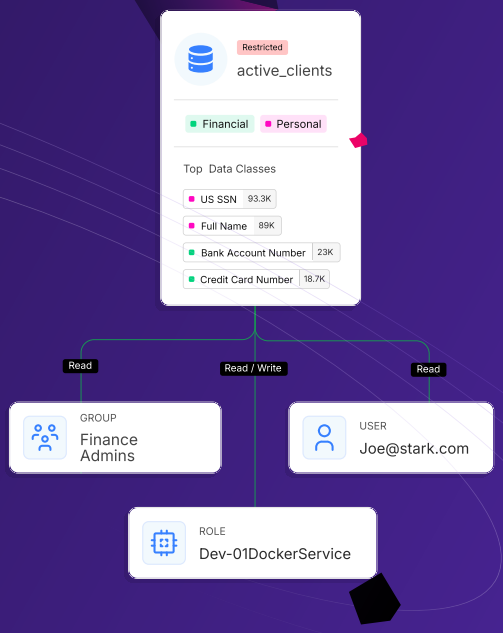
CYERA

Cyera Identity Module

Make identity part of data security

Cyera's Identity Module combines our high precision data discovery and classification capabilities with identity access insights, to provide better visibility into which employees, third parties, and non-human identities like services, AI tools, and applications have access to your sensitive data.



Complete Visibility Into Identity Data Access

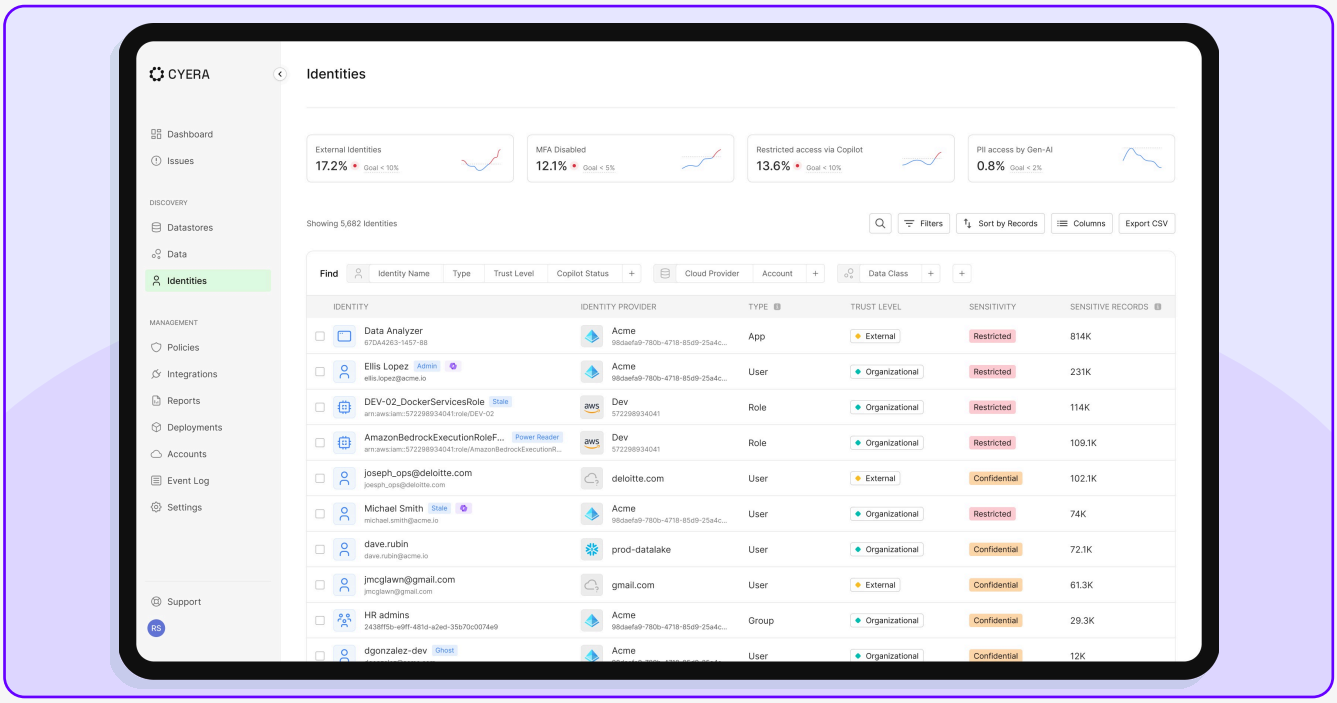
Cyera empowers you to ensure that your sensitive data is only accessible by the identities that require access to it. The module effectively identifies at-risk data, and high risk-identities to help prevent unauthorized access from individuals, third parties, and non-human identities, and determine the data blast radius in the event that an identity is compromised.

