

The Business Value of Cyera



Jennifer Glenn
Research Director,
Information and Data Security, IDC



Megan Szurley
Business Value Manager,
Business Value Strategy Practice, IDC

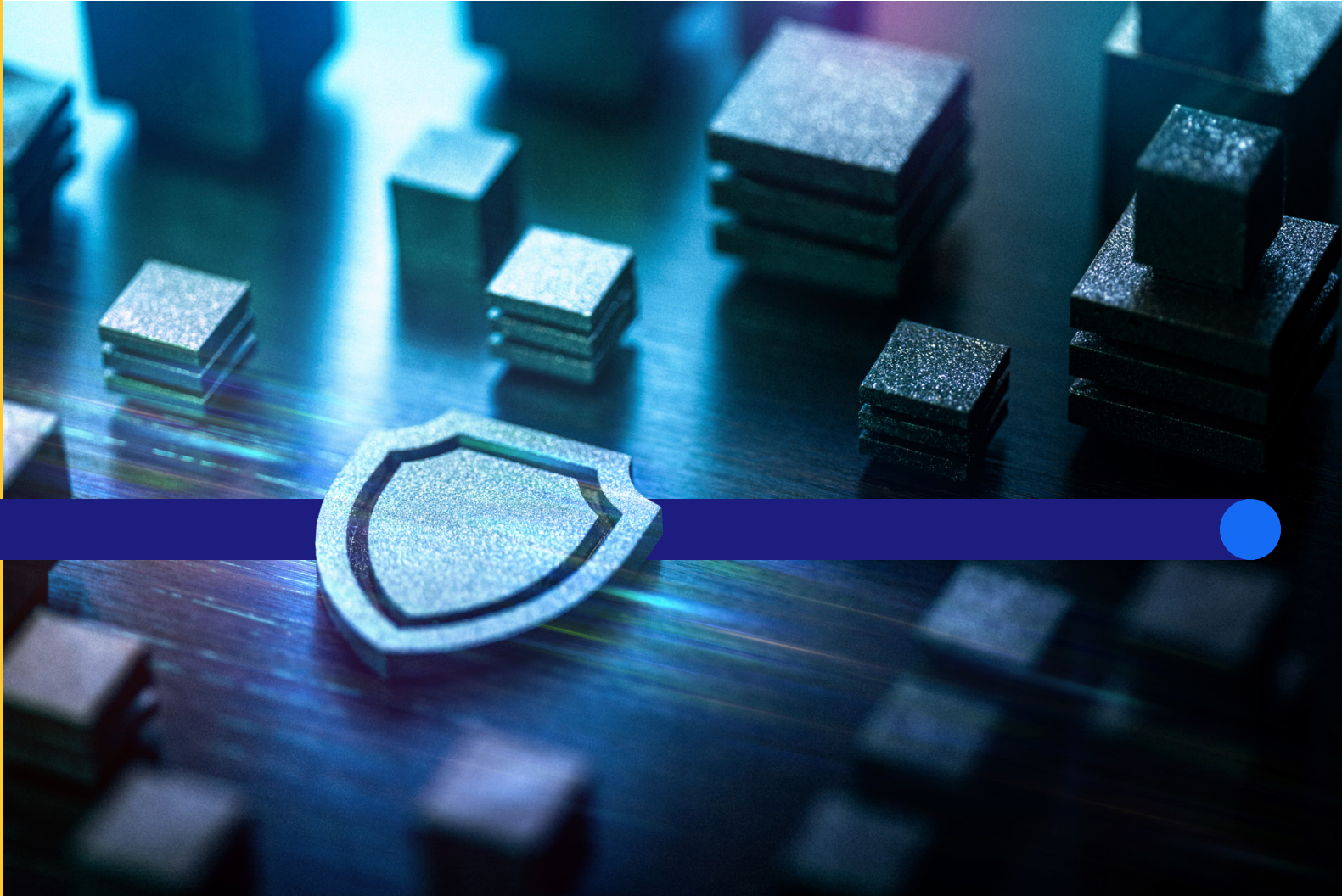


Table of Contents



Click any title to navigate directly to that page.

Business Value Highlights	3
Executive Summary	4
Situation Overview	6
Cyera Overview	7
The Business Value of Cyera	9
Study Firmographics	9
Choice and Use of Cyera	10
Business Value and Benefits of Cyera	13
Reducing IT Costs Through Consolidation and Deduplication	16
Improved Security Team Capabilities and Efficiency	17
Strengthening Data Governance and Reducing Risk	23
Governing Data Access for Safe AI Adoption	28
ROI Summary	29
Challenges and Opportunities	30
Challenges	30
Opportunities	31
Conclusion	32
Appendix A: Methodology	33
Appendix B: Supplemental Quotes	35
About the IDC Analysts	36

Business Value Highlights

Click each [→](#) to jump to related content. Use "Return to Highlights" in the page header to get back here.

78% more data threats identified and remediated



441% three-year ROI



4.5-month payback period



\$3.3 million average annual benefit per organization



99% more shadow data visible and classified



88% quicker to detect data threats



68% more actionable information



51% more efficient security teams



Executive Summary

Many organizations rely on data security posture management (DSPM) and data loss prevention (DLP) to protect sensitive data. DSPM technology is designed to discover and classify sensitive and/or confidential information across a business. This helps organizations to measure risk and assist in remediation across the cloud, software as a service (SaaS) applications, and on-premises environments. Armed with contextual information about what data they have, where that data resides, and who has access to it, security teams can use DLP to control how that data is used, shared, and moved. In theory, these two technologies offer organizations the visibility to understand their data risks and the ability to enforce policy controls that reduce that risk.

DLP has been a staple of enterprise security implementations for decades, and organizations invested heavily to customize and maintain policies, often with limited success. DSPM emerged in the early 2020s. Its context and discovery capabilities made it a natural complement to existing DLP investments. The value was so clear that nearly every major DLP vendor quickly built or acquired DSPM technology with the intent to integrate it with their products. However, even now, when both technologies are likely to sit within the same vendor portfolio, they are still often run as separate tools. This disconnectedness leaves teams to manually piece together context and wade through a high volume of false positives.

As organizations connect more sensitive data to AI systems, this fragmentation becomes a bigger liability. AI agents, which IDC predicts will be in use at half of all enterprises by 2027, can query, move, and act on data far faster than any person. They also inherit the same access and exposure gaps that already exist from fragmented DSPM and DLP implementations, just at machine speed. This makes getting full value from data security investments reliant on how well DSPM and DLP work together.

IDC interviewed customers using Cyera to understand the impact of its unified approach to DSPM and DLP across their environments.

Based on in-depth interviews with nine organizations, IDC calculates that these customers achieved benefits worth an annual average of \$3.3 million on a per-organization basis (\$31,000 per 100 TB of data) and a three-year ROI of 441%, with a payback period of 4.5 months, by:

- **Gaining comprehensive visibility and context into sensitive data:**
Before Cyera, interviewed organizations relied on manual inventories and siloed tools that covered only a fraction of their environments, leaving teams without a clear understanding of their data risk.

Cyera provided a continuous, contextualized view of sensitive data across cloud, SaaS, and on-premises systems, giving security teams not just visibility into where sensitive data lived but the accuracy and information needed, such as how broadly it was accessed, to prioritize and act on real risk.

- **Classifying data with high accuracy:**

Incumbent tools generated high volumes of false-positive alerts that forced security teams to spend most of their time re-validating findings rather than acting on them. Cyera's context-aware, AI-powered classification allowed teams to trust their results (without manual tuning to understand their business data) and respond to real issues immediately.

- **Significantly reducing manual effort and operational costs:**

Cyera replaced labor-intensive manual processes with automated, continuous coverage across the data environment. Scoping data environments, writing and tuning detection rules, and validating false positives can now be optimized, allowing security and governance teams to operate more efficiently. This enabled organizations to redeploy staff to higher-value work or avoid planned headcount growth.

