CYERA

EBOOK

The Business Value of Data Security

The Urgent Need for a Data Security Platform

The rapid proliferation of data has created large and complex attack surfaces, requiring a new approach to data security.

Challenge	Implication
The data landscape is bigger, more varied, and continues to grow.	All datasets must be identified and the amount of metadata collected about each data asset must be massively expanded.
Data resides in a rapidly expanding number of vastly different applications and repositories.	Key data about permissions and methods of protection must be harvested to create a full picture of the value of the data and the level of risk.
The process of securing data means configuring and monitoring data protection mechanisms in a diverse collection of distributed systems.	Policies for securing data must be translated into specific configuration mechanisms for a large number of distributed applications, infrastructure, and cybersecurity systems.
Vulnerabilities constantly appear in applications, repositories, and networks across a complex landscape.	Vulnerabilities must be identified and then evaluated using the data inventory to see how much risk they present.

A data security platform solves these challenges by:

✓ Enabling new data security capabilities, practices, and applications based on the **high-resolution view of data security.**

✓ Dramatically improving **breach readiness and response.**

✓ Providing **intelligence** and greater **data visibility** that improve other cybersecurity technologies.

✓ Rapidly **approving data use** for new initiatives such as AI or analytics.

The Four Fundamental Responsibilities of CISOs

Every Chief Information Security Officer (CISO) focuses on four areas:

- **Protect the assets and people of the organization**
- **Comply with regulations and reporting requirements**
- **Prepare for effective response and recovery when incidents occur**
- **Leverage security investments to support business growth and innovation**

Clear data visibility is crucial to success in these four focus areas and to make decisions about where to allocate time and money.

To be successful, every CISO must answer the following questions:

What data am I trying to protect?

To enable proper protection, a CISO must know what data exists. With a complete, accurate, and up-to-date data inventory, a detailed picture of your data security posture can be created and many more questions can be answered.

What is the value of my data?

Some data may cause huge harm if compromised or stolen. Other data may have little value. Data must be classified into numerous categories so that it is possible to quickly understand how important the data is.

How is data protected?

Data is housed in a variety of different systems, each with its own mechanisms for security. It is important to understand those protection mechanisms so it can be determined if they are sufficient and appropriate.

What data is at risk?

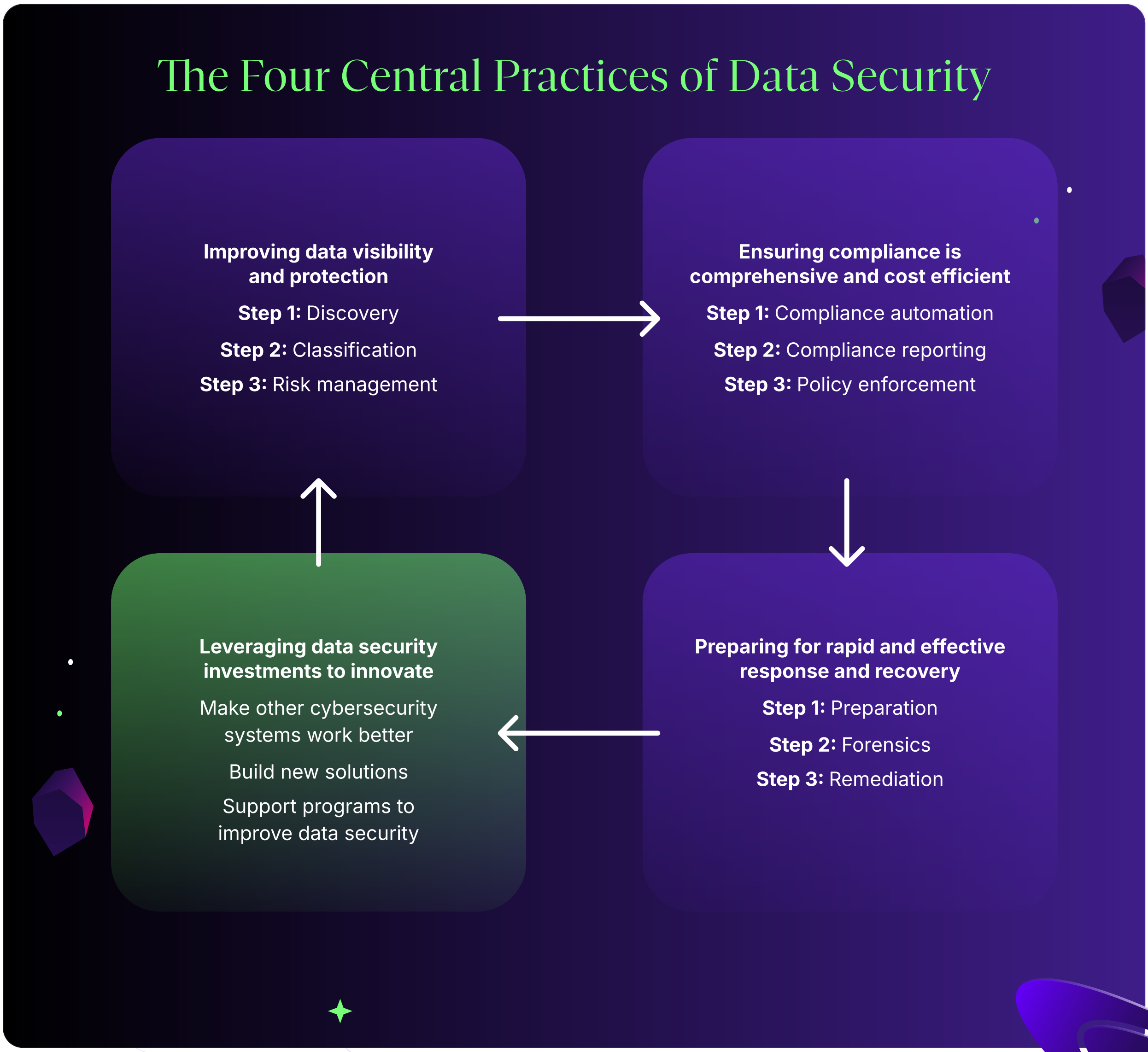
When insufficient controls, threats, or vulnerabilities are discovered in systems protecting data, appropriate measures must be taken based on the risk level.

