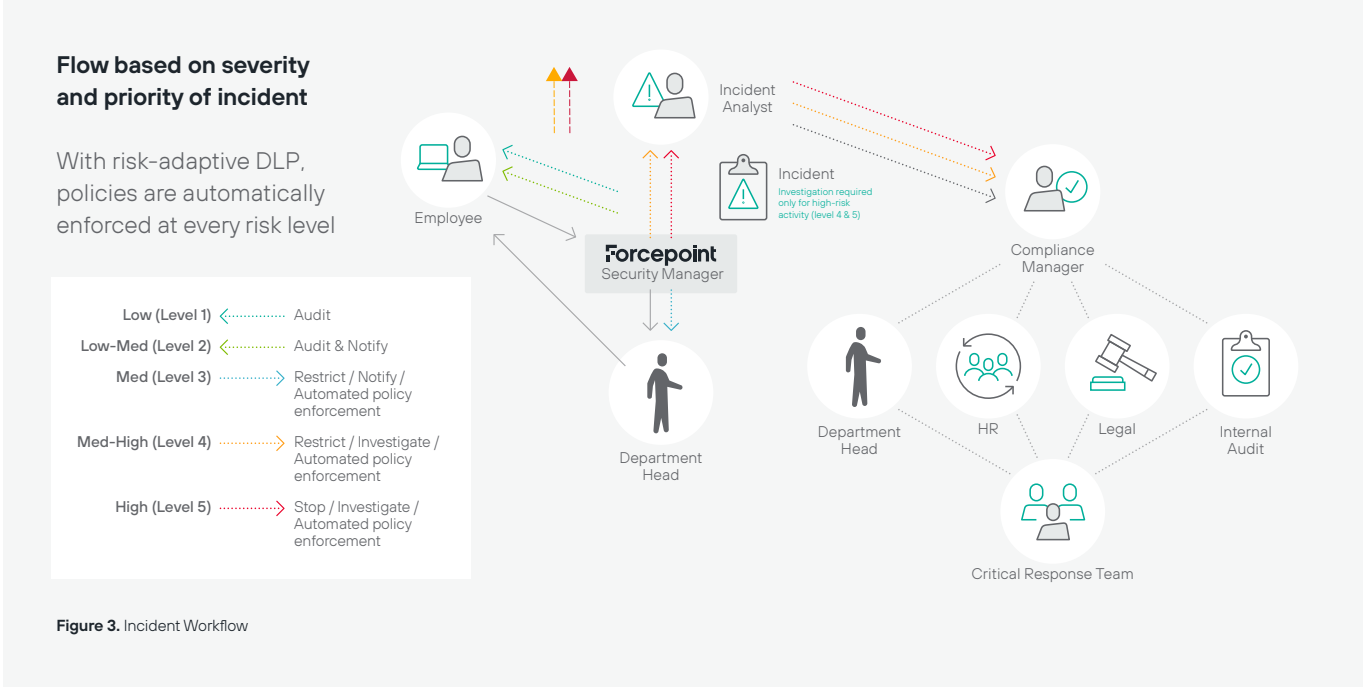


Figure 3. Incident Workflow

Phase 3:
Pilot the Monitoring Program

Goal: Implement network DLP to measure and begin to reduce risk.

Overview: Phase 3 has four additional steps. During Step 1, you assign roles and responsibilities to key stakeholders. In Step 2, you establish the technical framework. In Step 3, you expand the coverage of DLP controls. Then, in Step 4, integrate these controls throughout your organization.

Before it is actively applied, DLP should be run passively so that you understand the effects of your policies. 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.

After the initial monitoring, during which 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 RO (rate of occurrence) of data at risk. Then capture the results and report them to the executive team.

Risk-adaptive DLP Option: If you choose to implement a risk-adaptive DLP, you can run an analysis of incidents in audit-only mode versus graduated enforcement mode.

This contrasting data will highlight the reduced number of incidents requiring investigation without compromising your data. The observed results will be more indicative of true positives. It can also demonstrate the benefits of automation, reduced resources required to monitor and manage incidents, and increased productivity of impacted teams.

Step 1: Assign Roles and Responsibilities

Goal: Increase DLP program stability, scalability, and operational efficiency.

