FORTINET

2025

DATA SECURITY REPORT

Are Traditional DLP Solutions a Barrier to Preventing Data Loss?

Research by

Cybersecurity INSIDERS

AUGUST 2025

Executive Summary

Data security is no longer just about deploying tools to identify and prevent the outflow of sensitive information. It now requires a deep understanding of how sensitive data is created, stored, accessed, and used—and how users may, intentionally or unintentionally, put it at risk.

Today's efforts have also shifted away from purely technology-led strategies. With 64% of organizations now operating a formal data governance program and another 23% in the process of building one, it's clear that businesses are embracing programmatic approaches that integrate governance, policies, processes, and tools into a comprehensive data protection strategy. At the same time, security teams are securing stronger budget commitments to improve their ability to keep sensitive data from leaving the organization.

Yet despite these positive trends, 77% of organizations reported an insider-related incident in the past 18 months, with 58% experiencing six or more. Why are so many still struggling to protect sensitive data?

The findings suggest a surprising culprit: the very Data Loss Prevention (DLP) tools designed to stop data loss may now be holding organizations back. Insider-driven risk has become one of the most urgent and complex challenges in enterprise security. As data flows increasingly through users, cloud applications, AI tools, and hybrid work environments, traditional perimeter-based, content-only DLP tools can't keep up. These legacy systems were built to block outflows—not to understand the nuanced behaviors and contexts that expose sensitive data in modern workflows.

Security leaders are recognizing that modern data security requires more than enforcement—it demands visibility into the data, the activities, and the people putting that data at risk. Yet most organizations are still relying on traditional DLP tools that weren't designed for today's decentralized environments, unstructured data flows, or user-driven cloud and AI usage.

Based on a 2025 survey of 883 IT and cybersecurity professionals, this report explores the current state of enterprise data protection, where legacy DLP tools are falling short, and the capabilities security leaders are prioritizing as they modernize their data protection programs.

Key Findings Include:

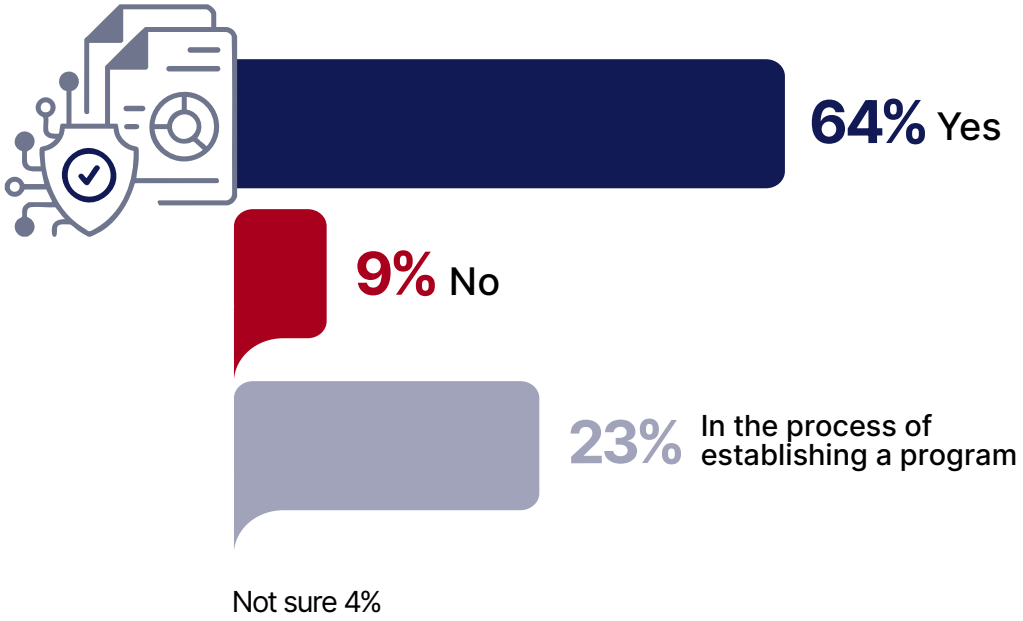
- **Sensitive data exposure is persistent**
  77% of organizations experienced insider-related data loss in the past 18 months, and 58% reported six or more incidents - many stemming from routine user activity rather than malicious intent.
- **Most incidents are unintentional, not malicious**
  49% of organizations experienced a data loss incident caused by negligent or careless employees versus only 16% involved confirmed malicious intent. Another 12% could not determine the cause, and 20% did not experience a data loss incident.
- **The business impact is material**
  45% reported financial or revenue loss, and 41% estimated damages between $1 million and $10 million for their most significant incident over the past 18 months. Only 8% said the impact was negligible.
- **Visibility into data use remains a major blind spot**
  72% of organizations say they can't see how users interact with sensitive data across endpoints, cloud services, or SaaS platforms.
- **Security leaders are prioritizing behavioral context and real-time visibility**
  The top capabilities sought in next-gen solutions are real-time behavioral analytics (66%), day one data visibility (61%), and control over shadow AI and SaaS tools (52%).