A data security program cannot succeed without data visibility and clarity. With data visibility and clarity, CISOs can properly allocate security investments to protect the organization, unblock initiatives, and drive innovation.

The Four Central Practices of Data Security

CISOs can play offense and improve their data security by taking concrete action in the following areas:

- Improving data visibility and protection
- Ensuring compliance is comprehensive and cost efficient
- Preparing for rapid and effective response and recovery
- Leveraging data security investments to innovate



The Four Central Practices of Data Security

Improving data visibility and protection

Step 1: Discovery

Step 2: Classification

Step 3: Risk management

Ensuring compliance is comprehensive and cost efficient

Step 1: Compliance automation

Step 2: Compliance reporting

Step 3: Policy enforcement

Preparing for rapid and effective response and recovery

Step 1: Preparation

Step 2: Forensics

Step 3: Remediation

Leveraging data security investments to innovate

Make other cybersecurity systems work better

Build new solutions

Support programs to improve data security

Practice: Improving Data Visibility and Protection

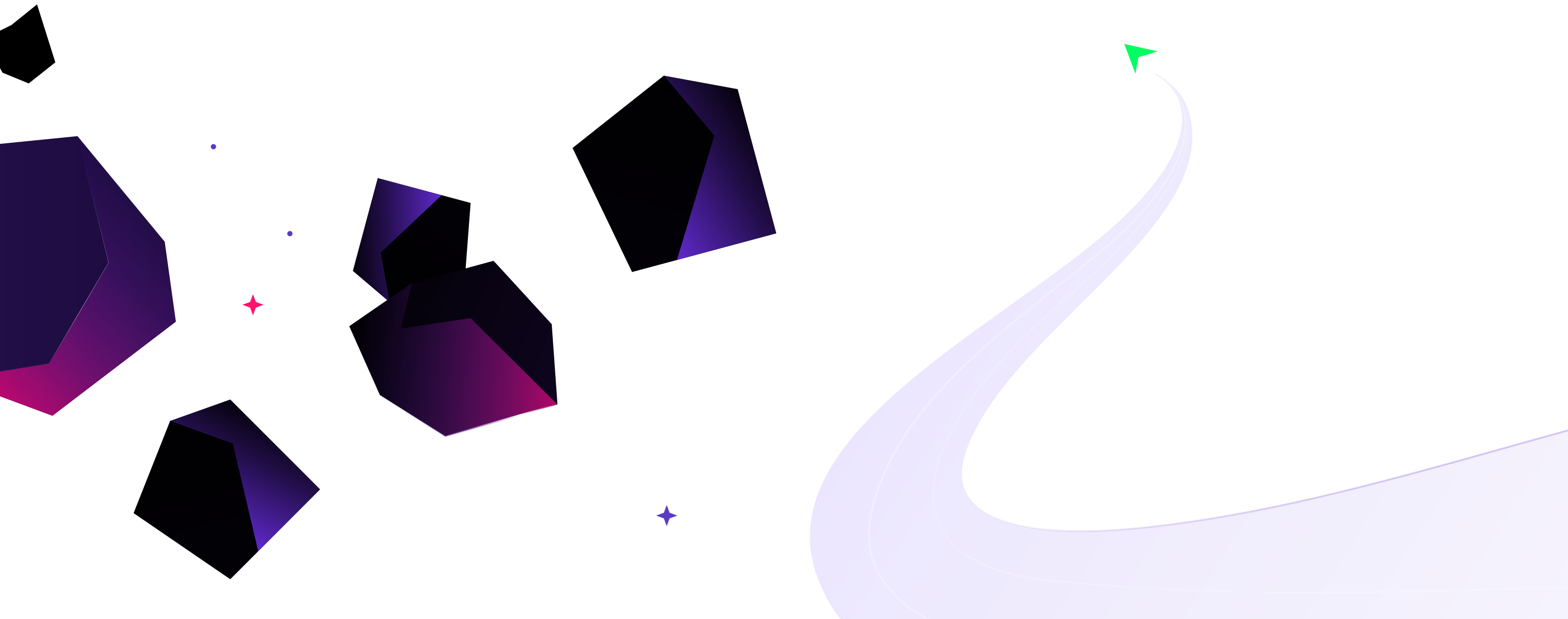
In the past, data security programs had no choice but to rely on manual processes for key tasks such as classification. The standard approach was to train lines of business staff to classify data and then have them deliver manual lists of how data was classified, often in spreadsheets. Much of the time, staff had little enthusiasm for the classification task and either marked all data as high value or classified inconsistently. In addition, the classification divided the data into a few broad categories, which were of little help in crafting specific policies to protect different types of data.

Manual classification does not support effective data security at scale, and has no hope of success in the modern data landscape.

The path for CISOs to comprehensive and effective data protection is a three-step journey.