Overview: There are typically four different roles assigned to help preserve the integrity of the DLP controls and to increase its operational efficiency:

- → Technical administrator
- → Incident analyst/manager
- → Forensics investigator
- → Auditor

Each role is defined according to its responsibilities and assigned to the appropriate stakeholder. At this stage, it's common to see members of the DLP implementation team act as the incident managers. However, as the DLP controls reach maturity and inspire a high level of confidence, these roles will be transitioned to the appropriate data owner.

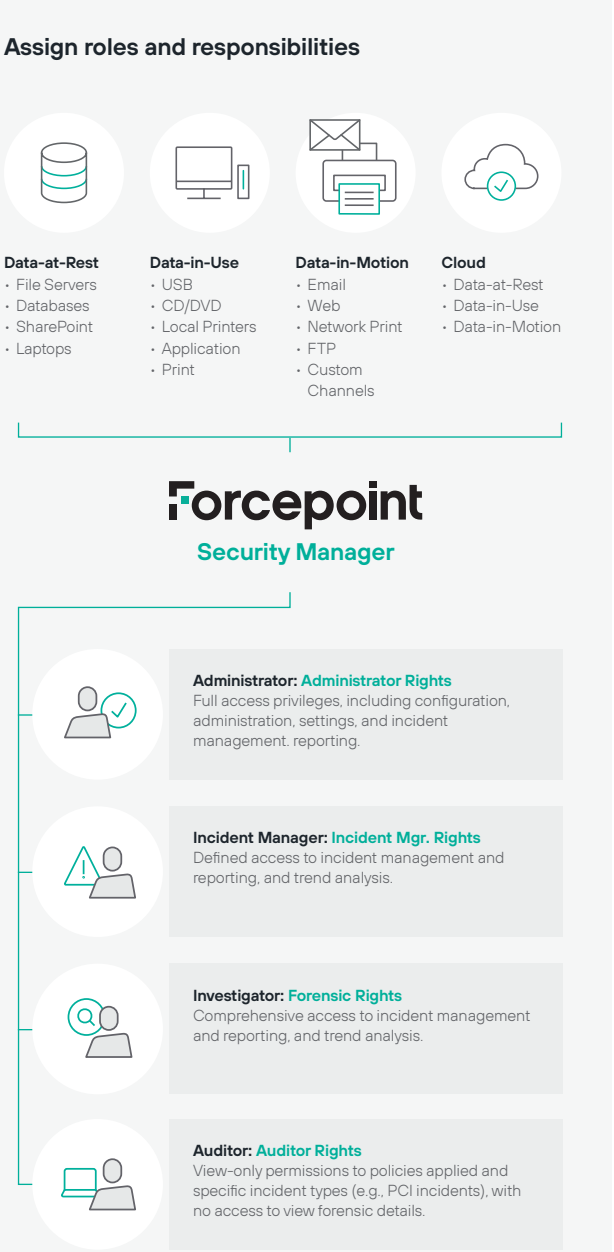


Figure 4. Assign Roles and Responsibilities

Step 2: Establish the Technical Framework

Goal: Create a baseline for data security controls to help your organization recognize normal user behavior and prevent high-impact data breaches.

Overview: 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). This audit-only approach can also be done when utilizing a Risk-adaptive DLP by setting each risk level to audit-only.

1. **Install and configure**
2. **Monitor network**
3. **Analyze results**
4. **Executive update 1**
5. **Risk mitigation activities** (e.g., activate block policies)
6. **Analyze results**
7. **Executive update 2**

Phases 4 and 5 cover reporting, ROI, and the tracking of risk reduction in more depth.

Establish the Technical Framework	Monday	Tuesday	Wednesday	Thursday	Friday
Week 1: Install / Tune / Train					
Week 2: Monitor					
Week 3: Monitor					
Week 4: Executive Update 1					
Week 5: Risk Mitigation					
Week 6: Executive Update 2					

Figure 5. Implementation Timeline - Part 1

Step 3: Expand the Coverage of DLP Controls

Goal: Implement DLP to endpoints and sanctioned cloud applications to measure and begin to reduce risk.

Overview: Now you're ready to address data-in-use and data-at-rest. During this step, you deploy DLP to endpoints and sanctioned cloud applications, monitor and analyze your data, update the executive team, and perform risk-mitigation activities much like you did in the beginning of Phase 3. The primary difference is that now you choose to respond to incidents based on the different channels and available options for data-in-use, which occurs at the endpoint and cloud applications. (You determined the incident severity and response according to the channel in Phase 2.)

