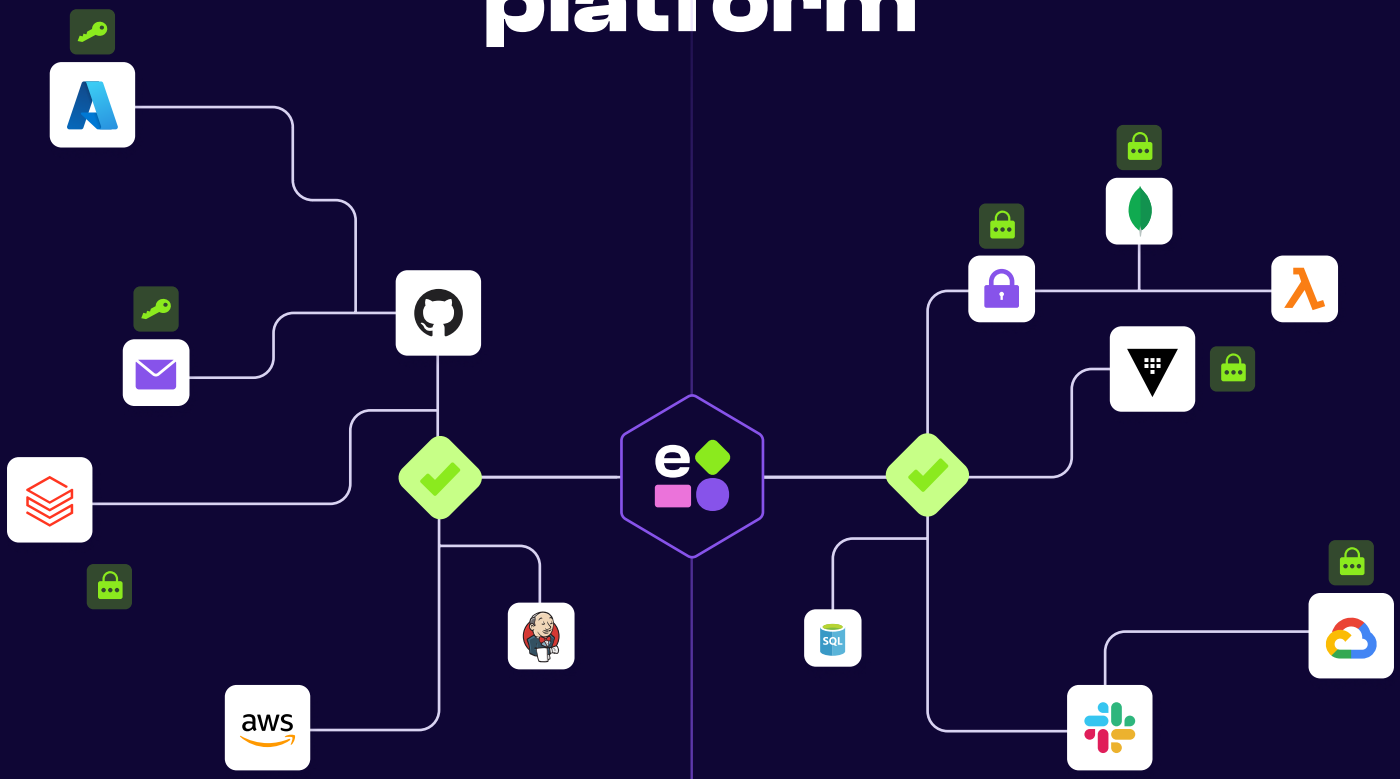
Entro solution

A comprehensive secrets security platform



Entro is the first and only comprehensive secrets security platform that provides a holistic approach to detecting, safeguarding, and enriching your secrets, vaults, secrets managers, collaboration tools and codebase. It offers a single pane of glass to protect private API keys, tokens, and secrets.

