safetica

Your Guide to a Comprehensive DLP Strategy: Processes, Tools, and Vendors

2026

Table of Contents

Your Guide to a Comprehensive DLP Strategy: Processes, Tools, and Vendors

Data Loss Prevention (DLP) has been around since the early 2000s, pioneered by various startups that focused primarily on network-based controls to block leaks at the perimeter.

Many early adopters deployed DLP as a foundational element in their cybersecurity posture, often alongside firewalls and intrusion detection systems, to enforce policies on data in motion.

The attitude toward DLP has unfortunately shifted since those early days. Regulations such as GDPR in 2018 and CCPA in 2020 mandated stricter data handling, pushing organizations to use DLP for audit trails and reporting rather than pure threat prevention. Fines were heavy and unforgiving for non-compliance.

However, when compliance becomes more important than risk management, priorities **become misaligned**. This landscape has caused DLP to become mostly a checkbox exercise for compliance reasons.

Adding to the problem is that early forms of DLP, which relied heavily on static rules and data at rest, simply weren't adequate to deal with new business realities. Security professionals were caught in a catch-22, implementing the best solutions that existed at the time, but still being hit by fines for data breaches because DLP technology wasn't good enough yet.

In our modern times, it's possible to manage risk *and* maintain compliance when the right system is used. DLP has changed significantly over the years, and organizations should reassess their needs for DLP, as well as what a modern DLP solution might look like. The trick is to use a system that was built from the bottom up with both needs in mind.

Modern DLP incorporates behavioral analytics to detect anomalies, differing from rule-based legacy systems that often generate high false positives.

Global data volumes have reached staggering levels and will only continue to grow as the world becomes more reliant on digital data. Everything from contracts to documentation is going online, significantly increasing the potential risk of data loss.

Security leaders must evaluate current deployments against these evolutions to close gaps in protection. This would include mapping their data ecosystems, identifying exposure points, conducting risk assessments that prioritize high-value assets, incorporating user behavior into policy enforcement, and integrating it all under one system that constantly monitors data at rest and in motion.

If it sounds like a lot, it is. But it's also possible with a modern, comprehensive DLP solution.

Preparing for this new reality requires understanding what the new risk landscape looks like, what tools and processes an org should consider, and how to approach vendors.

Consider the fact that **70% of data loss occurs at the endpoint**, giving a clue as to where the greatest concentration of protective measures should be. However, the simplistic answer of "focus on endpoints" fails to consider the complex nature of data storage and data transfer. Even though data is most often lost at endpoints, the compromise leading to data loss doesn't start and end there, it often originates in a different place.

The example should make it clear why security professionals must reevaluate their current DLP practices, while also selecting tools that provide contextual insights.

Context-aware protection requires visibility across the network, cloud apps, and user behavior, not just the endpoint. This guide will go over the new DLP landscape, what effective DLP looks like, and how to become a more informed buyer when it comes to DLP vendors.

The change in the DLP landscape

The scope of where an organization's data lies has increased dramatically. A wider use of SaaS tools and third parties than ever mean data naturally gravitates toward the cloud. This has led to data sprawl and ROT (redundant, obsolete, or trivial data) and often results in organizations having too much data in too many places.

This issue is exacerbated in hybrid environments, especially if assets are continuously shifting from on-prem to cloud-based. This migration exposes data to new risks and because cloud providers handle storage, but organizations retain responsibility for security configurations, meaning insecure cloud storage providers pass on most of the risk to the organization.

Vendors, SaaS, and the wide third-party ecosystem

Organizations have increased their reliance on third-party vendors, with the average firm using 106 SaaS apps in 2024. Enterprises average 131 SaaS tools. That's only SaaS tools, not including other vendors.

106
Average number of SaaS used inside an organization

131
Average number of SaaS used inside an enterprise organization

Vendors can often access sensitive data, creating potential leak points if they lack strict controls. While teams typically audit vendor access, inconsistent standards across partners can complicate enforcement while widespread SaaS adoption and streamlined implementation may mean SaaS vendors are onboarding in days without a security team even knowing or being able to properly vet them.

Open-source code and IDEs

Open-source dev environments are another risk area. Open-source components can contain known and unknown vulnerabilities. When those components are used in development or production systems, attackers can exploit them to gain unauthorized access, potentially exfiltrating data.

An extensive study of VS Code extensions found that over 2,000 extensions (roughly 8.5% of all extensions tested) are prone to data leakage. These open-source components are especially risky as, due to their nature, threat actors can easily develop exploit kits or attacks targeting them. By identifying a widely used component, attackers can target thousands of companies through a single vulnerability.