For data-at-rest, the process identifies and prioritizes targets to scan, and moves any stale data to a quarantine, where your legal and compliance teams can proceed according to your organization's data retention policies. In regards to compliance, it's about cooperation—so cooperate, but at a speed that is reasonable for your organization. Remember, nobody gets a prize for coming in first.

In case you need to perform a discovery task sooner rather than later, know that you can temporarily (or permanently) increase the speed at which discovery is performed by using local discovery agents, or by setting up multiple network discovery devices.

1. **Deploy endpoints & cloud application (sanctioned) and monitor**
2. **Start discovery scans**
3. **Analyze results**
4. **Executive update 3**
5. **Risk mitigation activities**
6. **Analyze results**
7. **Executive update 4**

Expand the Coverage of DLP Controls	Monday	Tuesday	Wednesday	Thursday	Friday
Week 7: Deploy Endpoints and Cloud Application (sanctioned)					
Week 8: Endpoint and Cloud Application (sanctioned) Monitoring/Data-at-Rest					
Week 9: Endpoint and Cloud Application (sanctioned) Monitoring/ Data-at-Rest					
Week 10: Executive Update 3					
Week 11: Risk Mitigation					
Week 12: Executive Update 4					

Figure 6. Implementation Timeline - Part 2

Step 4: Integrate DLP Controls Into the Rest of the Organization

Goal: Incident management is delegated to key stakeholders from major business units.

Overview: If you haven't yet directly involved the data owners and other key stakeholders with the DLP implementation, now is the time.

In particular, the role of incident manager is best suited for the data owners, because they are liable in the event of data loss. Putting incident management in their hands eliminates the middleman and improves operational efficiency. In addition, it enables them to accurately assess their risk tolerance, and properly understand how their data assets are used by others.

During this step, have the DLP implementation team host a kickoff meeting to introduce the DLP controls to others. Follow this with training to acclimate the new team members to the incident management application. Before turning over incident management responsibilities, set a period of time during which you provide assisted incident response to get the new team members up to speed.

1. **Create and engage committee**
2. **Program update and roles**
3. **Training**
4. **Assisted incident response**
5. **Executive update 5**
6. **Incident response by committee**
7. **Executive update 6**

Integrate DLP Controls Into the Rest of the Organization	Monday	Tuesday	Wednesday	Thursday	Friday
Week 13: Selection and Notification					
Week 14: Program Update and Roles					
Week 15: Training w/ Assisted Response					
Week 16: Executive Update 5					
Week 17: Incident Response by Committee					
Week 18: Executive Update 6					

Figure 7. Implementation Timeline - Part 3

Phase 4:

Move to Proactive Security

Goal: Transition to automated protection and response for high-risk events.

Overview: Organizations typically get to proactive, automated protection and personalization in two steps. The first is moving from audit to analysis. The second is automating response. Keep in mind that in almost all cases, there's no skipping stages in this journey.

Step 1: Analysis and Alerts

Goal: Begin analyzing data and its movement within an organization to understand what happened during a data breach.

Overview: You need to move beyond audit mode to analyze how a breach occurred. For this, you need visibility into where data lives, what it's doing, and where it travels. The challenge with Big Data search tools and traditional DLP products that only offer data discovery and control features is that such tools only alert cybersecurity administrators to data breaches after the fact, and don't include robust forensics tools for analysis. They are set in audit-only mode with good intentions – to avoid disrupting legitimate business transactions – but because of this, they do not offer as much help in preventing future incidents. Organizations at this stage may be "compliant" but not secure.

This post-breach analysis can be very robust and utilize the best available forensics tools, but it is ultimately still reactive in nature. Still, organizations at this stage of their journey are able to take the lessons they learn and manually adjust their data security policies to help stop the next incident.

Step 2: Proactive Automation and Personalization of Data Security

Goal: Become fully proactive about preventing a data breach via either infiltration or exfiltration by automatically analyzing user and system behavior, blocking access and activity deemed to be a threat, and automatically adjusting policies tailored to individuals as they learn the context around exhibited behavior. A fully automated approach provides a behavioral risk score for a user in an organization and proactively tailors security to the individual based on this scoring—without getting in the way of the user. Risk scores account for the vagaries of user interaction with data, systems, and applications, and provide needed context for behavior, which help reduce false flags. Actions that represent low risk are permitted while higher-risk activities generate automated responses that range from alerts to administrators, encryption, complete blocking, and other predefined security enforcement.

