REPORT

The DLP Disconnect

Why Decades of DLP Investment Still Aren't Paying Off

cyberhaven

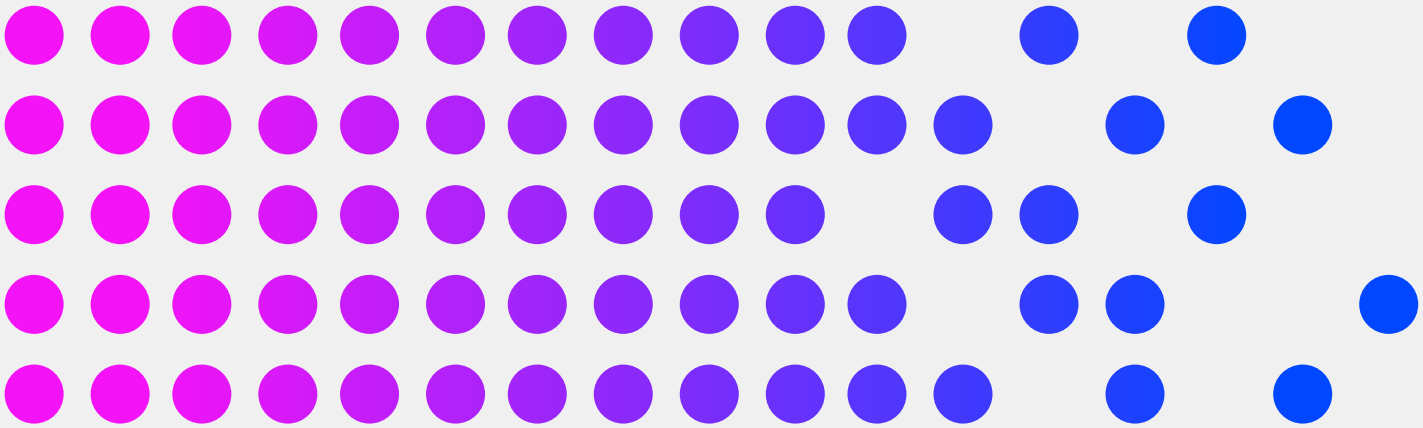
INTRODUCTION

The financial and reputational costs of data breaches continue to escalate year after year, putting immense pressure on organizations to safeguard their most sensitive information. Beyond the immediate expenses of incident response, regulatory fines, and legal settlements, the hidden costs of lost productivity, customer churn, and long-term brand damage often exceed what's visible on balance sheets.

Despite decades of investment in data loss prevention (DLP) technologies, organizations continue to struggle with effectively protecting sensitive information. Ultimately, the costs and exposure risks are increasing while the technology is struggling to provide effective protection. The DLP Disconnect is an exploratory research report that investigates the persistent pain points faced by security leaders and practitioners using legacy DLP solutions.

We surveyed 300 information security leaders – including DLP engineers and analysts, data privacy officers, SOC managers, VPs of IT, directors of IT and data security, and information security managers – to understand the operational, technical, and strategic challenges they encounter.

Data sprawl is being led by AI & data fragmentation



Sensitive data now lives in countless formats and systems, from cloud apps and collaboration platforms to personal devices. Each new tool and workflow creates another pocket of data that security teams have to monitor, classify, and protect. As fragmentation accelerates, it fuels sprawl, making it harder to know where critical data resides, who has access, and how it's being used.

77% say increasing data sprawl means that breaches are inevitable.

Security leaders admit that the rapid sprawl of data across devices, cloud platforms, and collaboration tools has made breaches feel inevitable. Sensitive data is constantly moving, copied, and shared in ways that traditional security tools struggle to track. As a result, organizations are facing an uphill battle where the sheer volume and dispersion of data erodes visibility and makes containment nearly impossible.

66% said that relying on legacy DLP to contain data breaches is like putting your finger in a dam to stop the flow.