Remote and hybrid work policies

Remote and hybrid work policies have decentralized data access. Employees access systems from various locations and devices, increasing endpoint risk. Multiple locations and global workforces can also fragment data management, further leading to data sprawl.

A widely distributed workforce can also be a nightmare for compliance. Different countries have different laws on where data can be stored or processed, leading to complications when data is accessed from someone outside of those jurisdictions.

Different teams might have specific preferences for collaboration tools, such as a preference for WhatsApp in LATAM versus Slack or Teams in the USA, which complicate a standardized DLP process and overall data visibility.

The above elements make DLP even more difficult than it already was, resulting in a landscape where **over 50% of businesses have suffered business disruption** due to data loss, while only 35% consider that they have a “mature” DLP program in place.

Why effective DLP requires complete visibility

88% of all data loss events were caused by 1% of users in 2024, highlighting how imperative it is to secure *every* device and *every* point of potential loss. All an infiltrator needs is a single weak spot to gain enough access to cause significant damage.

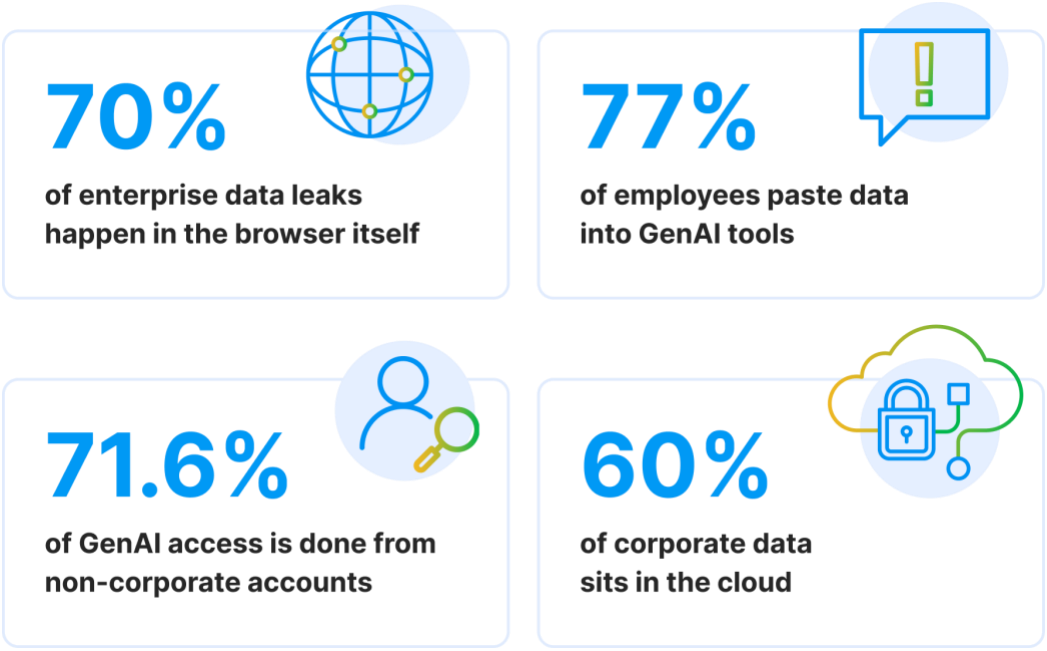
Visibility is difficult in a disparate data environment

Considering the new data landscape, it’s an understatement to say that visibility is a difficult and complex challenge. Data now lives across endpoints, SaaS apps, IaaS

platforms, third-party tools, collaboration platforms, personal devices, multiple employee-owned devices, IoT devices, and cloud storage.

Traditional perimeter-based visibility tools can't track or enforce policies consistently across all these layers and employees might use unauthorized services to share files or make their job easier, often without IT's knowledge.

The statistics related to an organization's lack of visibility are eye-opening.



Security departments weren't originally designed to track data across the kinds of environments they now operate in and have struggled to adapt in this new normal. Visibility breaks down because tools aren't integrated, data doesn't have boundaries, and most classification is shallow. What passes as "classification" is often just keyword matching or tagging a file as "confidential" once and assuming it stays that way, even when it's copied or shared.

Even with excellent classification, enforcing strong data hygiene can be a struggle. In many organizations, the data layer itself is fragmented and detached from the systems

meant to observe it. Until security professionals rethink where and how they instrument their data usage, comprehensive visibility will keep failing.

Consolidating data security is its own challenge

DLP is only effective if it covers all an organization's data which can be a challenge in the case of fragmented storage, which leads to incomplete protection.