- **Reducing exposure and accelerating threat detection:**

Interviewed organizations reduced the volume of sensitive data left over-permissioned or publicly exposed, shrinking the attack surface available to attackers. Cyera's continuous monitoring also caught threats that previous tools had missed entirely, allowing teams to detect and respond to incidents closer to when they occurred.

- **Governing data access for safe AI adoption:**

As study participants deployed generative AI tools, Cyera helped security teams understand which sensitive data was accessible to AI systems and remediate over-permissioned access before it became a risk. Organizations also used Cyera to detect unauthorized use of consumer AI tools, gaining clearer visibility into where corporate data was being shared externally.

As an insurance organization stated, *"We went from 28,000 false positives to 0 with Cyera; false positives have been completely eliminated."*

Situation Overview

AI is driving significant changes in how enterprises manage their data. That data now lives everywhere within the business, across multi-cloud infrastructure, SaaS applications, and on-premises systems and increasingly within the AI tools employees use in their day-to-day work. This sprawl has outpaced most organizations' ability to see, classify, and control it, leaving security and governance teams working from an incomplete and often outdated picture of risk.

For years, most of the security response to this sprawl focused on visibility. Organizations looked for ways to find and lock down sensitive data. This generated a lot of business disruption and lowered confidence in the data security discipline. The greater risk facing most organizations today is ensuring sensitive and confidential information remains secure but not too locked down to be used effectively in the AI initiatives that the organization is pushing. Visibility is still a critical foundation for securing data, but it's only a small piece of the solution. Organizations need accurate classification and business context around data access and use to create and enforce security policy more effectively. The businesses that get secure, well-governed data into AI systems faster will out-innovate those that don't. The data security conversation has shifted from *"how do we block this data from leaving the premises?"* to *"how do we free this data for use, safely?"*

Autonomous AI agents raise the stakes further. Where a generative AI chatbot might expose a document or excerpt with sensitive information, an agent acting on a user's behalf can touch far more data with less human oversight. This is exposing the limits of guardrails built for an earlier generation of data risk. Static classification rules, point-in-time access reviews, and DLP policies tuned for email and file shares were not designed to keep pace with AI agents that make split-second decisions about what data to use and how.

Buyer expectations are shifting as well. Now data security practitioners are looking for multi-use tools that offer end-to-end model trust, where discovery, classification, access, and usage can be verified before autonomy is granted. Meeting that bar requires more than data inventory. It needs continuous classification, accurate permission enforcement, and demonstrable trust before data is exposed to an AI model or agent.

Together, these dynamics are redefining enterprise data priorities, from point solutions addressing narrow visibility use cases toward platforms capable of continuously discovering, classifying, and governing data, so that it can be confidently and safely put to work across human and AI-driven processes.

Cyera Overview

Cyera, which Yotam Segev and Tamar Bar-Ilan founded in 2021, is a vendor of unified data and AI security. The founders' goal was to address the visibility gaps left by traditional data security tools. The company announced a \$600 million round of funding on June 10, 2026, at a \$12 billion valuation. This brings the company's total funding raised to over \$2 billion.

This investment is being used to extend the capabilities of its existing platform, which is designed to protect data across its entire life cycle.

For customers, this offers several benefits, including:

- **Faster deployment:**

Cyera is designed to be deployed without installing agents or standing up customer-managed infrastructure. It offers continuous scanning across SaaS, IaaS, DBaaS, and on-premises environments at petabyte scale. For customers, this translates to faster deployment. Customers in this study reported an average deployment time of 2.7 months in year one, considerably faster than the legacy tools and manual processes they had previously relied on.

- **Improved classification accuracy:**

Cyera's AI-native classification engine is designed to automatically identify sensitive, proprietary, regulated, and shadow data across structured and unstructured environments. It is designed to learn how each organization creates and uses that data over time to generate more precise alerts. Study participants reported that this accuracy drove a 57% reduction in false-positive alerts and a 47% reduction in overall alert noise. A telecommunications organization reported its classification accuracy rising from roughly 70% to about 95% after implementing Cyera.

- **Enhanced risk prioritization:**

Cyera is designed to correlate content, sensitivity, identity, access, usage, exposure, and ownership into a single, continuously updated model so that risk is pre-prioritized by business impact. Customers reported a 66% improvement in their ability to prioritize risk, using this added context to focus first on the exposures most likely to matter rather than treating every alert with equal urgency.



Cyera provides us with faster identification of over-permissioned paths and a more defensible way of prioritizing the remediation. It has also reduced our time spent hunting for any data risks and classification.”

Pharmaceutical organization

- **Unified DSPM and DLP:**

Cyera created its platform to operate its DSPM and DLP as a single system.

The visibility and classification generated by DSPM are designed to inform where and how DLP protections are applied. One customer said, *“Cyera helps security in three ways. First, it gives us visibility across all environments. Second, that visibility gives us the ability to label and classify data so we can apply additional protections. Third, we can stack DLP capabilities on the data we now have visibility into.”*

- **Improved efficiency:**

Cyera is designed with workflows that assist with investigation, prioritization, policy tuning, and remediation. This, combined with high-accuracy classification and consolidated visibility, gives security teams the information to work quickly. Study participants reported a 78% increase in threats identified and remediated and 47% less time to resolve or remediate alerts.

Rounding out its product portfolio is Cyera’s DataWatcher, which uses its own experts to operationalize the program, tuning policy, assessing materiality, and delivering 24 x 7 breach response so that posture doesn’t decay after deployment the way it does when no one owns keeping it current.

Since this research was conducted, Cyera has continued to expand its platform.

In August 2026, Cyera announced the availability of Agent Guardian. This capability is available via the same data security and AI platform as Cyera DSPM and Omni DLP and is designed to secure AI applications and agents. It works by discovering AI agents and AI assets across the environment and maps them to the identities, tools, connections, and sensitive data they can reach. It includes real-time guardrails with the intention to reduce the risk of inappropriate access or unsafe actions before they occur. Agent Guardian uses Cyera’s DSPM classification and identity context to know that an agent exists, what sensitive data it can reach, how it may use that data, its intent, and where controls are needed.

In August 2026, Cyera acquired Oasis Security and is rapidly integrating its non-human identity capabilities into its platform. The integration is intended to help customers see the sensitivity and residency of their data mapped directly to the human and non-human identities that can access and use it. This information will be available in the unified view with Cyera DSPM and Omni DLP. The company also plans to extend this integration further with the intent to help teams continuously verify whether that access and usage remains appropriate as organizational conditions change and get flagged when it isn’t. Cyera is a vendor of unified data and AI security. Its platform is designed to protect data across its entire life cycle.

The Business Value of Cyera

Study Firmographics

To quantify the business value of Cyera, IDC conducted in-depth interviews with nine organizations actively using the platform to discover, classify, and govern sensitive data. The study explored each organization's Cyera deployment in detail, covering the selection process and implementation through day-to-day operations. Participants were asked detailed quantitative and qualitative questions about their environments before and after deployment, the outcomes they observed, and the features they relied on most.

Table 1 (below) presents the firmographics of the interviewed organizations. Participants averaged 36,393 employees and \$20.8 billion in annual revenue, with an average of 328 IT and cybersecurity staff supporting 686 business applications. The organizations were headquartered in the United States and Canada and represented the aerospace, financial services, healthcare, insurance, manufacturing, pharmaceutical, and telecommunications industries.