As a result, forward-leaning organizations are moving to integrated, behavior-driven platforms that provide unified visibility, adapt to risks in real time, and deliver insight - not just enforcement. This report examines the current state of that transition and highlights the practices, capabilities, and priorities shaping the future of enterprise data protection.

Strategy First, Technology and Tactics Second

64% of security professionals report that their organizations have a data protection or data governance program in place, while another 23% say their organizations are in the process of establishing one. This is a clear indication that organizations have adopted a programmatic approach to their data security efforts, as opposed to a technology-led approach that oversimplifies the complexities involved in securing sensitive data and relies too heavily on traditional DLP tools.

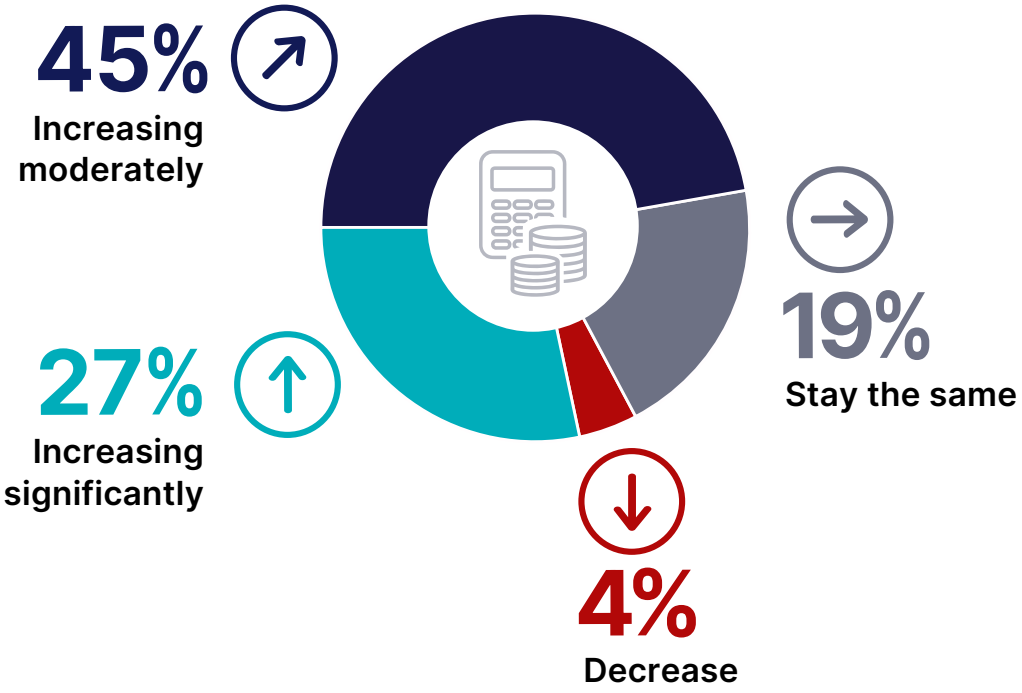
Does your organization have a formal data protection or data governance program in place for the protection of sensitive data?



Funding Isn't a Barrier to Better Data Security

Data protection is receiving real investment. 72% of organizations report that their budgets for insider risk or data protection are increasing, and 27% have experienced significant growth over the past year. This is good news, showing that security teams and executives at organizations at large are taking risks to sensitive data more seriously.

Which best describes your current insider risk or data protection budget trend?



