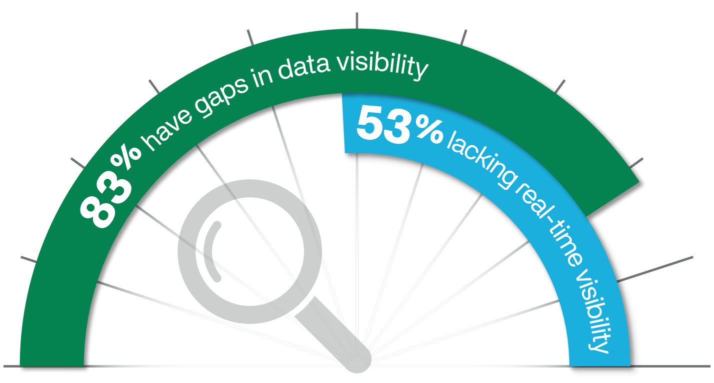
2025 Enterprise Data Security Confidence Index

The **2025 Enterprise Data Security Confidence Index** surveyed 530 cybersecurity professionals, revealing critical gaps in data visibility and AI governance across organizations.

BEDROCK SECURITY

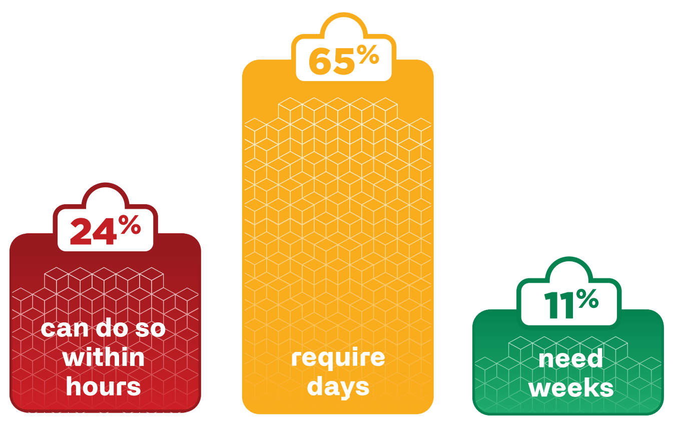
The Data Visibility Problem

1 Are there visibility gaps in your organization's ability to discover and classify data?



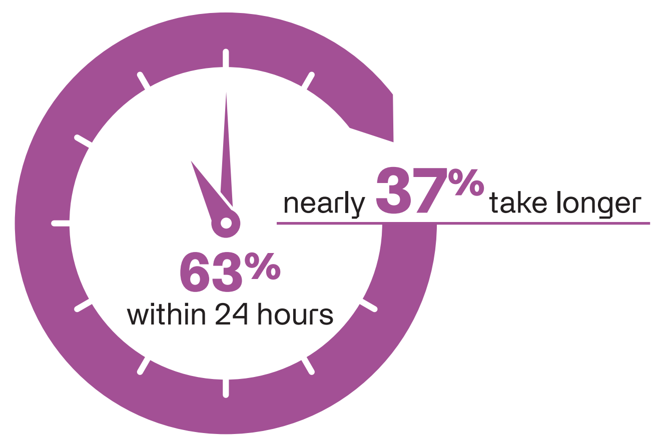
IMPACT: Visibility gaps hinder proactive risk mitigation, slowing breach response and compliance efforts. Accurate, real-time visibility is essential for effective data governance and swift security incident containment.

2 How quickly can your team demonstrate a complete data inventory?



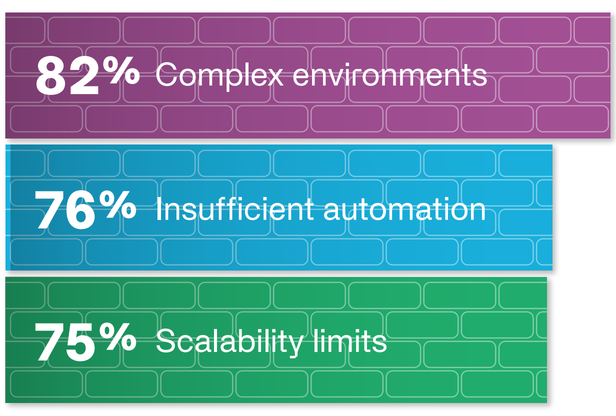
IMPACT: Delays in generating data inventories increase vulnerability windows, amplifying risk of noncompliance and magnifying potential damage. Immediate inventory capability is critical for timely response to breaches and audits.

3 How quickly can your team identify who accessed sensitive data in the last 30 days?



IMPACT: Delays in access tracking significantly extend exposure periods, escalating the risk of data breaches, compliance violations, and reputational damage. Timely access insights are essential for effective security posture.

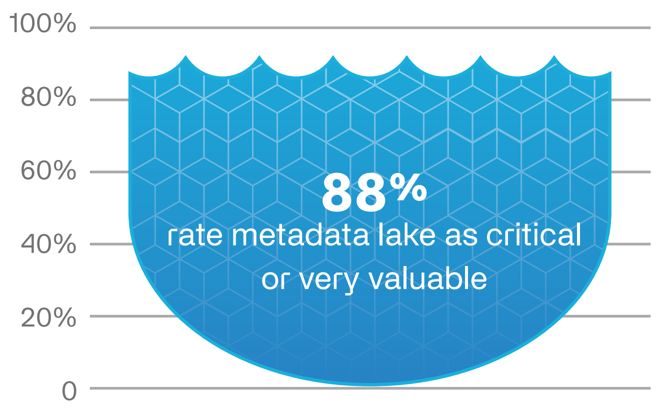
4 What are your top barriers to effective data security?