Modern enterprises suffer from data sprawl because of the issues outlined earlier, with data assets increasingly spread across numerous systems and storage locations. Traditional DLP solutions were designed for older, simpler infrastructures such as on-premises servers, managed endpoints, and corporate networks. As work has moved to SaaS apps, cloud storage, browser-based tools, hybrid clouds, and remote work, those legacy assumptions no longer hold.

Because of that shift, much of a company's sensitive data now resides or moves in channels that traditional DLP can't monitor. For example, employees might use SaaS applications or web tools to edit, upload, or share sensitive files. Legacy DLP solutions located solely at endpoint boundaries often miss these channels entirely.

This fragmentation creates blind spots where data leaks can happen outside the scope of traditional DLP coverage resulting in partial DLP deployment, such as only on endpoints or on-prem systems. It's no surprise that this yields in only partial protection, requiring security leaders to look for more comprehensive solutions, if they can identify these limitations in the first place.

Insider risk management

Insider risk management (IRM) is a critical extension of any comprehensive DLP strategy. Unlike external threats, insider risks originate from individuals who already have access to internal systems or credentials. This includes employees, contractors, and partners, whether their actions are intentional or because of negligence.

Human factors dominate data loss events. According to Verizon's 2024 Data Breach Investigations Report, **68% of data breaches involve a non-malicious human element**, such as falling for a social engineering scam.

IRM is a required extension of DLP's scope. DLP without insider risk awareness fails to account for the most common causes of data exposure. Comprehensive DLP strategies must include tools and processes capable of identifying and responding to insider risk rapidly.

What to prioritize when it comes to effective DLP: A process guide

Effective DLP starts with prioritization, otherwise efforts will be too broad and diluted.

> "Organizations often imagine that securing data via DLP solutions is only a matter of configuring a tool, and all will be well," says Ján Lakatoš, Director of Product at Safetica. "In reality, it entails integrating a whole new security process into their work environment and finding a balance between strict security and business enablement. And to reach an equilibrium that's nearly impossible because so many variables are at play."

Start with visibility

Visibility is the foundation of any effective DLP strategy. Without it, organizations can't discover where sensitive data resides, how it moves, or who's interacting with it.

Effective visibility requires continuous data discovery across all environments. It must also be identity-aware, linking data access to specific users and devices. This is essential for both real-time policy enforcement and post-incident investigation.

No DLP system can apply controls or detect misuse without first knowing what data exists and how it's stored.

Implement effective monitoring

Once visibility is established, monitoring enables the organization to track data access and movement in real time. Without monitoring, visibility remains passive, which might be useful for audits, but isn't useful for incident prevention or detection.

Effective monitoring captures both where the data is and how it behaves. It determines *who* accessed it, *what* actions they took, and whether those actions align with company policy. Ideally, monitoring would extend to sanctioned and unsanctioned tools, including browser-based tools and SaaS platforms.

Monitoring should be contextual because logging that a file was accessed isn't enough. The system should capture who accessed it, from where, on what device, and whether it was shared or exfiltrated. This context is critical for risk detection as it's the only way to feed more sophisticated DLP tools that can detect indicators of compromises or insider risk attack via anomalous behavior patterns rather than user-based rules or signatures.

Without continuous, multi-layered monitoring, DLP controls can't respond to real-world threats or enforce policies dynamically.

Prioritize consolidation and a simplified data architecture

Fragmented environments create blind spots and slow down reaction times, making consolidation necessary. A unified data architecture provides clear visibility into all data interaction. This clarity strengthens detection accuracy and reduces the number of potential failure points.

Having multiple rules across platforms regarding data classification or retention policies or a disparate policy based on disparate databases or environments can lead to conflicts. Consolidation and standardization ensure these rules are applied uniformly and removes configuration gaps.

This results in faster Incident Response because there's only a single place to check logs and adjust controls. Consolidation should also include an audit that ensures your data isn't stored on public-facing or unsecured databases and ensures you haven't missed areas where your data might live that you missed. Make it a priority to consolidate by reducing scattered data sources into a single, authoritative point of information so decisions and actions can be taken quickly and with clarity on the situation.

Don't overwhelm your team

Vendor complexity and too many tools can significantly increase the chances of data loss. Legacy tools make it challenging to implement effective DLP, which is why **78% of organizations** struggled with DLP tooling in 2024.

This isn't only true for your organization but for your team as well. Understaffing and skills gaps are widespread. Nearly all CISOs report that their teams are understaffed, and **90% of cybersecurity professionals** report skills gaps in their teams. However, too many security leaders see this gap and think more tools are the answer.