The metaphor reflects a harsh reality. At best, traditional DLP tools can slow leakage temporarily, but they lack the precision, context, and adaptability needed to truly contain threats. As data pours across cloud services, SaaS platforms, and collaboration tools, legacy DLP becomes less of a safeguard and more of a fragile patch.

71% say legacy DLP can't keep track of the volume and variety of data in their organization

Traditional rule-based systems weren't built for this level of complexity, leaving gaps in visibility and control. As data grows in both scale and diversity, the shortcomings of legacy DLP become more pronounced, making it harder for security teams to identify, monitor, and protect what matters most.

73% feel its likely that data has been exfiltrated that they don't yet know about.

This sobering reality underscores the visibility gap that plagues traditional DLP tools, which often only catch threats after the damage is done. With data scattered across cloud services, endpoints, and unmanaged collaboration channels, many organizations simply don't have the monitoring or context needed to spot subtle patterns of exfiltration in real time.

The disconnect between promise and performance

Traditional DLP solutions rely on outdated methods of classification and rigid policies that can't scale to the volume, velocity, and variety of data being created and shared. As a result, they miss critical risks, drown teams in noise, and provide only a fragmented view of where sensitive information is going.

40%

of respondents say they understand exactly where exfiltrated data has come from, and where it has been

Equally alarming...

45%

understand exactly who has interacted with exfiltrated data from source to egress

These gaps reveal how blind legacy DLP leaves organizations when it comes to understanding the full chain of data exposure. Without visibility into the movement and handling of sensitive data, investigations stall, accountability is blurred, and the true scope of a breach often remains unknown. In practice, this means organizations are left guessing at the impact of exfiltration long after the damage is done.

Now we wanted to understand where exactly these vulnerabilities existed. When asked if their legacy DLP solution allows them to reliably identify and prevent data exfiltration via any of the following methods, the results were alarming.

35%	Printing sensitive documents
34%	Importing to or exporting from public cloud applications (e.g.,SharePoint, Google Drive, Dropbox)
30%	Compressed or encrypted files (e.g., ZIP files)

29%	Encrypted messaging applications (e.g., WhatsApp)
29%	Inputting sensitive data into AI tools (e.g., ChatGPT, DeepSeek)
25%	Sending via AirDrop
24%	Sensitive non-text content (e.g., screengrabs or image files)

Fewer than half of respondents expressed confidence that their tools could consistently do the job in any one scenario. This lack of trust highlights a fundamental weakness: legacy DLP was built for simpler environments with predictable data flows. If security teams can't depend on their DLP to stop exfiltration when it matters most, the entire strategy creates a false sense of security.

But it gets worse. Not only are legacy DLP tools failing to deliver on their promise, they are forcing organizations to disable protection to avoid performance issues or unnecessary friction for users. 60% of respondents say employees are always trying to bypass our DLP, putting the organization at risk. They've admitted that:

44%	We've disabled the inspection of archive files (e.g., zip files)
42%	We've disabled the inspection of large files
39%	We've disabled DLP for the marketing department
34%	We've disabled DLP for the HR department
32%	We've disabled DLP for the finance department

Performance slowdowns, endless false positives, and user friction make strict enforcement nearly impossible. So instead of stopping data loss, teams end up loosening controls to reduce the noise. The result is a dangerous paradox. The tools meant to protect sensitive data are often sidelined, leaving organizations exposed at the moments they need defense most.

78% are frustrated with provider updates

Even when vendors attempt to fix problems or add new capabilities, the process is rarely smooth. Updates often introduce new bugs, break existing policies, or require lengthy retuning that disrupts daily operations. Instead of solving issues, patches can create more work for already overburdened security teams.

Legacy DLP is security that slows you down

Instead of enabling the business to move quickly and safely, outdated tools get in the way. Organizations are dealing with friction at every level – employees frustrated by unnecessary roadblocks, and security teams buried under manual tasks. While these tools may promise protection, in practice they act more like speed bumps that hinder productivity without meaningfully reducing risk.