Table 1
Firmographics of Interviewed Organizations

Firmographics	Average	Median	Minimum	Maximum
Number of employees	36,393	4,000	500	165,000
Number of total IT/cybersecurity staff	328	88	5	1,200
Total number of business applications	686	175	20	4,000
Annual revenue	\$20.8B	\$2.5B	\$225.0M	\$125.0B
Countries	The United States (8), Canada (1)			
Industries	Aerospace, Financial Services, Healthcare, Insurance (2), Manufacturing (2), Pharmaceutical, Telecommunications			

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Choice and Use of Cyera

Interviewed organizations adopted Cyera in response to fragmented, inconsistent visibility into where their sensitive data lived and who could access it. Most had relied on manual data inventories, regular-expression-based classification tools, or point solutions that covered only part of their multi-cloud, SaaS, and on-premises environments. For organizations managing large volumes of structured and unstructured data across many business applications and cloud infrastructure types, the inability to consistently locate and classify sensitive information had become a significant security and compliance risk. As data volumes grew and AI adoption accelerated, prior tools increasingly left organizations unable to answer basic questions about where sensitive data resided and how it was being used. Cyera was selected in part because of its ability to discover and classify data with materially higher accuracy than regex-driven tools and to deploy quickly using APIs rather than new infrastructure.

Study participants described their reasons for selecting Cyera:

Multi-cloud data sprawl (Manufacturing):

"Some of the challenges we wanted to solve with Cyera included managing multiple data sources across our multi-cloud environment so we could use AI for a competitive advantage, despite the constant cybersecurity risk of having that data spread across different silos. We also wanted better risk assessment of our databases' vulnerabilities, since our biggest challenge was managing data sprawl across the enterprise and protecting our unstructured data."

Centralized data risk view (Pharmaceutical):

"We selected Cyera because we needed a faster, more complete way to understand where sensitive data lived, who had access to it, and how it was being used across cloud, SaaS, and on-prem environments. Our highest priority was addressing the risks related to that data. The challenge wasn't a lack of security tools in general; it was that our view of data risk was fragmented, sometimes nonexistent, or simply not working. Cyera brought a centralized view of that data and all the surrounding information."

API-based deployment (Manufacturing):

"We chose Cyera for its ability to discover and classify our structured and unstructured data across multiple types of infrastructure and because we could operationalize it quickly using APIs and credentials instead of installing software and standing up a platform."

Holistic export control security (Aerospace):

"For Cyera in particular, the biggest benefit is having that holistic data security posture management across our entire ecosystem. As a defense contractor, we have to identify, mark, control, and share our export control data, including ITAR, EAR, and CUI, appropriately."

Better accuracy and integration (Insurance):

"We wanted something driven by more than regular expressions. Many established vendors we looked at were still mostly regex-driven, which felt like old-fashioned data loss prevention, while newer vendors, including Cyera, offered far more accurate classification. We also needed a vendor that would integrate well with our platforms, including immediate integration with our existing Microsoft tools and our email. Cyera was first to market with Office 365 Exchange Outlook integration, which mattered a lot given how email driven our insurance brokerage business is, and that was a huge differentiator for them."

Scalable, accurate data scanning (Telecommunications):

"We selected Cyera because we needed to scan for sensitive data at scale and at a much higher accuracy rate than our previous tool provided. That tool was labor-intensive, relying on roughly 30 to 35 employees and contractors to do the work."

Ability to close a data governance gap (Financial Services):

"We've struggled for years to get our arms around our data and understand where our critical and sensitive data lies. We're an old company with decades of accumulated data spread across file servers, databases, cloud environments, and Office 365, and we never had a solution to identify where our critical data lives, which is a core part of any strong security program. We felt there was a gap there, and a periodic gap assessment of our security program later identified data governance as an area we needed to strengthen. It wasn't until one of our auditors suggested we enhance our data governance program that it freed up the budget for me to start investigating Cyera."

Table 2 (next page) reflects the scale and complexity of the environments Cyera secures for interviewed organizations. Most notably, participants managed an average of 10,534 TB of data, the majority of it (68%) unstructured, the type of data legacy tools struggle most to discover and classify. AI adoption was already well underway across these organizations, with an average of 4,234 employees actively using 17 different AI tools or platforms, supporting more than half (52%) of company revenue.

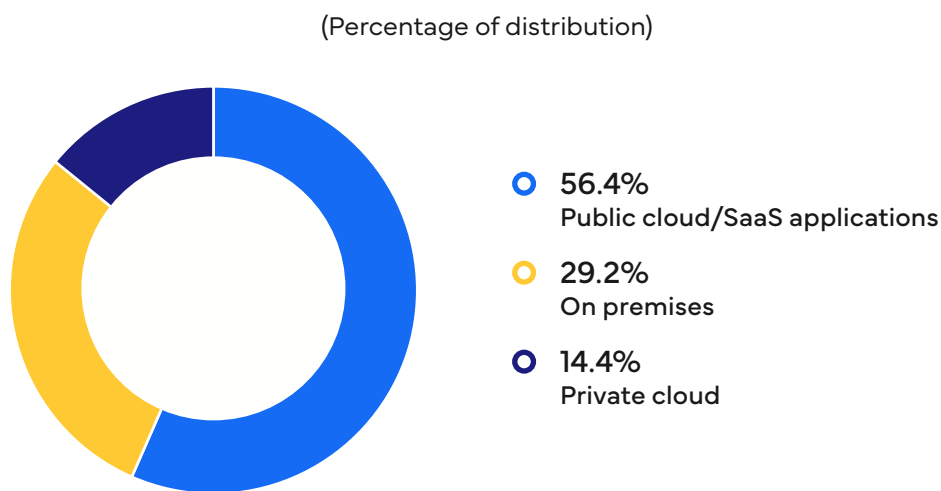
Table 2
Cyera Environment

Environment	Average	Median
Total TB of data	10,534	910
Percentage of data that is unstructured	68%	70%
Percentage of data public (e.g., available publicly, such as on a website)	4%	1%
Percentage of data internal (e.g., internal documents not subject to regulation but still important to the organization)	76%	95%
Percentage of data that is sensitive (e.g., subject to regulation such as PCI, HIPAA, or GDPR)	32%	25%
Percentage of data that is confidential (e.g., the most restricted information, such as company secrets or IP)	34%	25%
Number of data repositories	1,087,442	7,000
Number of AI tools/platforms	17	10
Number of employees using AI	4,234	1,010
Percentage of revenue supported	52%	55%

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Figure 1 (next page) presents the distribution of interviewed organizations' data environments across infrastructure types. As shown, 56% of data resided in public cloud or SaaS applications. The remaining data was on premises (29%) and managed in private cloud environments (14%). This reflected the environmental complexity that made consistent data visibility difficult to achieve with prior tools.

Figure 1
Data Environment Distribution



n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Business Value and Benefits of Cyera

IDC's analysis of the nine interviewed organizations identified measurable benefits across five core value drivers: comprehensive visibility into sensitive data, high-accuracy classification, significant reduction in manual effort and operational costs, reduced exposure and accelerated threat detection, and governing data access for safe AI adoption. For many organizations, those gains started with consolidating separate posture management, identity, and DLP tools into a single platform capable of inventorying data, assessing risk, and enforcing policy from one place. That consolidated view also surfaced sensitive data that had sat unclassified in plain text files and shared drives for years while giving teams a clearer picture of how data was actually being created, used, and stored across the business. Armed with that evidence, teams worked with business units to correct mistaken assumptions, redesign workflows, and monitor where sensitive data moved next, including uploads to webmail and AI tools. IDC found that Cyera had an impact beyond improving visibility and classification; study participants gained the ability to pair accurate data intelligence with the context needed to act on it and reduce risk.

Study participants described the most significant overall benefits as:

Unified security platform (Manufacturing):

"Cyera's platform consolidates our posture, identity access, and DLP needs in a single solution, and we're very confident that their discovery tools allow us to inventory all our data and cross-reference it with our identities so we can categorize it, manage risk, and enforce policies to ensure it doesn't get into the wrong hands. It also helps us protect our customer-facing AI technologies by keeping the wrong data out of the public domain, which enables us to more confidently accelerate our AI adoption."