Step 1: Discovery

- **Find all your data.** CISOs must be able to confidently assert that they can identify all data assets. With such a view it is possible to detect data sprawl, in which data is distributed for no reason, or where numerous copies of data exist.
- **Automate data discovery.** The breadth and complexity of the modern hybrid landscape requires the discovery and inventory creation process to be automated.
- **Expand collection of metadata.** The resulting data inventory must include a vast collection of metadata describing every dimension of data assets. For example, should the metadata capture the data security state of a dataset? Is it encrypted, hashed, or plain text?



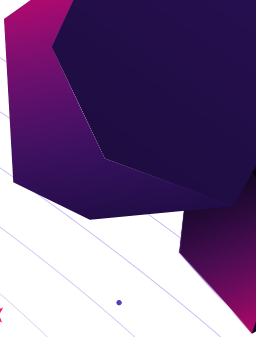
Step 2: Classification

- **Create detailed classification.** The assets in the data inventory must be precisely classified so that many questions can be answered about their risk profile. For example, 10 different forms for patient intake across a large number of hospitals all may be in one category so the same data security policy can be implemented.
- **Implement AI-native classification.** Manual classification can no longer keep up. AI-native methods are required to use the metadata collected from discovery and inspection of data assets to create a multi-dimensional classification.

Step 3: Risk Management

- **Create a risk score for each dataset.** Risk for a data asset consists of likelihood of a breach and the value of the asset under threat. The data inventory supports discovery of external exposure of sensitive business-critical data and dangerously broad access to data in violation of least privilege.
- **Prioritize work on remediation.** Risks to high-value assets must be addressed immediately. Addressing vulnerabilities to low-value assets can wait. Investments in cybersecurity can be made based on risk profile. Data minimization programs can reduce the attack surface.
- **Define policies tailored to each class of data.** With a complete classification, policies can be crafted to protect sensitive data and maintain usability.