Unknown / not disclosed 5%

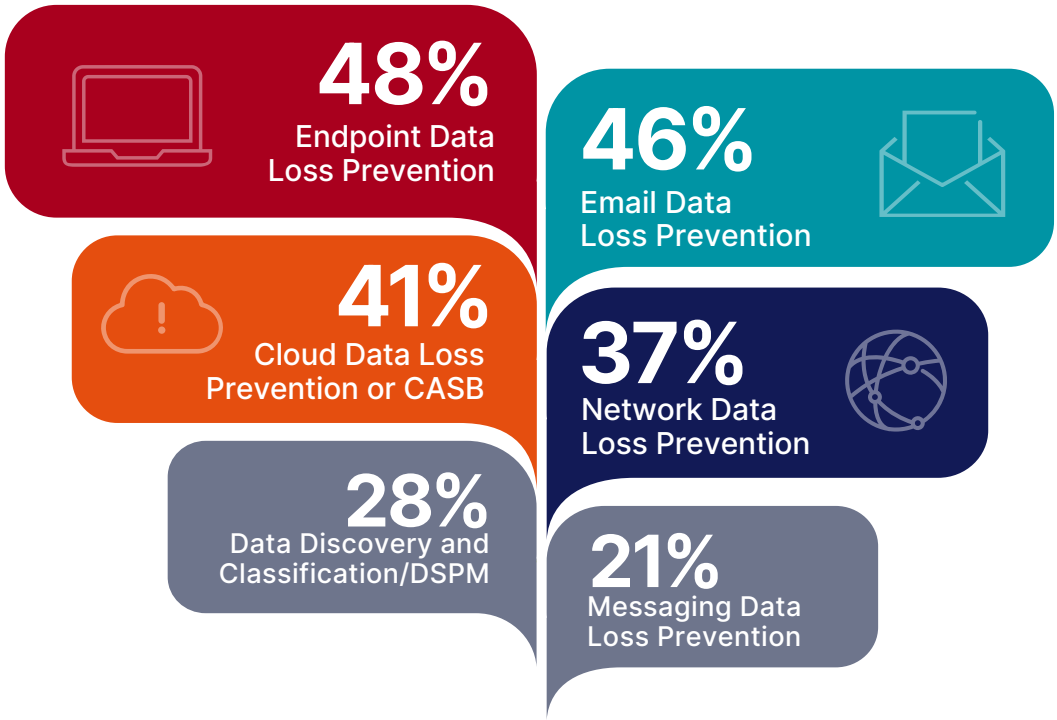
Fragmented Tools - Partial Protection

Even in organizations investing heavily in data protection, tool coverage often remains inconsistent and incomplete. According to the survey data, 48% use endpoint DLP, 46% have email DLP, and 41% deploy Cloud DLP or CASB. Network DLP adoption trails at 37%, and just 28% use DSPM or data classification tools to understand what they're trying to protect. Surprisingly, no single technology garnered more than 50% usage across organizations.

This fractured landscape creates gaps in enforcement and blind spots in visibility. A user might be blocked from emailing a sensitive file, but nothing prevents them from uploading it to personal cloud storage, dragging it into a Microsoft Teams chat, or pasting it into an AI tool. Each channel operates in isolation and policies don't follow the user or the data.

Security teams don't need more alerts—they need visibility and clarity: visibility into business data flows, the ability to connect individual events into patterns, and those patterns into risk. With today's fragmented toolsets, where legacy DLP often sits at the center, organizations end up without the visibility or clarity they need.

Which of the following technologies/tools does your organization utilize today?



Most Security Teams Can't See What Matters Most

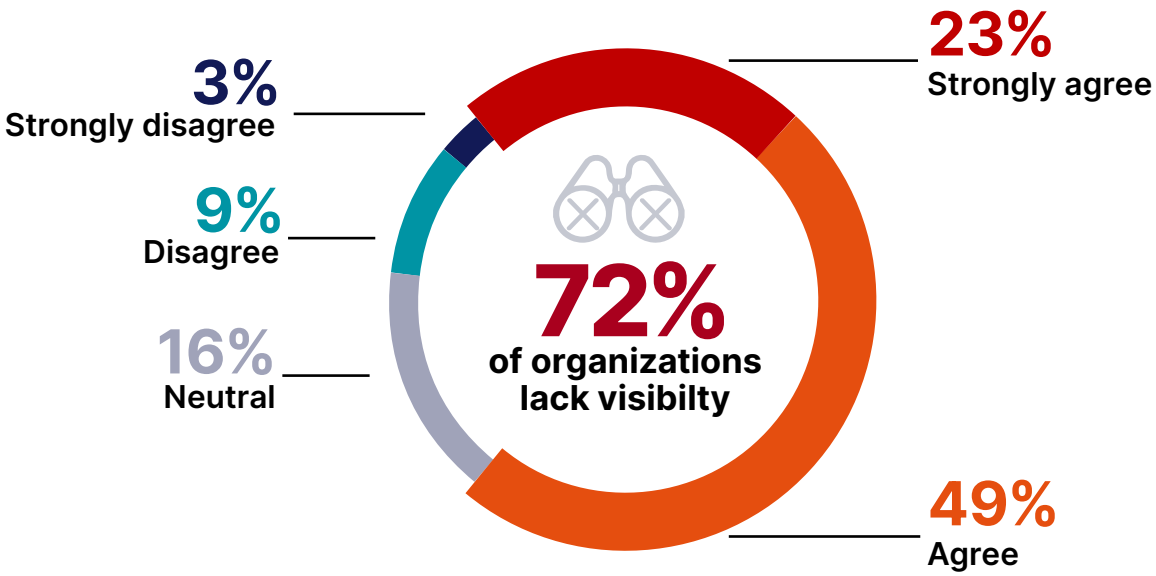
When it comes to sensitive data, most organizations are flying blind. 72% of respondents agree that they lack visibility into how users interact with sensitive data across endpoints and cloud applications.

The reality is that productivity is increasingly tied to the constant creation, iteration, use, and manipulation of sensitive data by users in your organization. Financial analysts model quarterly reports. Sales teams pull full customer exports. Healthcare professionals retrieve PHI in real time. Engineers create new product designs. Sensitive data is created or accessed constantly by users trying to do their jobs—often across cloud apps, unmanaged endpoints, or AI tools. As a result, sensitive data is being created and replicated at an increasingly rapid pace, with the risk of exposure directly tied to the growing prevalence of that data in users' hands.

Without understanding who is accessing what data, how often, and in what context, security teams can't distinguish between routine activity and emerging risk. Legacy DLP tools may log data movement, but they don't explain why it happened, who triggered it, or whether it was normal. That leaves teams reacting to alerts, rather than understanding the underlying behaviors.

The resulting lack of visibility and clarity means that sensitive data is being put at risk. As the following charts reflect, the exposure and loss of sensitive data is having a material impact on organizations.