Sensitive data visibility (Financial Services):

"The visibility into the location and quantity of sensitive information is a significant benefit of using Cyera. We didn't realize until we ran Cyera how many cleartext Social Security numbers, credentials, and credit card numbers we had stored in text files on people's OneDrives and file servers. The ability to apply classification labels to that information has also been valuable, since we'd never really been able to classify those documents properly."

Data usage visibility (Manufacturing):

"A big benefit of Cyera is understanding how our business uses data, which has brought to light many insecure processes, some inherited over time. Understanding how employees create data, what communications and training they need, and how they use and store data they take in from outside or generate themselves has also been significant. That gives us insight into how we can protect ourselves and help the business understand what it should be doing to protect us."

Data workflow redesign (Insurance):

"Being able to bring Cyera's results to the business teams and reimagine with them how they do business is a significant benefit. They believe they're handling data one way, and using the evidence we have from Cyera, we can show them how they're actually using it. For example, they may believe a team is storing information in one place when the reality is that they're storing it in five places. We then work with the business teams to examine what their workflow actually is and help them redesign it to be more secure and more efficient."

DLP upload monitoring (Healthcare):

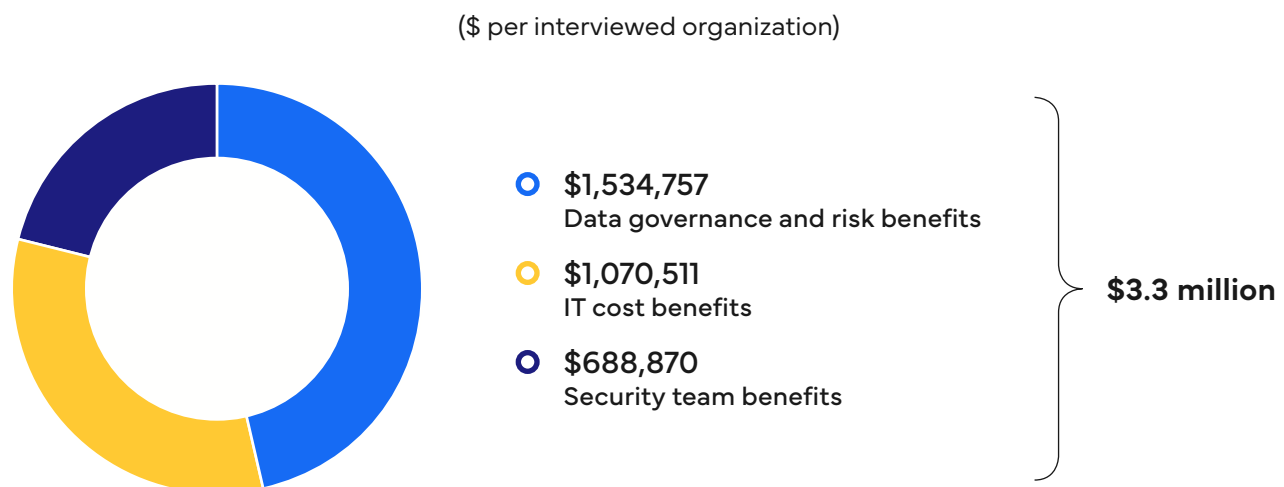
"Without Cyera, we wouldn't be able to tell if an employee has uploaded sensitive data to their webmail, to GenAI, or to our platform. We would have no way of knowing. The DLP gives us an additional layer of transparency, so right away we can tell them, 'On this day, you uploaded this information to ChatGPT.'"

Figure 2 (below) presents IDC's calculations of the average annual benefits realized by the interviewed organizations from their use of Cyera.

As shown, average annual benefits were quantified at \$3.3 million per organization (\$31,000 per 100 TB of data) across the following categories:

- **Data governance and risk benefits (\$1,534,757 per organization / \$14,570 per 100 TB):**
Interviewed organizations reduced the manual workload on data governance teams through automated classification, inventory, and reporting while also lowering their exposure to breach costs and end-user disruption. Faster detection and remediation of over-permissioned and publicly exposed data reduced the likelihood and severity of security incidents.
- **IT cost benefits (\$1,070,511 per organization / \$10,162 per 100 TB):**
Cyera's broad platform coverage let organizations retire redundant point tools and reduce reliance on manual data storage management. By identifying redundant and obsolete data across their environments, the organizations also avoided unnecessary storage costs alongside licensing savings from tool consolidation.
- **Security team benefits (\$688,870 per organization / \$6,539 per 100 TB):**
Cyera's automated, high-accuracy scanning and classification reduced the manual effort security teams spent investigating false positives, allowing existing staff to manage a growing data footprint and avoid additional hiring.

→ **Figure 2**
Average Annual Benefits per Organization



n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Reducing IT Costs Through Consolidation and Deduplication

The IT impact of Cyera was reflected in reduced spending on data storage and redundant point tools. Legacy environments required organizations to maintain separate solutions for cloud scanning, on-premises discovery, and DLP enforcement, often paying for capabilities that overlapped or went unused. Cyera's broader coverage across cloud, SaaS, and on-premises infrastructure, combined with its bundled DLP capabilities, allowed organizations to retire redundant tools and eliminate unnecessary data storage.

Participants described the cost impact of consolidating onto Cyera:

Reduced storage costs (Pharmaceutical):

"There's definitely been around a 10% reduction in our data storage costs from Cyera. The reduction is mostly around ghost data stores, which is an excellent feature within DSPM that we've made good use of."

Deletion of unused data (Financial Services):

"One capability Cyera is adding for us is the ability to see when a file was last accessed and to apply retention policies across our unstructured data. If a file hasn't been accessed in the last four years, we can move it into an archive and put a retention policy on that archive. If nobody looks for it within 90 days, we purge it. So, I'd expect that over the next 12 months, we'll start seeing a significant reduction in our overall file storage, not just files containing sensitive data."

Consolidated point solutions (Manufacturing):

"We had implemented some other solutions in the cloud, but they were not as comprehensive, and the AI tools were not as advanced as Cyera, so we retired them."

Reduced maintenance effort (Insurance):

"We were putting many hours per month into trying to improve and fix our old solution. That cost went away once we moved to Cyera."

IDC validated these findings by quantifying the annual savings organizations achieved through tool consolidation. As **Table 3 (next page)** shows, interviewed organizations realized an average of \$152,500 in annual savings by retiring legacy scanning, classification, and DLP tools that Cyera's broader platform coverage made redundant.

Table 3
Annual Tool Consolidation Impact

Impact	Average Annual Savings
Average annual savings from tool consolidation	\$152,500

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Beyond tool consolidation, Cyera reduced the volume of data organizations paid to store. By identifying redundant, obsolete, and orphaned data across their environments that legacy tools had not surfaced, interviewed organizations avoided or reduced an average of 283.6 TB of stored data. At an assumed average cost of \$3,500 per TB, IDC calculated annual cost avoidance of \$992,500 per organization, as **Table 4 (below)** shows.

Table 4
Annual Data Storage Cost Impact

Impact	With Cyera
Number of TB reduced/avoided	283.6 TB
Average cost per TB	\$3,500
Annual cost avoidance	\$992,500

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Improved Security Team Capabilities and Efficiency

Cyera's impact on security operations for the interviewed organizations centered on the accuracy of its classification engine and the breadth of its visibility across cloud, SaaS, and on-premises environments.

Legacy tools relied heavily on regular expressions and produced high volumes of false-positive alerts that required security analysts to spend the majority of their time validating findings rather than remediating real risk. Cyera's context-aware, AI-powered classification allowed teams to trust its output and act on findings immediately. The team also benefited from its consolidated visibility, which eliminated blind spots that prior point tools had left uncovered.