Using a data security platform to create visibility as just described, makes sure that all data is identified and evaluated with respect to risk, avoiding hidden risks.



Ensuring Compliance is Comprehensive and Cost Efficient

Present-day CISOs have to grapple with a large and growing number of regulations about privacy and data usage. More regulations are constantly emerging, increasing the burden. Complying with such regulations is challenging for a number of reasons:

01 Enforcement methods vary.

Some regulations involve criminal penalties, while others involve fines. CISOs must determine which parts of which regulations are the most critical.

02 Regulations vary based on the type of data.

Personally identifiable information (PII) or credit card data may have a whole set of burdens.

03 Regulations vary by geography.

Entering a new market may require a company-wide change in data management and compliance.

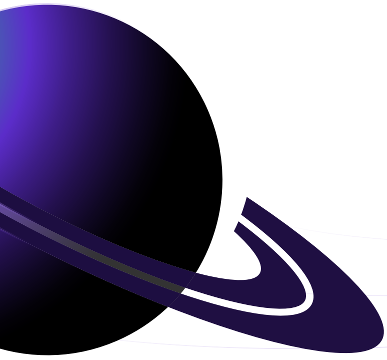
04 Regulations vary by industry.

Most industries have their own set of requirements, making compliance complex for organizations that operate across verticals.

05 Controls are distributed.

The regulations may require controls that must be implemented in a wide variety of systems and applications.

Playing whack-a-mole with regulations by using one-off compliance processes is not only inefficient, but it’s unlikely to keep up. Instead, CISOs can use the following three steps to play offense and get ahead of compliance mandates.



Step 1: Compliance Automation

- **Expand visibility as far as possible.** The full visibility provided by a data inventory enables CISOs to make compliance processes far more efficient and ensure reporting is comprehensive. All data that is subject to compliance can be quickly identified and then evaluated to find gaps in reporting, controls, or protection.
- **Create an integration, automation, and reporting framework.** Once again, a manual approach to compliance is a nonstarter. So is attempting to build a new reporting and compliance framework each time a new regulation comes into force. Making compliance efficient, automated, and fully auditable, requires the kind of knowledge of your data that a data security platform provides.
- **Use the power of existing systems.** Compliance controls will be implemented in a wide range of systems. Some systems may have sophisticated controls inside them already, such as ERP systems. Others are dedicated to controlling data security, like DLP systems. It is vital that these systems are orchestrated to work together. Varying types of proof of compliance will be required.

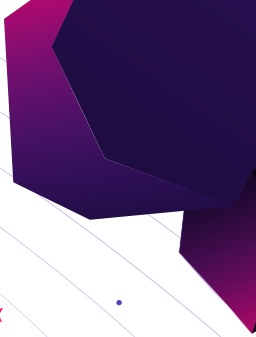
Step 2: Compliance Reporting

- **Automate reporting.** Compliance reporting processes can be automated to ensure that all mandated information is provided on schedule. As the reporting burden grows, patterns emerge about the kind of information that is required and the automation becomes more efficient.
- **Create a clearing house for compliance.** The data security platform can be the central repository for information about how data is secured and what controls are in place.

Step 3: Policy Enforcement

- **Active enforcement.** Don't wait for regulatory violations. Policies for data security and compliance can be actively enforced based on the visibility provided by the data inventory.
- **Automated enforcement.** All of the important details of regulations should be embedded in platforms that search for violations. Automated alerts and remediation processes can be triggered when compliance violations are found.

A proactive approach to automated compliance avoids large fines and provides a framework for quickly implementing new compliance mandates as they arise.



Preparing for Rapid and Effective Response and Recovery

Incident response is a tough job, one that is inextricably entwined with both breach readiness, which takes place before attacks, and business resiliency mechanisms, which are used after. Before the arrival of data security platforms CISOs had to fly blind during key parts of the incident response process.