Do you lack visibility into how users interact with sensitive data across endpoints and cloud applications?

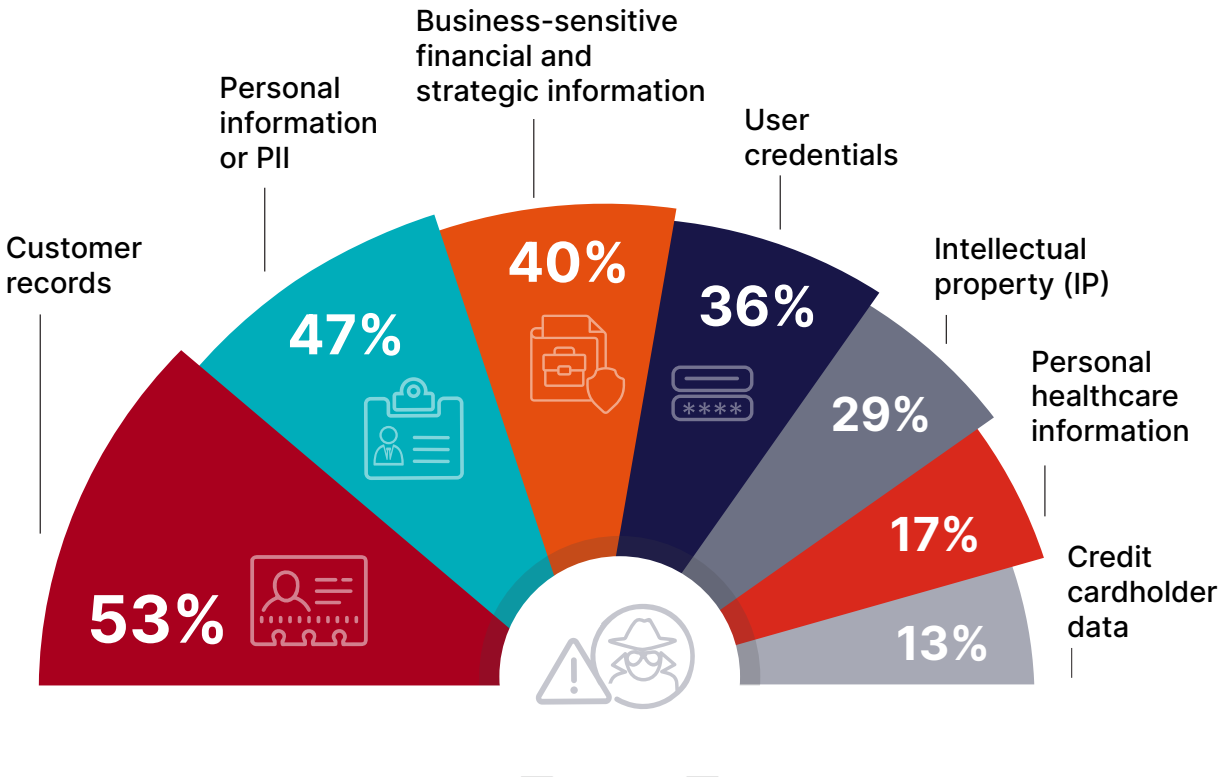


The Sensitive Data That's Getting Out

Data Loss Prevention isn't just about stopping known sensitive fields like PII or cardholder data—it's about protecting the information and intellectual property that powers the business. In the most significant data loss incidents reported by survey respondents, the top categories of exposed data were customer records (53%) and personally identifiable information (47%)—the very assets that trigger regulatory scrutiny and compliance risk.

Just behind them: business-sensitive content such as financials, strategic plans, and product roadmaps (40%), user credentials (36%), and intellectual property (29%). While IP ranks lower overall, that reflects its relevance to only certain sectors—not its value. In manufacturing, biotech, and design-driven industries, leaked IP can have a decade-long tail of financial damage. One stolen or leaked design file, R&D dataset, or proprietary algorithm can erode a company's competitive position before the breach is even detected.

What type of sensitive data was involved in the most significant incident?