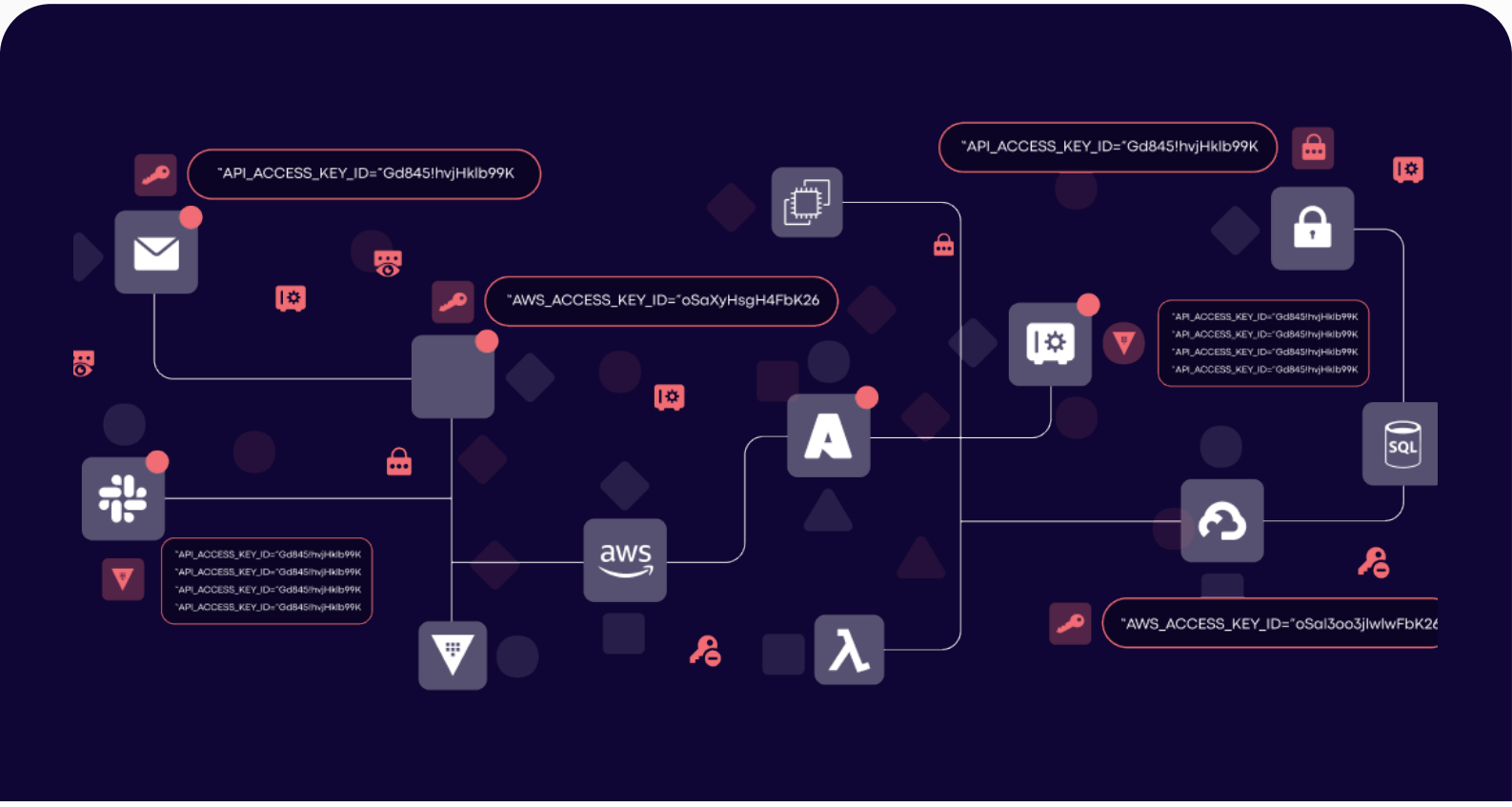
Featuring deep secret analysis and context enrichment capabilities Entro enables security teams to take immediate action to reduce the programmatic attack surface.

The need

Your secrets are out of control

Companies in 2023 face an increasing risk of data breaches due to compromised authentication credentials. Poor authentication and access control of secrets keys can make them easier to access for malicious actors, leading to data exfiltration. Companies need to stay vigilant about their API Keys security hygiene and access control to mitigate the risk of a data breach.

Known as the “The API Secret problem”, this is when insecure privileged accounts, credentials, and secrets (e.g. API secrets, access tokens, connection-strings, encryption keys, certificates, passwords, etc.) are used, making it easier for attackers to gain access to sensitive systems. Privileged accounts, credentials, and secrets that are not properly managed and secured are particularly vulnerable. These include secrets that lack dedicated solutions and CISO oversight, secrets with weak passwords, and secrets that are shared across multiple users.