The Value of Cyera's Identity Module

- **Discover identities within your environment**
- **Link identities to sensitive data access activities**
- **Enable zero trust data access principles**
- **Detect high-risk human and machine identities**
- **Detect unauthorized data exposure**
- **Know what data AI tools can access, use or learn from**

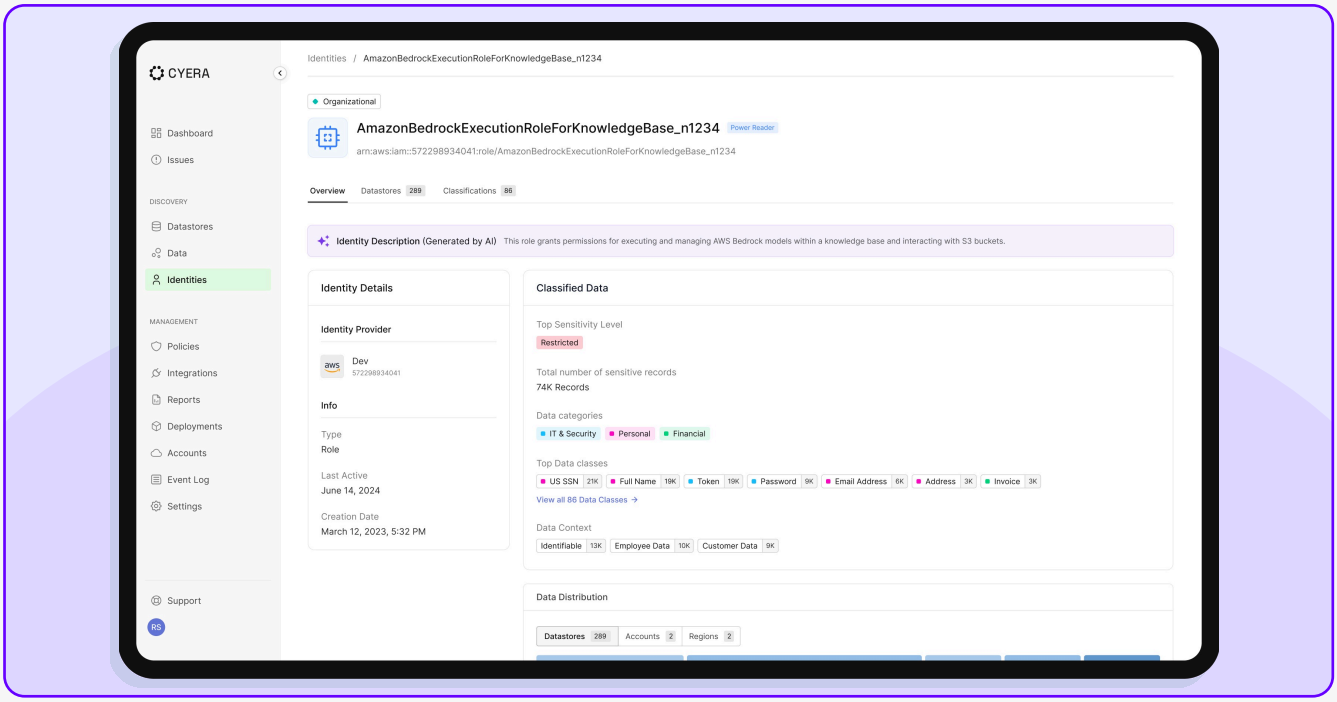
Centralize Identity Data Access Insights

Cyera provides a unified view of all identities, human and non-human, to show who or what can access sensitive data across environments.



Pinpoint Risky Identities with Sensitive Data Access

Detect unauthorized, risky, or stale identities that have access to sensitive data, especially risky identities with old passwords or no MFA.



Benefit From Making Identity Part of Data Security

Monitor and manage sensitive data access based on contextual identity and data insights.

Common Use Cases:

Data Access Analysis

Gain comprehensive visibility into who is accessing what data, to ensure data security and compliance.

Identity-Centric Risk Identification

Use context to address risks related to user, such as no MFA, weak passwords, stale users, and ghost users.

Reduce Overly-permissive Access

Minimize exposure of sensitive data by compartmentalizing access based on role and data type for safe sharing of data.

Third-Party Data Sharing

Determine the third-party identities with access to sensitive data, minimizing potential regulatory fines and ensuring safe data sharing to auditors and suppliers.

Core Functionality

Identity Access Explorer

See who or what accesses sensitive data to improve visibility into excessive permissions and insider threats.

Offending Identities

Identify who triggered the risk, investigate related issues, and remediate issues immediately in the platform.

AI Data Access Insights

See which users have access to AI tools and what sensitive data is accessible to GenAI.

Third-Party Access Insights

Monitor trusted and untrusted third parties that have access to sensitive data.

Want to see Cyera Identity in action? Request a free demo