Participants described the operational impact on their security teams:

Accuracy driving speed (Insurance):

"Accuracy is a benefit of Cyera, and it is what drives speed. The lack of false positives means we're not distracted investigating what Cyera gives us. When it delivers results, we can act on them immediately and use that information to reduce risk, rather than spending a lot of time reviewing the results."

Faster risk remediation (Pharmaceutical):

"Cyera provides us with faster identification of over-permissioned paths and a more defensible way of prioritizing the remediation. It has also reduced our time spent hunting for any data risks and classification."

AI-powered data visibility (Manufacturing):

"The most impactful features of Cyera are visibility into data across cloud, SaaS, and multi-cloud environments and AI-powered classification and contextualization of our data. It ties identities to data and lets us build a risk scorecard for data that is private or secret. It's essentially AI-driven security posture management."

Data sprawl visibility (Financial Services):

"Data sprawl has been a major challenge for us. We have so much data across so many different data stores, accumulated over decades because we're an old company, and it's been very difficult to get visibility into who has access to what and which files are still in use and which aren't. Without a tool like Cyera, it would have been an impossible effort to do manually."

Visibility, classification, and DLP (Aerospace):

"I think Cyera helps security in three ways. First, it gives us visibility across all environments. Second, that visibility gives us the ability to label and classify data so we can apply additional protections. Third, we can stack DLP capabilities on the data we now have visibility into."

Freed analyst time (Aerospace):

"Having Cyera has really allowed us to focus more of my security analysts' time on other work. It's also helped with staffing, since we've always been stretched thin with a pretty lean team. It's helped us avoid having to make a business case for additional staff."

IDC next quantified the impact of Cyera on security team efficiency. Before deployment, the organizations dedicated significant analyst time to manual scanning, classification, and the investigation of false-positive alerts generated by legacy tools. After deployment, Cyera's automated, continuous scanning and high-accuracy classification allowed existing security staff to manage a larger data footprint without a corresponding increase in headcount. As **Table 5 (below)** shows, security teams achieved 51% greater efficiency following deployment, meaning they needed 5.0 fewer full-time equivalents (FTEs) to manage security operations compared to their pre-Cyera environments. IDC valued this efficiency gain at \$503,099 per year.

→ **Table 5**
Security Team Efficiency Gain

Efficiency Gain	Without Cyera	With Cyera	Difference	Benefit
FTE count	9.9	4.9	5.0	51%
Value of staff time per year	\$994,612	\$491,512	\$503,099	51%

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Because Cyera automated manual scanning and classification and eliminated the time analysts had previously spent chasing false positives, interviewed organizations also avoided hiring additional security staff to keep pace with their growing data footprint. A financial services organization noted, *"If we didn't have Cyera, and auditors said they didn't like our data governance program, my only other option would have been to hire two analysts to do nothing but go through the data and maintain it."*

As indicated in **Table 6 (below)**, interviewed organizations avoided an average of 2.4 security expert FTEs, representing \$241,667 in annual salary avoidance.

Table 6
Hiring Avoidance: Security Experts

Hiring Avoidance: Security Experts	FTEs Avoided	Salary Avoidance
Security experts avoided	2.4	\$241,667

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

The accuracy of Cyera’s classification also translated into measurable gains in how quickly and confidently interviewed organizations could act on data intelligence. A telecommunications organization noted, “The accuracy of the LLMs in Cyera is impactful, along with the tuning and the speed with which it can scan. We’re scanning hundreds of millions of files across millions of data stores. Our old solution had no ability to scan OneDrive and SharePoint files at all. We scanned 128 TB in less than 24 hours while in production, in the middle of the week, with no performance hit on that database. Our previous solution would have taken three weeks to scan that same data, and our accuracy went up from 70% to about 95% with Cyera; previously, we had to have someone manually check it.” The platform’s context-aware classification closed blind spots left by tools that covered only part of the environment and reduced the false positive alerts that had previously required manual review before a team could act.

IDC validated the following improvements in data intelligence actionability:

- **80% improvement in data visibility:**
Cyera closed blind spots left by tools that only covered part of the environment, giving security teams a consistent view of where sensitive data resided across cloud, SaaS, and on-premises systems.
- **66% improvement in risk prioritization:**
Study participants used the sensitivity and access context Cyera provided to prioritize which risks to address first, rather than treating every alert with equal urgency.

- **47% reduction in alert noise:**

Cyera's context-aware classification lowered the volume of false-positive alerts, which cut down the noise that had previously required manual review before a team could act.

- ➔ **68% improvement in actionable information:**

Because Cyera's findings carried greater accuracy and context, participants acted on results directly instead of spending time validating them before responding.

That added context carried through to how quickly security teams moved through their alert workflows. By surfacing data sensitivity and access history alongside each finding, Cyera let teams judge which alerts mattered most rather than treating each one as an open-ended investigation. One insurance organization put it simply: *"We went from 28,000 false positives to 0 with Cyera; false positives have been completely eliminated."*

IDC validated the following improvements in alert-based key performance indicators:

- **58% less time to investigate alerts:**

By surfacing context such as data sensitivity and access history alongside each alert, Cyera helped participants spend less time chasing down details and more time acting on confirmed findings.

- **44% less time to triage alerts:**

Participants used that added context to quickly judge which alerts mattered most, rather than treating each one as an open-ended investigation.

- **57% reduction in false-positive alerts:**

Cyera's context-aware classification cut down false positives compared to prior tools, so the alerts reaching security teams reflected real risk rather than noise.

- **47% less time to resolve or remediate alerts:**

With clearer visibility into what was exposed and who had access to it, participants moved more directly from identifying a risk to closing it.

Interviewed organizations also gained a clear view of who had access to their sensitive data and where it was exposed. Before deployment, organizations had limited insight into stale permissions, open sharing links, and organization-wide access settings that left sensitive data unnecessarily exposed.

Following deployment, IDC validated the following reductions in sensitive and confidential data exposure:

- **48% fewer over-permissioned users:**

Stale permissions, including access that former employees and outside contractors still held, had often gone unnoticed for years. Cyera cross-referenced its data classification with identity and access information to surface exactly which users held unnecessary or organization-wide access, giving security teams a defensible basis for revoking it.

- **78% less publicly accessible sensitive data:**

Before Cyera, organizations had limited insight into which sensitive files were exposed through open sharing links, organization-wide access settings, or misconfigured permissions. Cyera identified data shared more broadly than intended and treated public exposure as one of the primary risk types it tracked, letting organizations lock down or eliminate that exposure.

Continuous, automated scanning and visibility further strengthened interviewed organizations' ability to detect and respond to data threats and accessibility concerns. Cyera helped close detection gaps that once left threats unnoticed. This helped teams respond to incidents as they were unfolding, rather than after the fact.

As a manufacturing organization stated, *"Cyera helps us understand what the data is, who has access to it, who has accessed it, and what kind of activity they've had with it. We can use that information to avoid triggering an alert when we know something isn't risky or is authorized or to know exactly what we're looking at when it is. That means our investigations are much more targeted. We save time and energy for everyone involved and approach things more intelligently, rather than treating it like a fishing expedition to figure out what we missed."*

IDC validated the following improvements in threat detection:

- **78% more data threats identified and remediated:**

Several interviewed organizations described entire categories of threats, such as data egress or unauthorized file access, that had gone completely undetected before Cyera was in place. By combining data classification with identity and activity monitoring, Cyera gave teams a way to catch behavior that would have otherwise gone unnoticed.

- **88% quicker to detect data threats:**

Organizations had typically relied on manual review or after-the-fact investigation, so threats were often discovered well after sensitive data had already been exposed. Continuous, automated scanning gave teams ongoing visibility into how data was being accessed rather than periodic snapshots. This fundamental switch let them catch and respond to threats much closer to when they occurred.