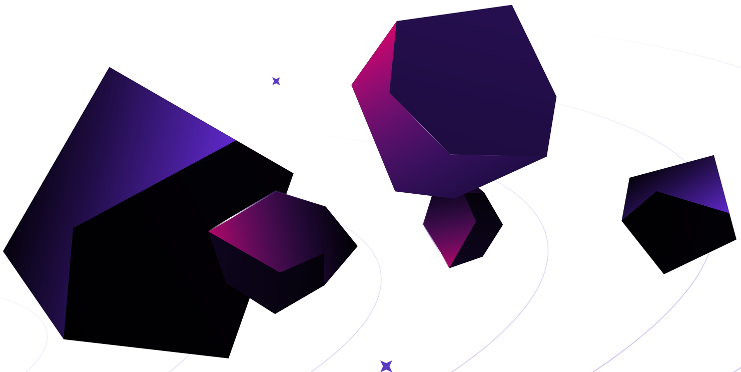
Before attacks, the recommended actions described in the data security protection section mentioned above must be executed to make sure that attacks are anticipated and prepared for. In the wake of an attack, CISOs are required to report on the scope of the attack. Board and compliance regulations require disclosure of how much data was compromised or stolen. Answering such questions inaccurately or slowly can be a career-limiting move. In addition, inaccurate reporting may require repeated public statements, which amplify the damage.

Remediation and resiliency plans also require testing and validation, but doing so for all data is often cost-prohibitive. Breach readiness must focus on the most valuable data.

CISOs can use these three steps to increase breach readiness to streamline response and recovery processes:

Step 1: Preparation

- **Analyze current data security measures protecting high-value data.** To prepare for attacks against the most valuable assets, CISOs can use their data inventory to identify and analyze the protections currently in place. Special attention should be given to the most high-value and high-risk data.
- **Expand early detection measures.** Use all existing cybersecurity systems for monitoring and detection of data security related events.
- **Create plans to enable rapid response to minimize the data attack blast surface.** Create plans and playbooks for the most common and most likely attacks. A detailed understanding of data that is involved in the attack can accelerate responses designed to limit damage.



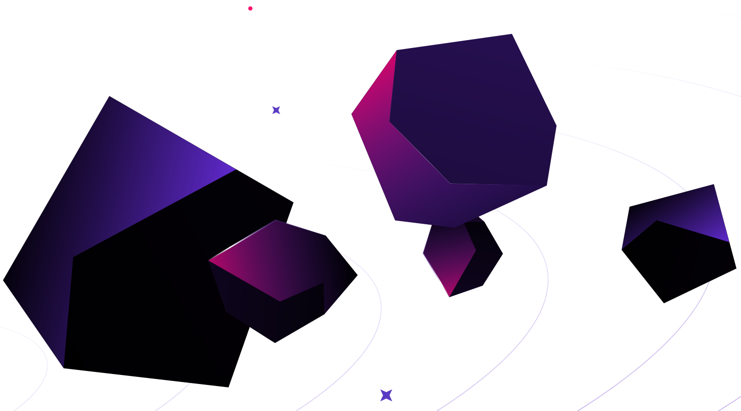
Step 2: Forensics

- **Create standards for data security forensic reporting.** When attacks occur, a full complement of forensic information related to the data in question should be rapidly assembled using the data inventory and other data sources. CISOs can also accurately determine what data is involved, avoiding repeated public updates based on inaccurate reporting. The standards should specify what constitutes full reporting.
- **Accurately report on data breaches in a timely manner both internally and externally.** Don't rush to report before a full understanding has been gained. A complete data inventory makes forensic analysis straightforward, reducing the risk that orphaned or unknown data is involved in attacks.

Step 3: Remediation

- **Review and test remediation methods.** Before attacks, CISOs can use the data inventory to make sure appropriate remediation methods such as backups are available for the most important data assets.
- **Proactively uncover gaps in remediation and resilience planning.** A full data inventory can reveal data that was orphaned and should be deleted, or data that is important and not part of current planning.
- **Perform risk-adjusted validation of remediation and resiliency mechanisms.** The most valuable data can be clearly identified so that business-continuity plans can be validated and tested.
- **Use attacks to increase the quality of defenses.** After attacks, the data landscape can be audited to determine if the exploited vulnerabilities exist elsewhere.

With advanced preparation, informed and enabled by a data security platform, skills and capacity for incident response and remediation can be developed before attacks, reducing their impact and severity when they occur.