65%

say their team is overwhelmed with benign DLP alerts

Instead of highlighting the few signals that truly matter, legacy tools flood security teams with noise. This nonstop barrage not only burns time and resources, it desensitizes analysts to the point where real risks can slip through unnoticed. The constant triage of false alarms leaves security teams exhausted, reactive, and unable to focus on proactive strategies, turning DLP into a source of distraction rather than protection.

51% (on average)
of alerts are false positives

For many, DLP has shifted from being a protective measure to a daily operational burden that slows the business down while still leaving sensitive data at risk. Instead of empowering security teams, legacy tools often create more work. Respondents said they spend 34% of their time on administrative DLP tasks, including tweaking manual rulesets and policies, jumping between tools to protect multiple channels of egress.

63% say that over-zealous DLP is hindering employees from doing their jobs

Security leaders admit that over-zealous DLP policies are actively hindering employees from doing their jobs. Legacy tools force a tradeoff between security and usability, often defaulting to blocking legitimate activity. These heavy-handed controls don't just frustrate employees; they create workarounds that introduce even greater risk.

41%

of respondents feel this blocks legitimate business activities

For security teams, this creates a constant cycle of wasted effort as they chase down non-issues, draining time and resources that should be spent on real threats. The net effect is a system that undermines both security and productivity, creating friction without delivering meaningful protection. But the friction doesn't stop with false positives. Security teams are also burdened with unforeseen administrative issues.

61% say, every day I wake up to a raft of new issues caused by our clunky DLP

Reimagine DLP with Cyberhaven

It's safe to say that we've proven just how ineffective legacy DLP solutions are. These tools rely heavily on rigid, manually defined rules and patterns, which forces organizations to predict every possible scenario in advance. In practice, this means endless debates over classification, constant policy tuning, and a high risk of blind spots when data doesn't fit neatly into predefined categories. As evidence, *67% feel DLP puts too much pressure on us to define what is and isn't sensitive data.*

And beyond the complex user experience, performance is equally subpar. The kernel-based model that many of the traditional vendors use was designed for a different era, when monitoring endpoints at the operating system level seemed like the most effective way to control data. Today, that approach is not only outdated but also increasingly unstable, prone to compatibility issues, performance slowdowns, and operational risk every time an OS update rolls out.

63%

feel Kernel-based DLP solutions haven't been relevant since 2019

52%

are planning to move to a solution that doesn't need kernel-access

Security leaders are signaling a clear shift. The future of data protection lies in approaches that deliver visibility and control without relying on fragile, kernel-level hooks. That's where Cyberhaven comes in.

Cyberhaven takes a fundamentally different approach. We've reimagined DLP with AI-powered automation and streamlined controls, so you finally get real protection that's easy to manage. Our AI-native platform doesn't just inspect content: it traces its entire journey. See where data lives, comes from, how it changed, and who interacted with it.

By tracing data flows from the moment sensitive information is created through every copy, share, and transfer, Cyberhaven delivers the visibility and precision legacy tools can't match. The result is protection that actually works—without the noise, the friction, or the endless policy tuning. By partnering with Cyberhaven, you can achieve up to:

5x

Faster Incident Investigation

NAVAN

2x

Faster Incident Resolution

Largest Customer
(Enterprise AI Tech)

90%

Fewer False Positives

motorola

We deliver:

Data lineage
Our data lineage technology maps the full journey of sensitive data, from creation to every movement, transformation, and fragmentation.

AI-based content intelligence
Cyberhaven uses AI to classify sensitive data the moment it's created and continuously updates that classification as the data evolves.

Autonomous risk detection
Linea AI Detection Agent applies predictive AI using proprietary Large Lineage Models (LLiM) to instantly detect risky activity.

Accelerated investigations
Linea AI Analyst Agent launches deep investigations, gathers evidence, and delivers clear reports with next steps to resolve issues faster.

Ready to see how modern data protection is supposed to work?

Sign up for a demo and experience the difference for yourself.

cyberhaven

Cyberhaven.com