This is what modern data security looks like – an adaptive, automated process that creates as little business friction as possible by stopping dangerous activity but not impeding regular users and systems with overzealous blocking. Risk-based DLP solutions are designed to empower business goals rather than acting as a brake on them, protecting an organization's people and data without impacting how people use data to do their work.

> **"Risk-based DLP solutions are designed to empower business goals rather than acting as a brake on them, protecting an organization's people and data without impacting how people use data to do their work."**

By making the leap from passive data loss prevention to risk-adaptive data security, organizations can lower the risk of brand or financial damage resulting from data breaches while leveraging behavioral intelligence to better achieve their goals.

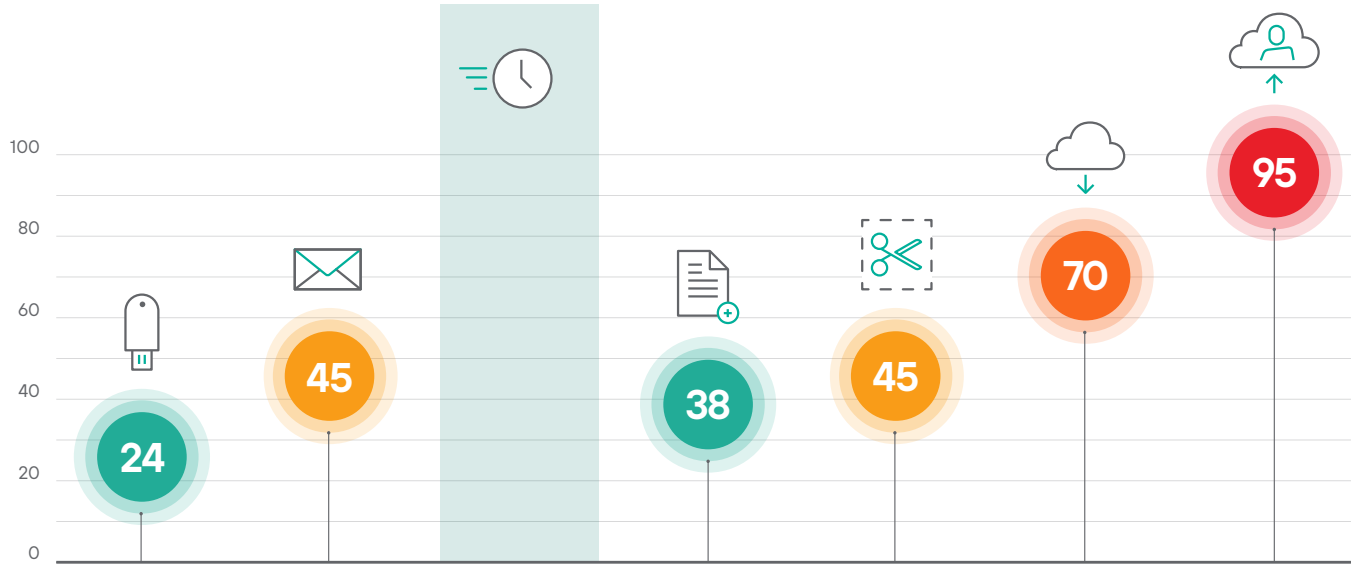


Figure 8. Showing How a User's Activity Can Increase Their Risk Score

Phase 5:
Track the Results of Risk Reduction

Goal: Show ROI by demonstrating a measurable reduction in risk.