Strengthening Data Governance and Reducing Risk

For data governance teams, Cyera provided a current, operational view of where sensitive data lived, how it should be treated, and who was accountable for it. Legacy environments left governance teams compiling documentation by hand for audits and struggling to establish clear data ownership across the business. Cyera's automated classification, identity correlation, and reporting capabilities gave governance teams a foundation they had not previously had.

Participants described the impact on their data governance programs:

Cross-environment visibility (Pharmaceutical):

"Cyera provides a more current and operational view of where sensitive data is and how it should be treated. The most positive impacts have been better cross-environment visibility, which we didn't have before, and more consistent classification."

Unstructured data discovery (Telecommunications):

"Cyera has given us the ability to find unstructured data on servers, where we find sensitive data that people forgot was sitting in a flat file or CSV. It's also shown us how much confidential material people had stored in OneDrive that wasn't protected."

Identity and data lineage (Insurance):

"Cyera combines detailed identity information with detailed data information, including lineage, so that we can tell the entire story about what's going on with any single piece of information."

USB and DLP enforcement (Healthcare):

"Cyera enables us to monitor and detect when someone is using a USB drive, whether for legitimate or illegitimate purposes; we know about it, and Cyera's DLP lets us block it. If someone tries to use ChatGPT by uploading sensitive information, we block that too. DLP policy enforcement, DSPM external permissions reports, and DSPM data classification all make a big impact."

Faster audit readiness (Manufacturing):

"Our overall audit readiness has been transformed with Cyera. We now have unified visibility across our structured and unstructured cloud data. It also gives us the ability to do automated data attestation, which has reduced the time it takes to disclose information to auditors from two weeks to one week on average. Lastly, Cyera's identity mapping capabilities tie data to user IDs, which has helped us provide clear audit trails."

Faster sensitive data reports (Financial Services):

"Now we can go into Cyera, ask questions, and get the reports we need within minutes. It's helped us reduce both the overall number of sensitive records and the ones exposed externally, cutting the need to run those investigations ourselves or buy an attack surface management solution to find that information. We also expect a significant reduction in overall data storage soon, since we can now implement retention policies and start purging old data that's been sitting there for years."

The automation described above translated into efficiency gains for data governance teams. Before deployment, governance teams manually inventoried data, tracked ownership, and compiled reporting for audits and policy enforcement, tasks that required substantial and ongoing staff time. After deployment, Cyera's automated classification and inventory capabilities significantly reduced this manual workload. As **Table 7 (below)** shows, data governance teams achieved 48% greater efficiency following deployment, meaning they needed 2.6 fewer FTEs to manage governance responsibilities compared to their prior approach. IDC valued this efficiency gain at \$264,780 per year.

Table 7
Data Governance Team Efficiency Gain

Efficiency Gain	Without Cyera	With Cyera	Difference	Benefit
FTE count	5.5	2.9	2.6	48%
Value of staff time per year	\$551,625	\$286,845	\$264,780	48%

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Reducing data risk translated directly into a lower financial exposure to a severe data breach. By reducing the volume of sensitive data left over-permissioned or publicly exposed, Cyera shrank the attack surface available to attackers. It also supported faster detection and remediation, which helped teams catch and contain incidents before they escalated into costlier events. A pharmaceutical organization noted, *"We have been able to address risk because Cyera identified issues during implementation that we remediated immediately, which reduced our risk of exposure right away. It also helped with ongoing risks like external threat activity, sensitive data sprawl, and inconsistent access controls."*

As **Table 8 (below)** shows, interviewed organizations reduced their percent chance of a severe or critical incident from 39% to 32%, a 17% reduction in the calculated annual cost of data breaches, worth \$302,178 per year.

Table 8
Potential Data Breach Cost Risk

Cost Risk	Without Cyera	With Cyera	Difference	Benefit
Percent chance of severe or critical incident per year	39%	32%	7%	17%
Average cost of severe data breach	\$4,583,333	\$4,583,333	N/A	N/A
Calculated annual cost of data breaches	\$1,768,844	\$1,466,667	\$302,178	17%

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

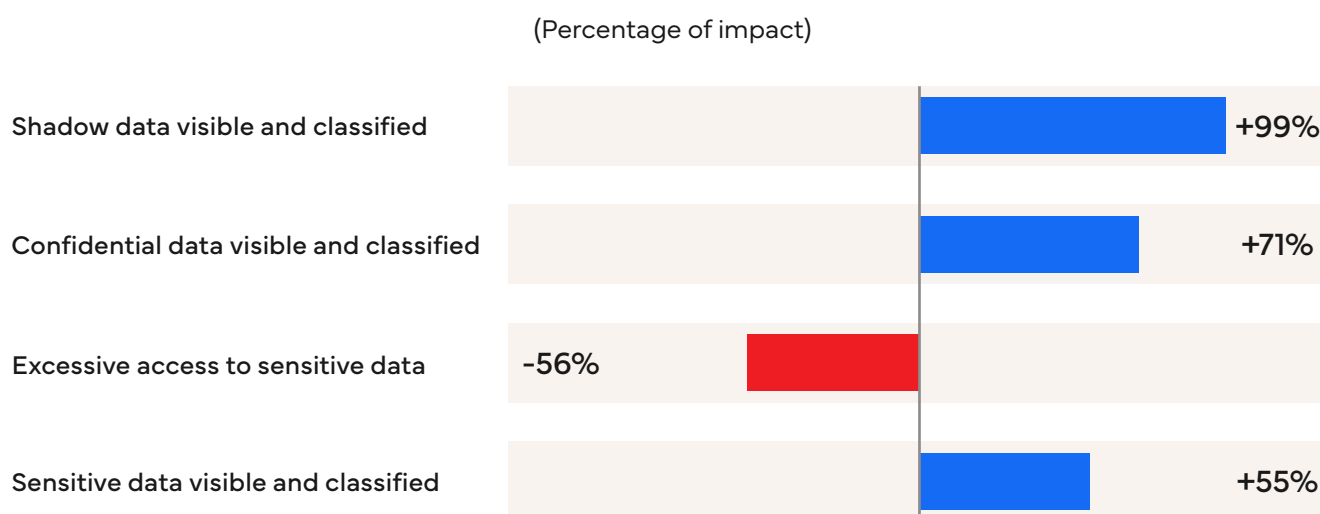
Beyond breach risk, governance teams at interviewed organizations extended their visibility past typical sensitive data categories to include source code and other business-critical information with Cyera. The solution paired that visibility with valuable context on how data was used and accessed.

IDC validated the following improvements in data visibility:

- 78% increase in data visibility:**
 Several organizations had no visibility into where their business-critical data lived before Cyera, describing it as a complete blind spot even outside of source code specifically. Cyera's classification surfaced that data across the environment, giving teams a view into information they had never been able to locate or account for.
- 66% improvement in data context to inform decisions:**
 Before Cyera, organizations could often tell that sensitive data existed but had little sense of how it was used, who accessed it, or why it mattered to the business. Cyera connected that data to its usage and access patterns, and organizations used the added context to make more informed decisions about policy enforcement and where to focus remediation.

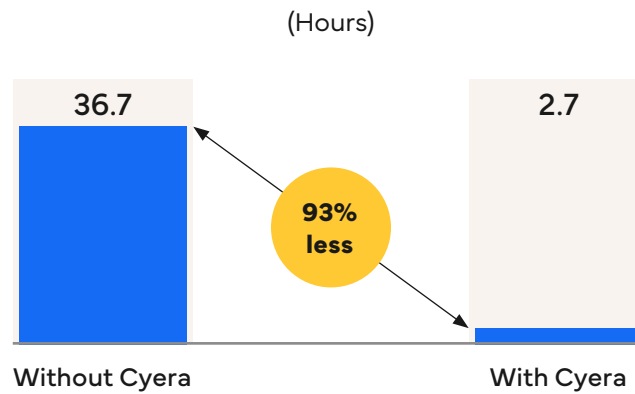
Figure 3 (below) breaks down the resulting improvement in interviewed organizations' ability to govern their data following deployment of Cyera. As shown, organizations achieved the largest improvement in shadow data visibility and classification, followed by confidential data visibility, inappropriate or excessive access remediation, and general sensitive data visibility and classification.

