cyera

The Key Data Security Issues Modern Organizations are Facing

We developed this content in response to **common challenges** observed across security and data teams.

As sensitive data spreads across cloud, SaaS, on-prem, third parties, and AI workflows, teams face **growing alert noise, limited visibility, over-permissive access,** and **increasing regulatory pressure.** At the same time, they are expected to respond faster and with greater precision.

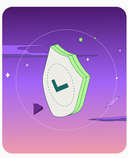
This page highlights **key data security challenges,** explains their **significance,** and shows where **gaps in visibility and control** create real risks.

If these issues sound familiar, this content will help you understand what drives them and what needs to change to address them effectively.

DLP

Cut DLP False Positives by **95%**

Cyera reduces DLP noise by accurately identifying sensitive data in motion and at rest, allowing security teams to focus on real risk instead of alert overload.



Governance and Compliance

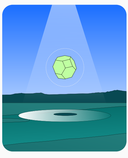
Only **11%** of organizations say they're fully prepared for regulatory requirements tied to AI data governance.

The average cost of non-compliance is $15M per organization. Stay compliant as your data moves. Cyera maps and classifies sensitive data across your environment and aligns it with frameworks like GDPR, HIPAA, and PCI, keeping you audit ready by surfacing violations and automating remediation.

Highly Sensitive Data

82% of data breaches now involve cloud-stored data.

Protect highly sensitive data everywhere. Cyera automatically discovers and classifies PII, PHI, PCI, IP and financial data across your environment, ensuring sensitive information is protected, governed and accessed only by those who need it.



Over Permissive Access

2/3 of orgs have already caught AI accessing more data than necessary.

Eliminate excessive access to sensitive data. Cyera connects identity directly to data, revealing who and what can access sensitive information so you can enforce least privilege and reduce risk.

Data Sprawl

39% of breaches span multiple environments.

Turn data sprawl into clear visibility. As data expands across cloud SaaS and on prem environments, Cyera maps your data landscape and highlights what is sensitive where it resides and who can access it.

Gen AI Use

83% already use AI, yet only 13% have strong visibility.

Adopt Gen AI without compromising data security. Get visibility and control over data accessed by Gen AI applications, enforcing policies that restrict sensitive data usage while enabling safe innovation.

Data Breach

the average cost of a data breach reached **$4.88** million in 2024.

Gain instant visibility when every second counts with immediate insight into what sensitive data was exposed where it lives and who has access, enabling fast precise response and reduced impact.

Privacy

57% of organizations cannot block or restrict risky AI activity, increasing the likelihood of sensitive data exposure through prompts and outputs.

Protect privacy across your data landscape, with visibility and control needed to safeguard sensitive data, reduce exposure and maintain privacy at scale.

Remediation

61% of organizations lack confidence in their ability to detect and respond to data exposures.

Act on data risk the moment it appears with fast automated remediation across cloud and SaaS environments, minimizing exposure and reducing operational burden.

Third Party Risk

Only **13%** of enterprises are confident about their data classification

60% do not feel confident they can detect data security exposures You can't protect what you can't see. Cyera tracks how third parties interact with sensitive data, alerts on risky access, and helps you maintain compliance while reducing indirect breach risk.

Discovery Classification and Response

Only **15%** apply data classification to real-time access control

Cyera automatically discovers and classifies sensitive data across your environment and provides the context and controls needed to respond quickly when risk appears.