Overview: There are two key points to add to the risk-reduction tracking process that was first mentioned in Phase 3. They are:

1. Relative incidents should be grouped 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.

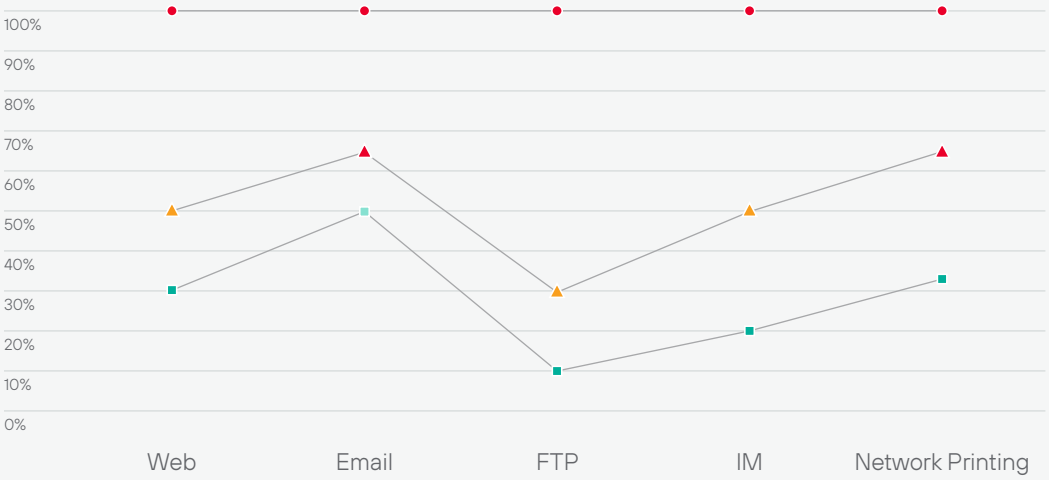
2. Maintain consistency between risk-reduction phases. To preserve the integrity of your results, the monitoring and risk-reduction periods need to be of equal length. In the beginning, we recommend two weeks to improve time-to-value and to simplify analysis. However, you are in the best position to determine what is most reasonable for your organization.

Below is an example of how grouping is applied and risk reduction is tracked. Note that there is a consistent time period, a focus on high-risk incidents, and that these incidents are grouped by their relative channel.

Risk-adaptive DLP Option: If you have decided to take a risk-adaptive approach, you'll want to 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)

Finally, when updating your executive team on the DLP process and its results, remember that less is more. Focus on the big picture as you explain your organization's high-risk vectors and outline your recommended risk-mitigation activities and the cost, benefits, and effort of each.

Likelihood of Data Loss



Marker Legend

- High
- Moderate
- Low
- Acceptable
- 30 days baseline
- 60 days
- 90 days

Number of Incidents over 90 Days

Incidents	Web	Email	FTP	IM	Network Printing
30 days baseline	200	150	50	10	45
60 days baseline	100	100	15	15	30
› 60-day risk reduction	50%	33%	70%	50%	33%
90 days baseline	60	76	5	2	15
› 90-day risk reduction	70%	49%	90%	80%	67%

Goals

- **60 days** 25% + reduction
- **90 days** 50% + reduction

Figure 9. Tracking Risk of Data Loss

Conclusion

A successful DLP implementation will not come from a new technical bell or whistle, and it cannot be racked and stacked in the data center. Instead, it will depend on your ability to:

1. Understand a DLP vendor's methodology and execution strategy. Your organization benefits by discerning how different vendors approach DLP. Doing so allows you to determine the most promising vendor methodologies for your environment, and which DLP technologies to evaluate. Considering a vendor who provides a risk-adaptive solution can add long-standing advantages to an organization, including increased efficiency and productivity. And do not forget: applying one vendor's methodology to another's technology has negative long-term implications.

2. Apply the risk formula for data loss. Once your security team understands and applies the risk formula for data loss, it can collaborate with data owners to identify and prioritize data assets. In addition, every risk-mitigation activity should be designed with the sole purpose of lowering the rate of occurrence (RO) of data loss. RO is the proper measurement for tracking risk reduction and showing the ROI for DLP controls. As a reminder: take special notice when comparing traditional DLP solutions with a DLP with risk-adaptive technology to ensure you aren't comparing false positives to real positives.

3. Apply the 80/20 rule for resource allocation. By understanding which data loss vectors pose the greatest risk of a high-impact data breach, your organization can use the 80/20 rule for allocating resources and formulate effective data protection strategies.

4. Follow the Nine Steps to DLP Success. Whether you take a traditional DLP approach or a risk-adaptive one, our nine-step process is a proven formula to implement DLP controls in a manner that is practical for your business to follow and which will deliver actionable, measurable, and risk-adaptive results.

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.

[Practical-Exec-Guide-to-DLP-Whitepaper-EN] 24SEPT2021