The importance of security strategy for today's organizations when using secrets and private keys in the cloud is more crucial than ever.

According to research

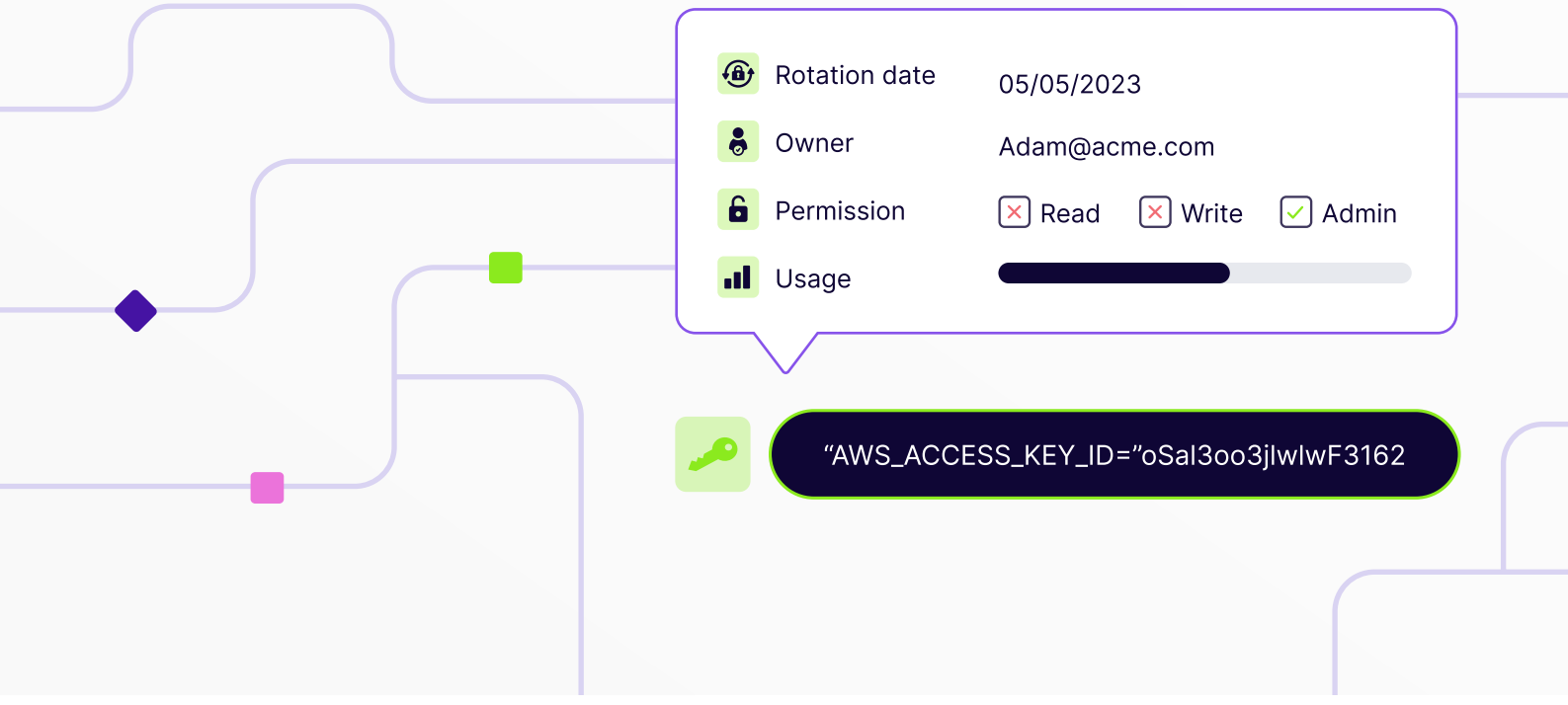
45% of the data breaches were cloud-based, and cloud misconfiguration.

contributed to **15%** of breaches.

Data breaches can have a significant impact on business profitability and customer costs. They can lead to lost customers, reputational damage, regulatory fines, and legal fees. Additionally, the cost of responding to a data breach can be significant, including costs for investigation, remediation, and disclosure.