Leveraging Data Security Investments To Innovate

Cybersecurity is a domain populated by numerous systems, each taking care of a different problem. Almost every cybersecurity system, however, shares the goal of protecting data. As we have described above, a data security platform sheds light on where the most important data resides, how valuable it is, and how it's protected. This vital information can be used to make other cybersecurity systems work better, build new solutions, and support programs to improve data security. In these ways, a data security platform can meet the core responsibilities of CISOs.

Here are some illuminating examples of use cases that show the power that a data security platform gives CISOs to meet their fundamental responsibilities:

Playing whack-a-mole with regulations by using one-off compliance processes is not only inefficient, but it's unlikely to keep up. Instead, CISOs can use the following three steps to play offense and get ahead of compliance mandates.

Protect

- **Destruction of unneeded data:** Once a data security platform is in place, a classic first step is to reduce risk by shrinking the data landscape. A data destruction program identifies and deletes high risk data and other orphan data that is not being used.
- **Enhance zero trust network access (ZTNA) effectiveness:** Information and analytics from a data security platform can also improve the effectiveness of zero-trust security systems by identifying who has access to data and allowing that to be an input to risk scoring.
- **Tune identity access management (IAM) configuration:** Data security platforms can provide intelligence to improve IAM systems by helping analyze who has access to high-value data enabling precise audits of IAM configuration to enforce least-privilege access.

Comply

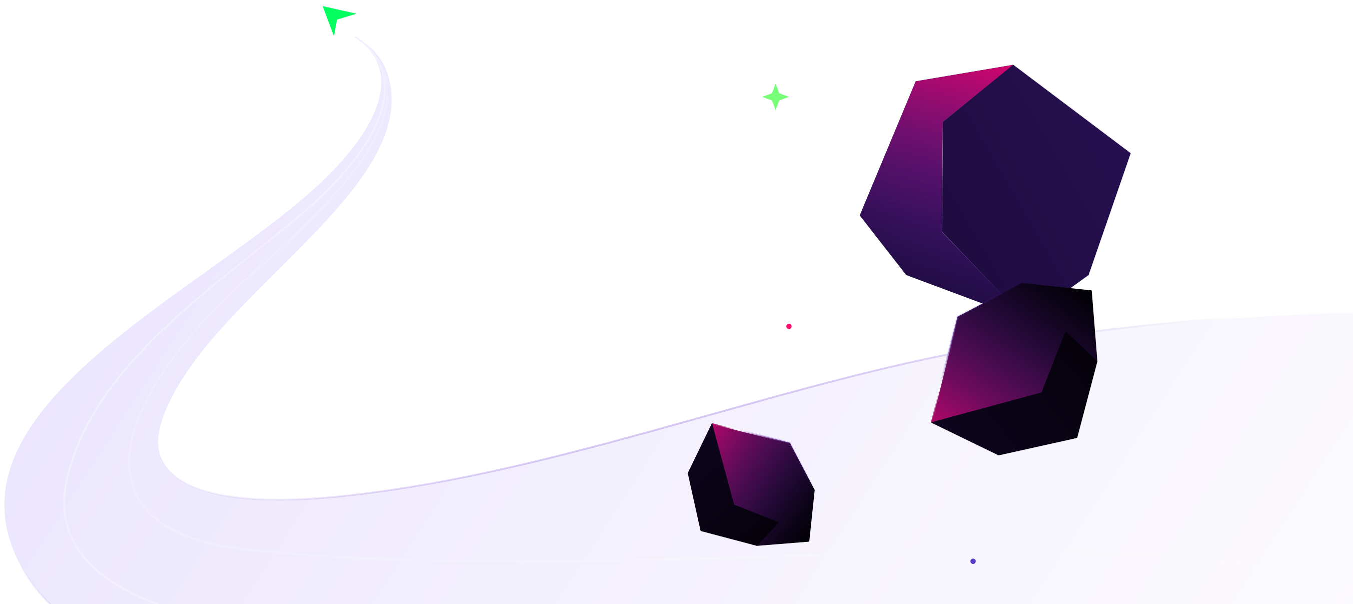
- **Improve governance:** A data security platform can improve data governance by identifying opportunities to expand and refine policies and controls for handling data. Data security platforms show a clear picture of current governance mechanisms, including defining access policies, retention guidelines, sharing restrictions, and compliance requirements.
- **Expand monitoring:** A data security platform can help implement expanded and continuous monitoring of data access and usage patterns that enable the detection of potential security violations. By maintaining real-time visibility, security teams can quickly identify and respond to threats, ensuring that data is protected as required by compliance standards.
- **Analyze control flow:** A data security platform can help manage control flow, tracking how data moves across networks, devices, and users to prevent unauthorized access. This includes monitoring external transfers and enforcing sharing policies. By making data flows more visible, the CISO can prevent data exfiltration and ensure compliance with regulations that limit the movement of sensitive data.