→ **Figure 3**
Impact on Ability to Govern Data



n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

The previously mentioned visibility and continuous classification of data also shortened how long it took interviewed organizations to locate and provide sensitive data in response to audits, data subject access requests, and other data requests. As **Figure 4 (next page)** shows, Cyera reduced the average time required per request from 36.7 hours to 2.7 hours, a 93% reduction, by allowing organizations to look up continuously classified and indexed data on demand rather than searching for it manually.

Figure 4**Time Reduction in Locating and Providing Sensitive Data for Requests**

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

IDC also found that interviewed organizations experienced fewer data security incidents that impacted internal end users because Cyera reduced the over-permissioned and publicly exposed data that incidents could exploit. If an incident did occur, participants found that they could resolve the incidents quicker with Cyera, limiting how long end users were disrupted. As **Table 9 (below)** shows, the number of incidents per year fell from 24.1 to 10.0, a 58% reduction, while the time to resolve each incident fell from 10.8 hours to 3.0 hours, a 73% reduction. Combined, these improvements reduced the total number of FTEs impacted annually by 89% and were worth \$1,092,331 in recovered productivity.

Table 9**Data Security Incidents: End-User Benefit**

Benefit	Without Cyera	With Cyera	Difference	Benefit
Number of incidents per year	24.1	10.0	14.1	58%
Time to resolve per incident, hours	10.8	3.0	7.9	73%

Table 9 continued next page

Table 9 continued from previous page

Benefit	Without Cyera	With Cyera	Difference	Benefit
Users impacted by incident	635	635	N/A	N/A
Percentage of productivity loss factor	20%	20%	N/A	N/A
Total number of FTEs impacted per year	17.6	2.0	15.6	89%
Value of lost productive time per year	\$1,231,960	\$139,629	\$1,092,331	89%

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Governing Data Access for Safe AI Adoption

As interviewed organizations expanded their use of GenAI, Cyera gave security and governance teams the visibility needed to govern that adoption safely. The platform helped organizations understand which sensitive data was accessible to AI systems, remediate over-permissioned access before it became a risk, and detect unauthorized use of consumer AI tools.

Participants described how Cyera supported their AI governance efforts:

Prioritizing AI use cases by risk (Insurance):

"We've been able to confidently prioritize which AI applications to move forward with and deprioritize the ones that didn't use sensitive data types with Cyera. We're also using Cyera to block the use of HIPAA data in our own custom-built LLMs and AI solutions."

Trusting accuracy enough to deploy AI at scale (Telecommunications):

"It's not about productivity gain; it's about visibility and increased confidence in what data is exposed and the impact that visibility and confidence have on unleashing initiatives and workstreams. We're more confident there's no leakage of bad data, so we're willing to deploy AI at scale."

Protecting export-controlled data from AI access (Aerospace):

"Cyera provides the data classification and visibility foundation that lets us safely expand AI adoption. With our Copilot pilot underway and thousands of employees getting AI access, Cyera makes sure AI models can't inappropriately reach our export-controlled data."

Confidently scaling AI rollouts (Manufacturing):

"AI agents inherit permissions from the user, so reducing our overall access to sensitive data made us more confident rolling AI out to larger groups much more quickly. Cyera's AI discoverability also helped us understand what tools were in use, whether by shadow AI agents or by our own employees, so we could roll out AI more confidently."

Detecting and governing shadow AI usage (Healthcare):

"Based on Cyera's DLP, we could see there was a huge spike in AI usage; people were using Gemini and other tools. We said, 'You're not allowed to use any of this; if anyone goes to the browser and tries to access it, we block it. The only tools you can use are the approved ones.' It's because of Cyera that we can see it, and we're better positioning ourselves."

ROI Summary

Summing up the financial and business-related benefits presented for study participants' use of Cyera, IDC calculated an average three-year return on investment. As **Table 10 (below)** shows, IDC projects that these organizations will achieve three-year discounted benefits worth an average of \$7.8 million per organization through reduced IT costs, improved security and governance team efficiencies, avoided hiring, and reduced breach and incident risk. These benefits compare with total three-year discounted costs of \$1.4 million per organization, resulting in an average three-year ROI of 441% with a payback period of 4.5 months.

Table 10
Three-Year ROI Analysis

ROI Analysis	Per Organization	Per 100 TB
Discounted benefits	\$7,841,400	\$74,439
Discounted investment	\$1,449,900	\$13,764

[Table 10 continued next page](#)

Table 10 continued from previous page

ROI Analysis	Per Organization	Per 100 TB
Net present value	\$6,391,500	\$60,675
→ ROI	441%	441%
→ Payback	4.5 months	4.5 months
Discount factor	12%	12%

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Challenges and Opportunities

Challenges

The information protection market is more crowded than at any point in history. Legacy data security vendors have expanded their portfolios with DSPM technology, lineage capabilities, and visibility tools to address the gaps in their portfolios. Vendors in adjacent markets are recognizing the significance associated with keeping data secure, monitored, and governed and are also actively courting data security budgets. With so many vendors talking about the same challenges, using similar language, true differentiation will come down to execution and integration depth.

Enterprise data volume continues to grow exponentially across cloud, SaaS, and on-premises environments, and endpoints. The bulk of this data is unstructured, ungoverned, and, often, generated by AI systems themselves. Organizations' data estates that are being scanned now will be materially different in six months, and vendor tools need to be able to keep ahead of these changes.

In addition to the tools from adjacent markets, security organizations will also be contending with different stakeholders regarding the safety, availability, and security of data. Security teams, data governance departments, privacy officers, legal teams, and, increasingly, AI and platform engineering teams all have a stake in how sensitive data is classified, accessed, and used. While vendors can supply visibility and context, they cannot supply organizational alignment, which is a significant factor in how quickly or broadly any technology is implemented.

Finally, compliance requirements remain constantly in flux, trying to keep up with technology changes. Data privacy, AI governance, and industry-specific regulations are continuously changing, and often, these requirements vary from region to region. This creates complexity and confusion about what compliant data handling involves and how to demonstrate it. Vendors operating in this space are expected to keep pace with regulatory change as a baseline capability.

Security teams looking to unlock their data value with AI while still maintaining governance and control need to look beyond point products and visibility. These teams will need to create a foundation that gets business teams to accept data ownership and change how they handle data once risk has been surfaced. Doing so requires ongoing change management, not just a technical rollout.

Opportunities

AI's growing footprint in the enterprise is reshaping who cares about data security and why. That shift is creating tremendous opportunity for vendors in this space. Traditionally, decisions about data visibility and protection were handled almost exclusively with security teams evaluating very specific technical criteria. That is no longer the case. Privacy officers, data governance leaders, and business unit leaders who are actively implementing AI are now active participants in these investments. Each stakeholder brings a different perspective, budget, and requirements that were not previously considered. As AI becomes embedded in day-to-day operations, business and data leaders outside of security are asking the same questions security teams have been asking for years: What data exists, where does it live, and who or what has access to it? This expands the buying center for data security tools beyond its current footprint.

The volume and complexity that AI adds to enterprise data is also changing how buyers evaluate security tools. For years, organizations relied on point solutions for discovery, classification, and enforcement. This approach was already straining security and data teams before AI. Now, with increased data volume and AI-driven dataflows growing faster than headcount, the bandwidth to manually integrate disconnected tools is just not there. Skills shortages compound the problem even further. Buyers are looking to platforms that can natively stitch together fragmented information into a single, informed view of risk, even if that means sacrificing some level of specialization. Vendors that can deliver broad data and AI security capabilities, with a unified view of critical alerts and relevant information, will be well positioned to capture market share.