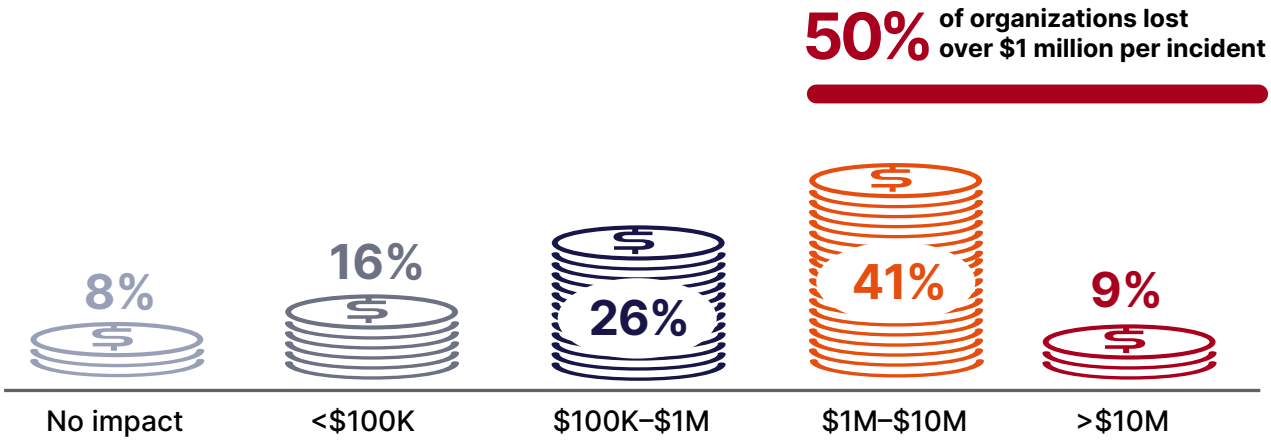
The Real Cost of Data Exposure

The consequences of sensitive data exposure don't end with the security team—they ripple across the business with real and measurable impact. In their most serious incidents, 45% of organizations reported revenue or financial loss, 43% cited reputational damage, and 39% experienced operational disruption. Legal and regulatory fallout affected 36%, while 29% reported loss of intellectual property—a critical issue in sectors where leaked designs or proprietary code can permanently damage competitive position.

But beyond categories of impact, the scale of financial loss is staggering. 76% of organizations said their most significant incident cost them more than $100,000, and 41% reported losses between $1 million and $10 million. Another 9% said the toll exceeded $10 million.

These numbers dismantle any illusion that data loss is just a policy violation or compliance event. In nearly every case, the fallout spans revenue, brand equity, and business continuity. Only 8% said their most serious incident had no meaningful impact, meaning nearly nine out of ten suffered consequences they could quantify.

Can you estimate the financial impact of a data exposure incident.



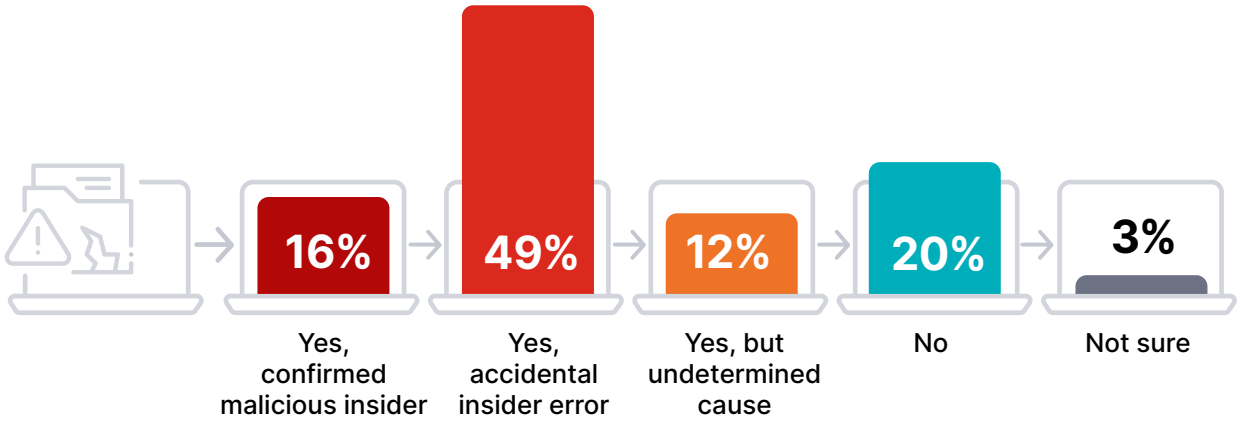
Data Loss Is Becoming Routine

The exposure of sensitive data from within the organization is no longer an isolated incident—it's a constant undercurrent in modern environments. 77% of organizations confirmed at least one insider-related data loss incident in the past 18 months. When asked about the frequency of incidents, 29% reported detecting between one and five incidents, and 37% reported experiencing between six and 20 incidents.

Over time, this erodes confidence in controls and increases the risk that truly harmful behavior gets missed entirely. That's why forward-looking organizations are moving from static enforcement to real-time, behavior-aware visibility—not just to reduce false positives, but to identify patterns before they turn into headlines.

Has your organization experienced a data loss incident involving an insider in the past 18 months?

77% **of organizations experienced an insider-related data loss incident in the past 18 months**



Traditional DLP as a Barrier to Preventing Data Loss

Most organizations have deployed DLP, but what looks like protection on paper often fails in practice. Tools block known patterns but lack visibility into how data is used, by whom, and in what context.

47% of respondents say their DLP is effective in preventing data loss, yet only 33% report immediate visibility into usage, and just 27% can see which users are putting data at risk. Visibility into SaaS and shadow tools is even worse: just 22% say they can monitor it effectively.