Respond

- **Accelerate forensics:** With a comprehensive data inventory and classification that a data security platform provides, a CISO can understand the scope of a security incident more rapidly. The platform provides detailed information about the location, sensitivity, and protection status of the affected data. This information is essential for analyzing the impact of a breach, and it helps the CISO understand how big an incident is, and differentiate between a minor event and a major event — which helps avoid the expense and time required to hire lawyers and other forensic experts to figure out what was stolen.
- **Audit and improve resilience:** With a full data inventory, it is possible to expand logging and auditing of activity for sensitive data, ensure complete and secure backups are in place and tested, and implement delete protection where needed.
- **Improve containment:** A data security platform helps CISOs contain incidents more effectively by using information about data sensitivity and access. By understanding the data's lineage and flow, they can identify where data has moved and take appropriate action to prevent further spread of a breach. This includes blocking anomalous behavior and investigating suspicious activity.

Leverage

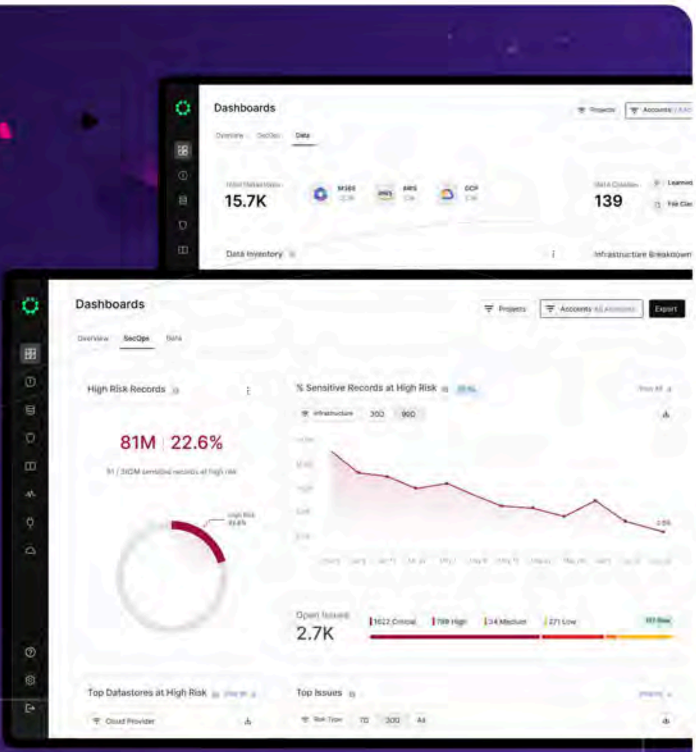
- **Promote safe use of data for AI:** As AI systems start to use more and more data, data security systems can identify which data is being incorporated in retrieval-augmented generation (RAG) and LLM applications. Once such data goes into a model, it is difficult and sometimes impossible to control. Approving use of data quickly is crucial. Data security information can be used to accelerate innovation by making sure that only appropriate data is used for AI.
- **Analyze data risk for new corporate initiatives:** The comprehensive visibility provided by a data security platform allows CISOs to confidently express an opinion about the data risks related to new corporate initiatives and technology deployments. Such speedy analysis avoids delays.
- **Support risk analysis for third parties:** When performing M&A transactions or creating new partnerships, the tools and skills related to implementing a data security platform can help analyze and surface data risks. Depending on the access provided to the third party data landscape, a detailed risk analysis may be possible that helps executives properly assess the business risks of the transaction or partnership.



CYERA

The Cyera Data Security Platform

Fuel business growth by pioneering the discovery and security of your most vital resource: data.



Protect Your Dataverse.

Data is everywhere—but visibility isn't. Most organizations don't know what data they have, where it lives, or who can access it. Cyera delivers clarity through automated discovery and AI-native classification—so you can spot risks, enforce protection, and ensure safe, compliant access to data for your business.