Together, these shifts are giving vendors a new way to position the value of what they sell. Data security has typically been funded and measured as a way to prevent bad outcomes. As enterprises increase their adoption of AI, they are recognizing that visibility and governance benefits extend beyond the data security discipline. These capabilities can create a secure foundation that enables the business to confidently implement AI. That reframing opens a second and potentially larger conversation with the business that is tied to growth and innovation.

Conclusion

The organizations in this study make it clear that closing the gap between data growth and data control pays for itself quickly. The customers interviewed for this research achieved average annual benefits of \$3.3 million, driven primarily by reduced manual workload and risk exposure across data governance teams, as well as IT cost savings from tool and storage consolidation and efficiency gains for security teams. Measured over a three-year period, these benefits translate into an average ROI of 441% against a discounted investment of \$1.4 million per organization, with payback achieved in 4.5 months.

These figures reflect a shift in how these organizations operate day to day, spending less time chasing false positives and manually piecing together risk and more time pushing the business forward. Cyera's customers attributed these changes to pairing AI-native classification and DLP enforcement, giving them a single, informed view of their data risk. As AI initiatives place new demands on how quickly and safely data can be used, that pairing is likely to matter even more. Organizations weighing whether to consolidate their data security stack now have a clear, quantified answer for what that decision is worth. ●

Appendix A: Methodology

IDC uses a discounted cash flow methodology for ROI. IDC's standard Business Value methodology was based on gathering data from organizations currently using Cyera as the foundation for its model. Based on interviews with organizations using Cyera, IDC performed a three-step process to calculate the ROI and payback period: measured the savings from reduced IT costs, increased security and governance team productivity, and reduced breach and incident risk over the term of the deployment attributable to use of Cyera; ascertained the investment made in implementing and using Cyera and the associated migration, training, and support costs; and projected the costs and benefits over a three-year period to calculate the ROI and break-even time.

Time values were multiplied by burdened salary to quantify efficiency and productivity savings. IDC used its standard salary assumptions of an average fully loaded IT salary of \$100,000 per year and a user salary of \$70,000 per year. The net present value of the three-year savings was calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. IDC applied a margin assumption of 15% for other user productivity gains and additional benefits attributed to interviewed organizations' use of Cyera, resulting in the net calculations applied to IDC's model, as shown in [Table 11 \(below\)](#) and [Table 12 \(next page\)](#).

Note: All numbers in this document may not be exact due to rounding.

Table 11
IDC Business Value Methodology Terminology

Terminology	Explanation
Present value of benefits (discounted benefits)	Present value of benefits is the current value of the total benefits over the time frame, reduced by the discount factor.
Present value of investment (discounted investment costs)	Present value of investment is the current value of the total investment over the time frame, reduced by the discount factor.
Net present value	Present value of cash flows equals discounted benefits minus discounted investments.
ROI	ROI is the ratio of the net present value and the discounted investment: NPV divided by discounted investment.

[Table 11 continued next page](#)

Table 11 continued from previous page

Terminology	Explanation
Payback period (months)	The payback period is the point at which cumulative benefits equal the investment up until that time.
Discount factor (average cost of capital)	The discount factor is used to discount the cash flow to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.

Source: IDC, 2026

Table 12

Specific Calculations: Benefits from the Use of Cyera

Category of Value	Average Quantitative Benefit	15% Margin Applied	Calculated Average Annual Value
Security team efficiency gains	51% higher efficiency worth 5.0 FTEs, \$100,000 salary	No	\$465,341
Hiring avoidance: security experts	2.4 FTEs avoided, \$100,000 salary	No	\$223,529
Data governance team efficiency gains	48% higher efficiency worth 2.6 FTEs, \$100,000 salary	No	\$244,908
Potential data breach or loss cost impact	\$302,178 annual cost reduction	No	\$279,499
Data security incidents, end-user benefit	89% fewer FTEs impacted, worth 15.6 FTEs, \$70,000 salary	No	\$1,010,350
Annual tool consolidation impact	\$152,500 annual cost reduction	No	\$152,500
Data storage cost impact	\$992,500 annual cost reduction	No	\$918,011
Total average annual benefits	\$3,294,138 per organization per year		

Note: includes 2.7 months deployment time in year one.

n = 9; Source: IDC Business Value In-Depth Interviews, July 2026

Appendix B: Supplemental Quotes

Building data ownership (Manufacturing):

"I've built three data governance programs in my career, and the hardest challenge is always getting people to take ownership of data. The first pushback I get is, 'What are my responsibilities?', which is fairly easy to determine. The harder question is, 'What does this actually mean? What am I actually owning?' People often don't know what data they have or what they're supposed to be responsible for because they don't understand its impact, and they won't take ownership of something without understanding that impact. With Cyera, we understand the types of data people are taking over, who has access to it, where it's stored, and some of its lineage, including where it's coming from. Ownership is one of the most crucial functions of data governance, and it's infinitely easier now because we can go back to people and tell them exactly what we think they should own based on their level in the company, their permission sets, and who rolls up through them. Coming to business leaders with that kind of intelligence, rather than just asking what they think, gives them a lot more confidence in us, and in turn, they're much more comfortable accepting ownership when we ask. Data mapping in general, including the lineage piece I mentioned, is another massive part of data governance. Understanding where data lives has been huge on its own, and it's a big part of what we're trying to accomplish."

Enabling higher-risk, revenue-generating projects (Insurance):

"We've been able to move forward with projects that have a bigger impact on revenue, even though they carry higher risk, because Cyera lets us properly manage, secure, and monitor how regulated data is used."

DLP upload visibility (Healthcare):

"Without Cyera product today, we would not be able to tell if an employee has uploaded sensitive data to their webmail, to GenAI, to our platform. Cyera is giving us a lot of good visibility in terms of how and what people are doing."

About the IDC Analysts



Jennifer Glenn

Research Director,
Information and Data Security, IDC

Jennifer Glenn is research director for the IDC Security and Trust Group and is responsible for the information and data security practice. Glenn's core coverage includes a broad range of technologies including all forms of messaging security; sensitive data management, such as data loss prevention (DLP) and data access governance (DAG); obfuscation technologies such as encryption, tokenization, and masking; digital rights management; and cryptographic rooted identity technologies, such as key management, and certificates. As part of this research, Glenn focuses on the critical role of data security in top enterprise initiatives such as trusted AI data, data sovereignty, and post-quantum cryptography (PQC) transition.

[More about Jennifer Glenn →](#)



Megan Szurley

Business Value Manager,
Business Value Strategy Practice, IDC

Megan Szurley is manager for the Business Value Strategy practice, responsible for creating custom business value research that determines the ROI and cost savings for enterprise technology products. Szurley's research focuses on the financial and operational impact of these products for organizations once deployed and in production. Prior to joining the Business Value Strategy practice, Szurley was a consulting manager within IDC's Custom Solutions division, delivering consultative support across every stage of the business life cycle: business planning and budgeting, sales and marketing, and performance measurement. In her position, Szurley partners with IDC analyst teams to support deliverables that focus on thought leadership, business value, custom analytics, buyer behavior, and content marketing. These customized deliverables are often derived from primary research and yield content marketing, market models, and customer insights.

[More about Megan Szurley →](#)

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

[IDC.com](#)[IDC on LinkedIn](#)[IDC Blog](#)

International Data Corporation (IDC) is the technology intelligence layer of the AI economy. A global leader in research and data for more than 60 years, IDC's expert analysts, proprietary datasets, and rigorous methodologies are trusted by business and IT leaders to guide critical business strategies and IT investments. Today, that intelligence is built into the tools and workflows where work gets done with IDC Quanta, making work sharper, teams faster, and businesses harder to beat.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)