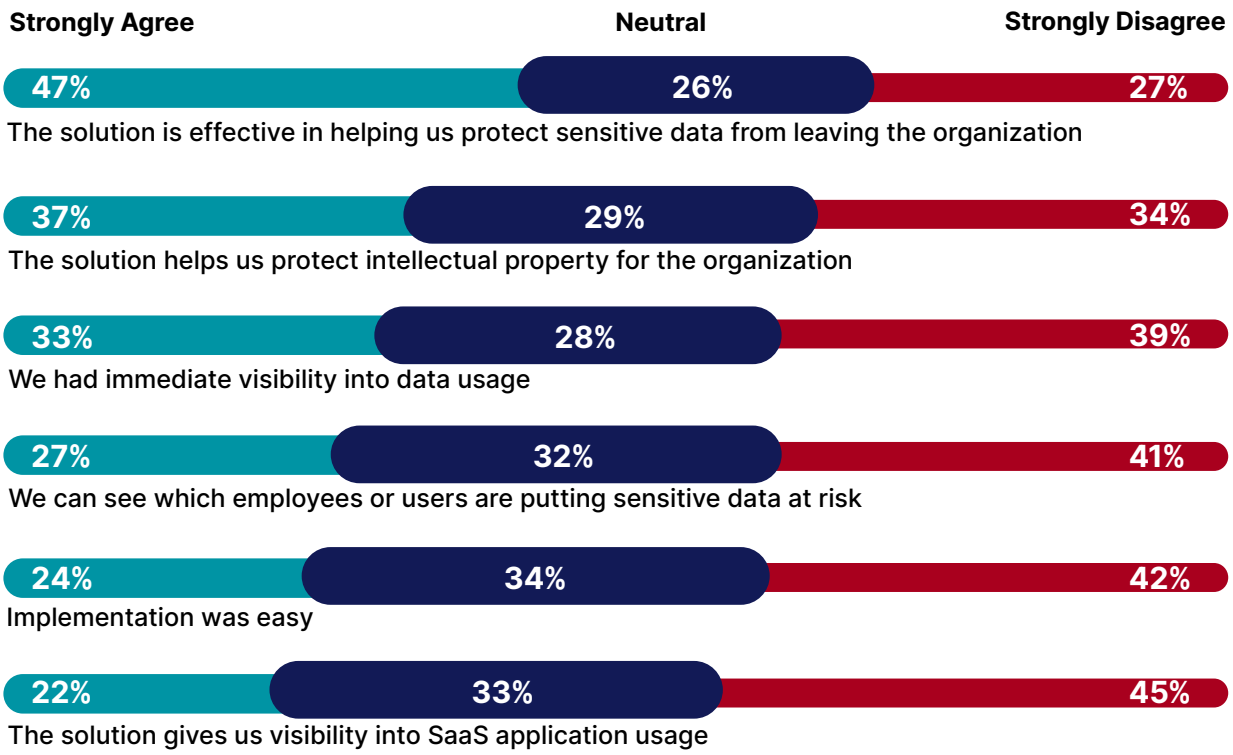
Even intellectual property, a high-value target in industries like tech and manufacturing, is poorly protected with only 37% strongly agreeing their solution helps.

This reflects a core limitation of traditional DLP: it flags violations but can't connect user behavior, intent, and risk signals into meaningful insight. That leaves security teams drowning in alerts but blind to the story behind them.

Deployment pain compounds the issue. Only 24% said implementation was easy, undermining time-to-value in already strained environments.

The result? Most DLP programs enforce rules but lack the context to enforce them intelligently. Without behavior-aware telemetry and integrated visibility, real protection remains out of reach.

If your organization currently uses a Data Loss Prevention solution, how would you rate the following?



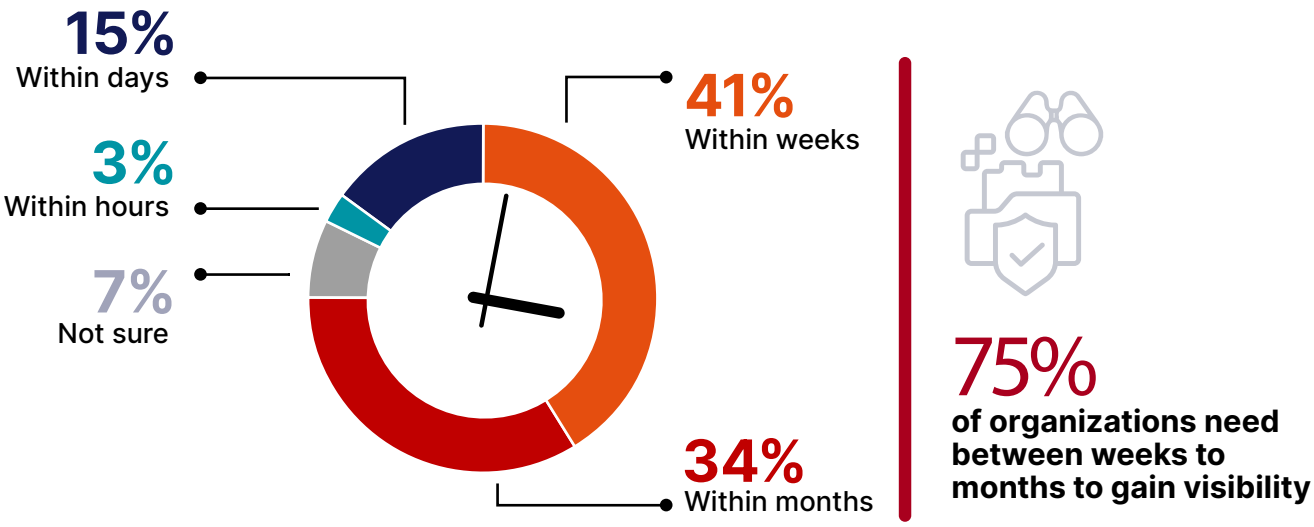
Slow to Start - Slow to Protect

Most organizations don't get meaningful insight from their DLP deployment until long after rollout. Only 3% said they gained visibility into data usage within hours, and just 15% within days. For the vast majority (75%) it took weeks or months after implementation to see useful results.