Discover data risks at scale, and with speed

Cloud adoption creates immense data sprawl. Control this complexity with continuous data discovery, enabling visibility across environments to reduce risk and enhance compliance.

Classify data with high precision, and rich context

Given the abundance of data, you need to know which data is most sensitive, and understand key context to help you better protect it. AI-native classification can help.

Protect data everywhere it lives and moves

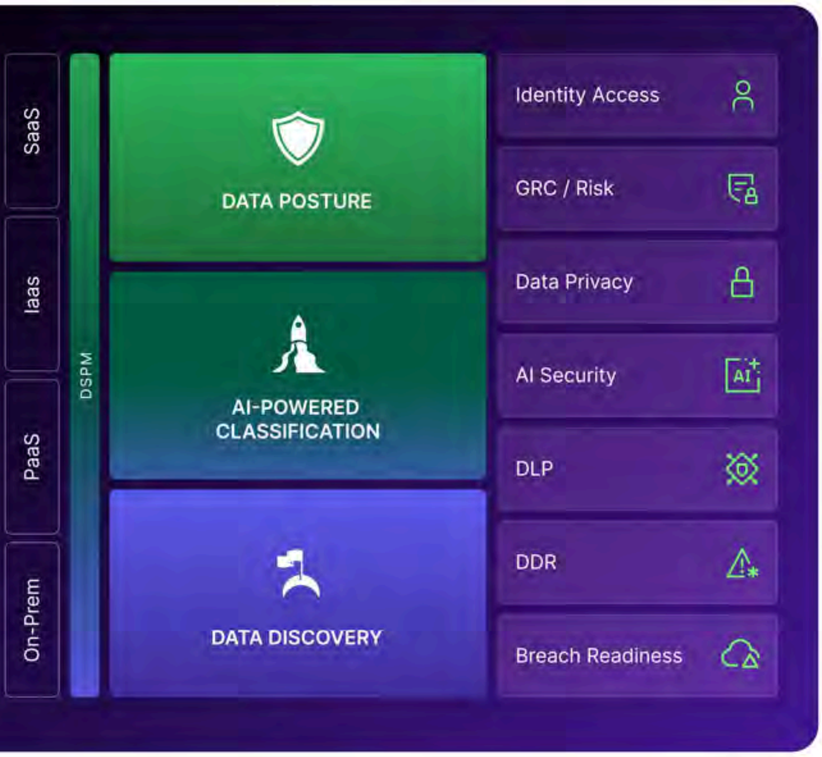
Fixing broken DLP starts with intelligence. Connect your fragmented systems, enrich alerts with context, and cut alert noise with an AI brain built for DLP.

Finally connect data and identity security

Data and identity go hand in hand. View identity through the lens of data for the first time so you know who – or what – is accessing critical data.

A Unified Platform for Everything Data Security

Cyera delivers an AI-powered platform that shows you where your data lives, how it's used, and how to keep it safe - everywhere it moves. Focus on real threats, boost operational efficiency, and unlock the full value of your data.



Data Security Posture Management (DSPM)

Discover and classify your sensitive data, determine what's at risk, and monitor it over time.

Data Governance, Risk & Compliance

Track data controls and policies for a risk-based approach to data governance and compliance.

AI Security

Leverage AI – responsibly and securely. Stop unauthorized data from entering AI models or copilots.

Data Detection and Response (DDR)

Continuously detect and respond to threats like unauthorized access, data exfiltration, and more.

Identity Access

Gain clarity into the human and non-human identities with access to sensitive data.

Data Privacy

Build a personal data inventory, identify privacy risks, and demonstrate privacy compliance.

Omni Data Loss Prevention (DLP)

Combine DSPM with a real-time DLP analysis engine to protect data at rest, in motion, and in use.

Breach Readiness

Conduct tabletop exercises, define recovery plans, and set materiality criteria for faster breach response.

Why Cyera?

- Agentless Discovery, Faster Data Visibility
- AI-Native Classification with 95%+ Precision
- Automated Risk Identification and Prioritization
- AI-Native Brain To Make Your DLP Actually Work
- Unmatched Scale to Match Your Data Growth

For more information visit cyera.com or scan→

CYERA

CYERA.IO