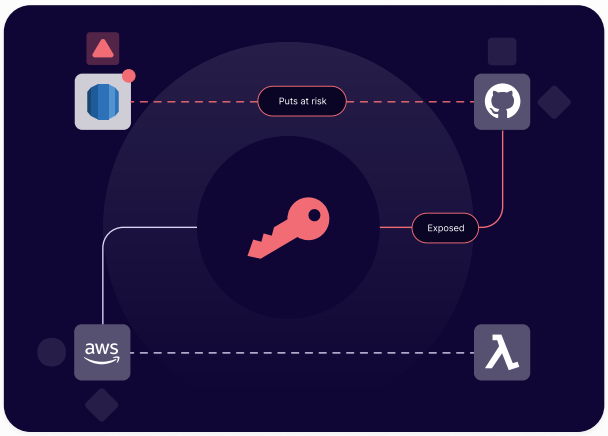
To ensure the security of your business, it is important to have a robust strategy that is suited to provide a comprehensive set of tools and observability to aid security teams to protect privileged access and understand how sensitive secrets keys are being used within their organization.

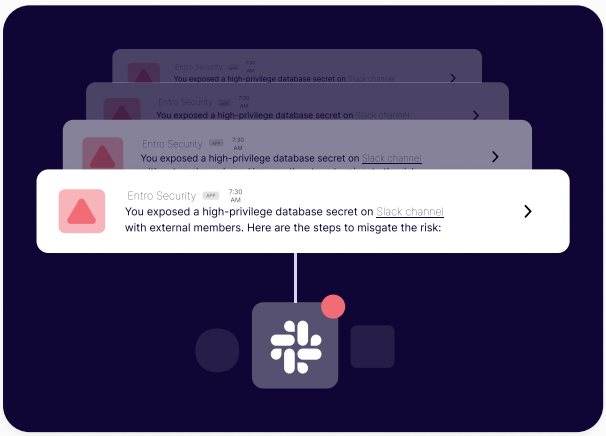
A well rounded strategy should include automated credential and secrets protection and ownership, identity access management, and secrets vulnerability detection and remediation.



Easy to integrate into your organization's tech stack, helping you to efficiently discover, manage and monitor secrets, enforce least privilege and role-based access controls, and ensure secure and supervised programmatic authentication of applications, containers, and other non-human identities.

Making identifying abnormal or malicious secrets activity seamless, while reducing API secrets risks, accelerating remediation, while saving time and money for both security and development teams.





Giving you all the needed information to be able to rotate secrets without causing downtime to the systems, or interfering with the software engineers' or DevOps work while keeping the company secured against secrets targeted attacks.

The perfect solution to facilitate your organization's secrets Security Strategy.
Entro provides a comprehensive approach to protecting your secrets and eliminating the risk of malicious activity.

Feature 01

Discover all secrets across all organization's solutions

Discover any and all secrets across all vaults, clouds, code, CI/CD, emails, and collaboration solutions, and assess risk severity with actionable context.

Benefits

- Secret inventory
- Security oversight
- Time savings

Feature 02

Deep secret analysis, secret classification and metadata enrichment

Visualize and understand which application is using what secret to access what cloud service, and vital secrets data, such as creation time, secrets privileges, rotation date, owner, risks, and more.

Benefits

- Reduced complexity
- Understand your secrets
- Compliance

Feature 03

Real-time Secret Detections and Rapid Response

Anomaly detection, rate limiting, access control monitoring, real-time discovery of secrets abnormal behavior, misuse, or abuse.

Benefits

- Increased security
- Continuous monitor
- Avoid secrets attacks

Feature 04

Save time by automating remediation

Reduce secret risks, excessive permission, dark-web leakage, and vault misconfiguration, accelerate remediation, and save the security and development teams time and money

Benefits

- Automate remediation
- Improved threat response time
- Achieve collaboration

Account	Storage	Secret	Severity	Status	Owner	Creation time	Environment
972845811113	AWS Secret Manager	jenkins_admin		new	adam@entro.security	about 12 months	Production
921144411958	AWS Secret Manager	eyal_personal_token		not in use	eyal@entro.security	about 2 months	Dev
acme-org-prod	Github Actions	storage_service_acc		active	valerie@entro.security	about 16 months	Production
972845811113	AWS Secret Manager	splunk-auth		disabled	john@entro.security	about 2 months	Production
921144411958	AWS Secret Manager	db-certificate		not in use	noah@entro.security	about 2 months	Dev
Entro workspace	Slack Channel	user access key		exposed	alex@entro.security	about 2 months	Production