This isn't just a tuning delay; it reflects deeper architectural limitations. Legacy DLP tools depend on complex policy configuration, siloed integrations, and static enforcement models. That means long ramp-up times, high operational overhead, and critical gaps in visibility during early deployment—all while risky behaviors are already happening.

Modern DLP must deliver usable insight from day one—across cloud, endpoint, and user behavior—not weeks into deployment.

For your most recent DLP implementation, how long did it take for your organization to gain visibility into data usage and exposure, and glean meaningful insights?



What Security Leaders Want from DLP

Security teams are clear on what today's DLP tools lack and what next-gen platforms must deliver. The top priorities signal a shift from static enforcement to real-time, behavior-aware insight:

- 66% prioritize behavioral analytics, pointing to the need for tools that detect intent, not just violations.
- 61% want "day one" visibility across environments, reflecting frustration with long deployments and blind spots.
- 52% cite shadow AI and SaaS control as essential, signaling that AI oversight is now a frontline capability, not a niche add-on.

Other priorities round out the shift: tracking data from origin to destination (38%), privacy-aware monitoring (33%), in-the-moment user coaching (29%), and forensics and case management, features which were once considered advanced, now expected.

What emerges is a clear picture: teams want context, not just alerts. Insight, not overhead, and solutions that explain what happened, why it happened, and what to do next—without needing months of tuning.

The comparison below illustrates how legacy DLP tools fall short of these priorities, and how next-gen solutions are closing the gap through integrated Data Loss Prevention, insider risk management, and visibility into SaaS application usage.

Traditional DLP Solutions	vs.	Next-Gen DLP Solutions
Business Use Case(s): DLP only		**Business Use Case(s):** DLP + IRM
Data Protection: Sensitive		**Data Protection:** Sensitive + IP
Deployment: On-prem or cloud-based		**Deployment:** Cloud-native + multi-tenant
Time-to-Value: Weeks to months		**Time-to-Value:** Days
Visibility: Policies required for visibility		**Visibility:** Policy-less, immediate visibility
Insights into SaaS and AI: Limited		**Insights into SaaS and AI:** Yes
Inspection: Content		**Inspection:** Content, data origin, context
Behavioral Analytics: None		**Behavioral Analytics:** Integrated
Incident Fidelity: Single Alert		**Incident Fidelity:** Sequenced alerts with data lineage
Forensics: Files		**Forensics:** Clipboards, files, screenshots
Case Management: None		**Case Management:** Integrated with AI assistant

From Enforcement to Insight: A New Mandate for Data Protection

Across every data point in this report, one theme is clear: the most important risk indicator is no longer the file, it's the behavior around it. Security teams don't just need to know what left the organization; they need to understand who moved it, why, and whether it matters.

This is why next-generation data protection strategies are moving beyond static controls and toward real-time, behavior-aware visibility. Rather than preemptively blocking every unknown action, organizations want tools that calculate risk, adapt enforcement, and guide response with context.

They're no longer seeking more rules but more clarity. The next generation of DLP isn't just about prevention; it's about visibility, context, and intent, giving defenders the insight they need to act with confidence.

The following best practices reflect that shift, offering practical guidance for building modern, intelligence-driven data protection programs that align with today's environments and tomorrow's threats.

Best Practices for Modern Data Loss Prevention

To meet today's data protection challenges, organizations must move beyond static, policy-heavy DLP and adopt a modern approach—one built on real-time visibility, behavioral context, and unified control across endpoints, cloud, SaaS, and AI tools. The following best practices reflect that shift and provide a practical blueprint for implementing next-generation DLP:

1

START WITH DAY-ONE VISIBILITY

75% of organizations wait weeks or months to gain insight from DLP tools. That delay creates a critical blind spot during rollout. Modern solutions must provide immediate telemetry across cloud apps, endpoints, and AI tools - without requiring complex policy setup first.

2

MONITOR BEHAVIOR, NOT JUST VIOLATIONS

66% of leaders prioritize behavioral analytics, yet few can identify which users are putting data at risk. DLP must move beyond rule—breaking to detect deviations from normal usage patterns, including frequency, timing, and method of access.

3

CORRELATE IDENTITY, ACCESS, AND ACTIVITY

Static rules can't assess intent. By linking user identity, data access patterns, and contextual risk signals, organizations can distinguish between routine activity and high-risk behavior, enabling a more precise response and fewer false positivies.

