cyera

CUSTOMER STORY

How a multinational pharmaceutical company uses Cyera to improve data security and compliance

CASE STUDY	INDUSTRY	REGION
Global Provider	Pharmaceutical	Multi-national

Customer Story Summary

DATA LANDSCAPE	CLOUD PROVIDERS	DATA VOLUME
Hybrid Cloud	Amazon Web Services	Over 9PB of Data
	Microsoft 365	Over 2 million Records

CHALLENGES

- Lack of visibility into sensitive patient and third-party data under management
- Gaps in identifying the sensitive data that requires encryption
- Over-privileged access to sensitive data

RESULTS

- Dynamic sensitive data inventory across their hybrid cloud landscape
- Continuous data security posture assessment including sensitive data access graphs
- Automated remediation workflows for sensitive data exposure

Challenge

As a multi-national pharmaceutical provider, the company conducts life-changing research and development. They work with innovative companies, research hospitals, academic institutions, scientists, and organizations to solve unmet medical needs. To drive scientific innovation and insights, data is collected and stored in AWS and shared across the organization using Microsoft 365. Some of the data includes patient data, research data, clinical trial data, and patent information. Given its global presence, the company easily had over nine petabytes of data in scope. This data is sensitive due to business, research and development, compliance, and privacy concerns, and they believe deeply in their responsibility to protect and manage that data.

Transparent and responsible sharing and reuse of health data are integral to the company's mission to discover and deliver life-transforming treatments, which is why it is critical for the security team to make certain that the diverse types of data stored in cloud environments are encrypted at rest and in motion. The collection of health data is rapidly increasing, keeping pace with technology and collaborations within and outside of health systems. The company is also now collecting patient data and feedback, further adding to the complexity and quantity of data. This ever-growing health data requires not only the protection of individuals' personal data but also the proprietary data belonging to third parties, creating new challenges for their security teams to govern data access and modification.

The CISO needed a solution to help them overcome gaps in their visibility and understanding of their sensitive data exposure, including:

- Lack of visibility into sensitive patient and third-party data under management
- Gaps in identifying the sensitive data that requires encryption
- Over-privileged access to sensitive data

Solution

The company chose Cyera's data security platform to analyze its cloud data stores. In just five minutes, the company deployed Cyera on several hundred accounts, quickly discovering all data stores and identifying over nine petabytes of data. They integrated Cyera's data into Splunk to create a centralized data lake with information and context on all their cloud data, which will help them rapidly identify and remediate any potential security and privacy risks present within it. Cyera helped to ensure that:

1. **Sensitive data across the cloud environment is securely stored and encrypted both when at rest and in motion**
2. **Logs are configured for maximum visibility into data access and modification**
3. **Data and security analysts could establish data lineage and govern access**

Cyera worked with the security team to elevate their company's security posture and compliance capabilities. This decreased the company's business continuity risks while improving responsibly sharing and reusing of health data, practices that advanced medical innovation and patient health outcomes. Using Cyera, the company was able to quickly identify its personally identifiable information (PII), guarantee that it had the information needed to put guardrails around its sensitive data, and identify and secure data stores.

> "Cyera helps us create a security posture and compliance framework to more effectively share data across stakeholder groups"
>
> Cloud Security Architect

Results

Complete data inventory and visibility

Cyera enables the company to quickly discover all the sensitive data that it manages. The identification of sensitive data gives the company the ability to create a more transparent process for sharing and reusing health data to advance the field of medicine. Cyera verifies that data is collected, used, reused, and shared responsibly in a way that supports scientific discovery and advancement.

Increased cyber-resilience

Due to the quantity and complexity of the company's cloud data, it is critical for the security team to verify that their security posture is strong. While the absence of data exposure or data loss is always a sign of success, the company wants to make certain that the attack surface is minimal and remediation workflows are automated. They are now able to:

1. **Create and tune risk metrics to protect the most sensitive data**
2. **Define internal remediation workflows**
3. **Define roles and responsibilities across business units and incident response teams**
4. **Integrate Cyera with the internal ecosystem, including the security information and event management (SIEM) solution, data catalog, and workflow automation**

Compliance assurance for healthcare data privacy regulations

By increasing visibility into the data, the company is fully equipped to adhere to regulations regarding data processing. Cyera assists in considering data-sharing requests in such a way that it maintains trust with society and protects the personal data of individuals and the proprietary data of other third parties. The completeness of data inventory allows the security team to generate reports for the executive team and other stakeholders that communicate the company's data security and compliance posture, showing that the data is governed properly and has proper access control.

Achieve operational resilience and preparedness

As a global organization with many partnerships and collaborations, the company believes it is imperative to be able to recover from or adapt to any occurrence that may impair its ability to perform mission-critical functions. To assure operational resilience and preparedness for adverse events, the company dedicates considerable efforts to increasing the security and protection of its data.

The pharmaceutical leader builds trust with consumers and partners by using Cyera to help it:

- **Create custom policies and rulesets** to ensure internal compliance with data policies
- **Maintain compliance with industry regulations** around data retention and deletion
- **Communicate strategy and executive-level accountability** across the enterprise

About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data and their security exposure, and delivers automated remediation to reduce their attack surface. Learn more at www.cyera.io, or follow Cyera on LinkedIn.

Trusted by:

Cboe ARMIS GRANICUS LifeLabs ACV