This can result in burnout for your team and too much complexity, which would impact your team's effectiveness. Focus on automation to handle routine tasks. Limit tool sprawl to essential integrations. This increases capacity while preventing overload.

Don't add to the overload of an already strained team by adding tool complexity to the mix.

A primer on DLP tools

Plenty of DLP tools exist, and it's the cybersecurity leader's job to be an informed consumer, otherwise you might be purchasing a tool that's a poor fit for your company, your security team, and your risk profile.

Not all tools are created equally, and they don't serve all companies equally. Security leaders should look for tools that facilitate proactivity and align with the priorities you've identified as part of your DLP security strategy.

Below, we provide a list of which types of tools will help you build an effective DLP tech stack.

Discovery and classification tools

Discovery and classification tools scan an organization's data, find where information is stored, and sort it into meaningful categories. Their core purpose is to make hidden data across all locations (cloud, on-prem, third party) visible and label it properly so that proper protection can be applied.

These tools look across computers, servers, cloud storage, email systems, shared folders, and sometimes even old archives. They identify things like customer records, payment details, personal identities, internal documents, and intellectual property.

Once identified, they apply clear tags to the data that allows security rules to be enforced automatically, such as blocking downloads or preventing external sharing.

MDM (mobile device management)
Mobile Device Management (MDM) tools create a controlled environment for any phone, tablet, or even a laptop that touches business information.

These tools give an organization the power to set rules for how devices behave, no matter where those devices are located. This is central to data loss prevention because the biggest risk with mobile devices is that they move and connect to multiple networks daily. They leave offices, connect to unsafe networks, get misplaced, and store sensitive files that can easily fall into the wrong hands if the device is stolen.

An MDM solution solves several problems at once, such as:

- Making sure each device has strong protection at the lock screen.
- Separating personal content from work content so employees can use their devices without exposing business files.
- Controlling which apps can open or copy work documents.
- Tracking devices so they can be recovered or wiped.
- Allowing remote removal of work data.
- Providing one central view of device activity and giving early warning if a device (or data on the device) is at risk.

Insider Risk Management (IRM)
IRM tools focus on preventing data loss that comes from people inside the organization. This includes employees, contractors, and anyone else with legitimate access to systems.

These tools watch for actions that could lead to data being taken or misused. They look for patterns of behavior that suggest rising risk, such as unusually large downloads, attempts to bypass restrictions, copying large amounts of files, accessing data at odd hours, or moving information to non-employer owned locations.

Anomalous behavior doesn't always mean a bad intention, but the risk is still there. In the worst-case scenario, a user account may have been compromised and in the best-case

scenario, employer data is falling outside the scope of visibility for an org. The result doesn't change. The risk of data loss and a data breach is still present.

Insider threats don't always have to be malicious, and they often aren't. However, innocent negligence or poor security hygiene doesn't reduce the need to address IR.

Insider risk management is often treated as separate from data loss tools because it focuses on human behavior instead of file movements or device rules. However, it should be considered with data loss prevention because many incidents happen even when traditional controls are in place. By complementing the two, you can achieve a more secure environment and organization.

Where vendors can help with DLP

These steps should provide you with a strong starting point on how to implement a modern, effective DLP strategy.

> "It's important to understand what the goals and or expectations are," says Miloš Blata, Director of Sales Engineering at Safetica. "Is it data classification, data protection, secure perimeter checks, discovering where the Data-in-Rest resides, meeting a regulatory compliance or standard, knowing what is going on in general, logging and effectively managing it (ideally using AI), a combination of some of those, or everything combined? Once this 0th step is clarified, managing a DLP configuration becomes much simpler."

As you approach your vendors, consider the above and ask yourself the following questions.

- Is the vendor addressing a key priority outlined here?
- Is it increasing management or complexity? Or is it increasing efficiency and lowering operational burdens?
- When considering the entire scope of your DLP strategy, how much of it does this vendor impact? If it's too small, you'll likely have to find additional vendors.
- Does the vendor deliver integrated DLP and IRM in a single platform, or will you need to manage multiple tools and integrations?

These questions will help you assess what vendors will make the most impact on your organization.

As you continue to build out your DLP strategy, remember to consider the fundamentals. A sound strategy is one that covers all aspects of data protection but also incorporates the new risks posed by a widespread digital footprint and the ever-evolving threat insiders risks pose. However, a strong foundation is enough to ensure your DLP strategy can adapt to these new threats and risks. Take the time to build that foundation, then you're ready to find the right tools and vendor.