4

PROTECT THE ENTIRE DATA JOURNEY ACROSS CHANNELS

Email is no longer the primary data exit path. Only 12% feel prepared for AI exposure and many lack coverage for personal cloud, SaaS apps, or unmanaged endpoints. Modern DLP must follow the data wherever it flows—not stop at the perimeter.

5

USE AI TO CUT THROUGH THE NOISE

AI shouldn't just generate more alerts but enhance prioritization, triage, and root-cause investigation. The most effective platforms use AI to sequence user behavior, detect anomalies, and spotlight what actually matters.

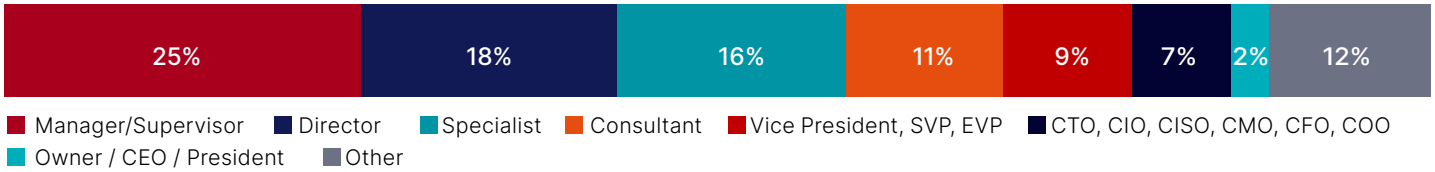
Demographics & Methodology

This report is based on a 2025 survey of 883 IT and cybersecurity professionals, conducted by Cybersecurity Insiders in partnership with Fortinet. Respondents represented a range of industries, company sizes, and roles—including CISOs, security architects, SOC leaders, and data protection professionals.

The survey focused on key challenges in Data Loss Prevention, including visibility gaps, implementation maturity, and priorities for next-generation solutions. Responses were self-reported and collected via structured multiple-choice questions.

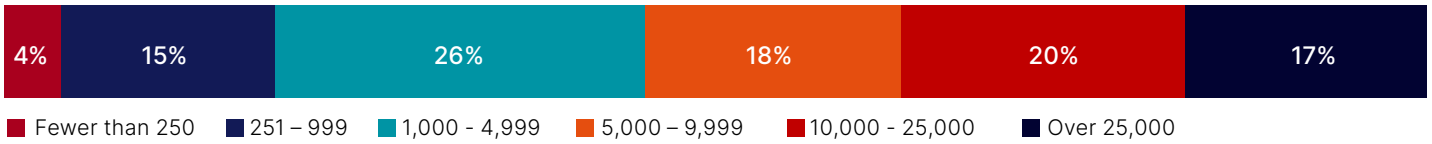
With 883 qualified responses, the survey has a margin of error of ±3.3% at a 95% confidence level, offering a statistically meaningful snapshot of current enterprise data protection practices and perceptions.

CAREER LEVEL

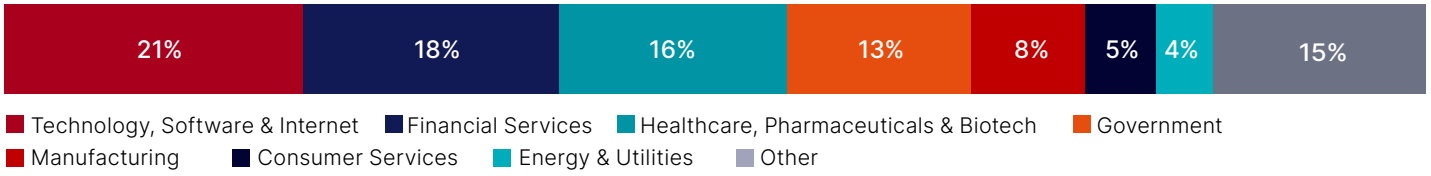


DEPARTMENT

COMPANY SIZE



INDUSTRY



Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, applications, multi-cloud, or edge environments. Fortinet ranks #1 as a security company, with more than 800,000 clients who trust their solutions and services to protect their businesses.

www.fortinet.com

Cybersecurity
INSIDERS

STRATEGIC INSIGHT FOR CYBERSECURITY LEADERS

Cybersecurity Insiders delivers evidence-backed insights that empower security leaders to make informed, strategic decisions. Backed by over a decade of research and a global network of 600,000+ cybersecurity professionals, we provide actionable intelligence to help leaders navigate emerging threats, evaluate new technologies, and shape forward-looking strategies with confidence.

For cybersecurity vendors, we turn research into results — delivering credibility, visibility, and demand through high-impact formats such as:

- Data-powered market reports that establish thought leadership,
- Webinars that build trust with buyers through credible, expert-led narratives,
- CISO guides that showcase best practices,
- Product reviews that independently validate solutions,
- Thought leadership articles that educate buyers, and
- Award programs that elevate brand reputation.

By combining this content with built-in distribution, we help brands earn trust, amplify awareness, and drive demand in a crowded cybersecurity market.

For more information visit

cybersecurity-insiders.com