IMPACT: Complexity, insufficient automation, and scalability constraints significantly impede effective security management, leaving organizations exposed to breaches, slowing response times, and increasing regulatory risk.

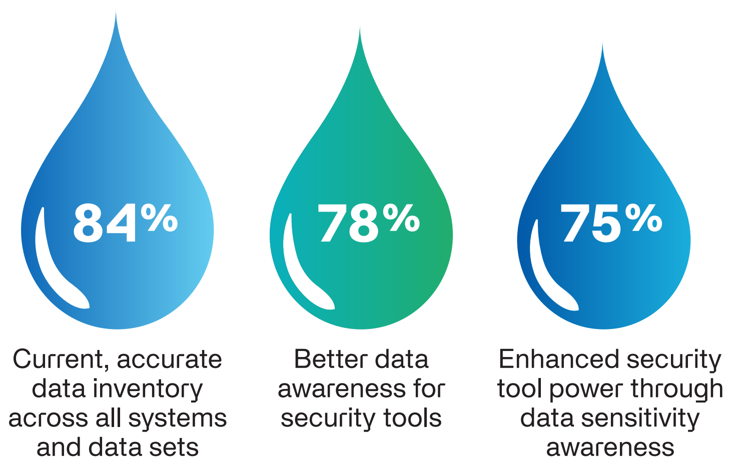
The Data Visibility Solutions

5 How valuable is an automated, accurate metadata lake to solving data visibility issues?



IMPACT: Organizations overwhelmingly recognize the critical role of metadata lakes in reducing manual overhead, enabling automated compliance enforcement, accelerating incident response, and improving overall security effectiveness.

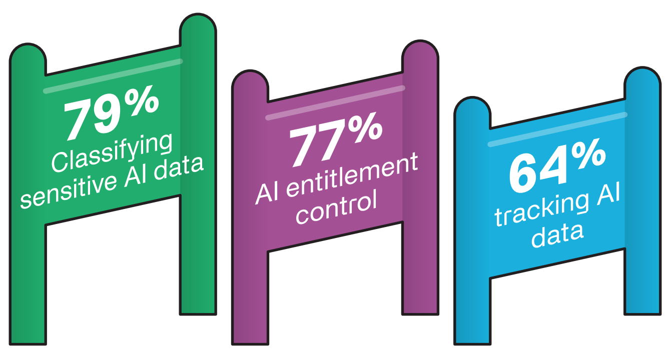
6 What are the benefits of a metadata lake?



IMPACT: Organizations recognize that accurate data inventories, enhanced data context for security tools, and increased sensitivity awareness significantly improve security posture, streamline operations, and enable proactive risk management.

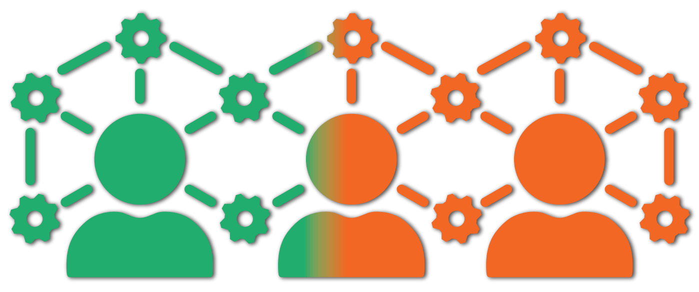
AI Security Reality Check

7 What are your biggest AI security hurdles?



IMPACT: Difficulty classifying and tracking AI training data, along with entitlement controls, increases breach risks and regulatory non-compliance. Organizations must improve AI data governance to secure their evolving data ecosystems.

8 How confident are you in controlling sensitive data used for AI/ML training?

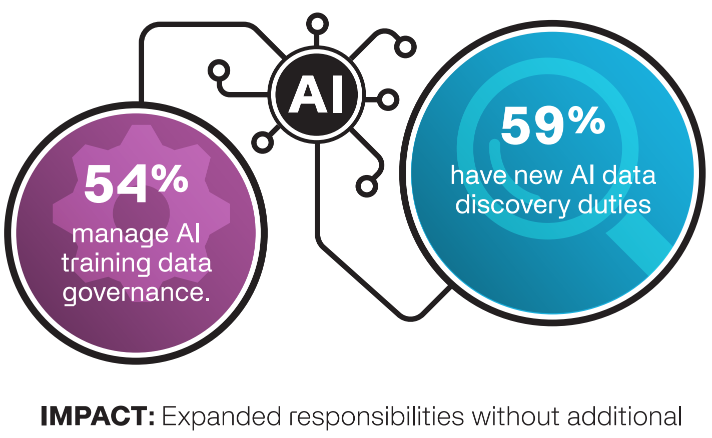


Less than half **48%** express high confidence.

IMPACT: Low confidence in AI/ML data controls raises the risk of unintended data exposure, compliance penalties, and reputational damage. Stronger AI data governance is required for secure, compliant AI adoption.

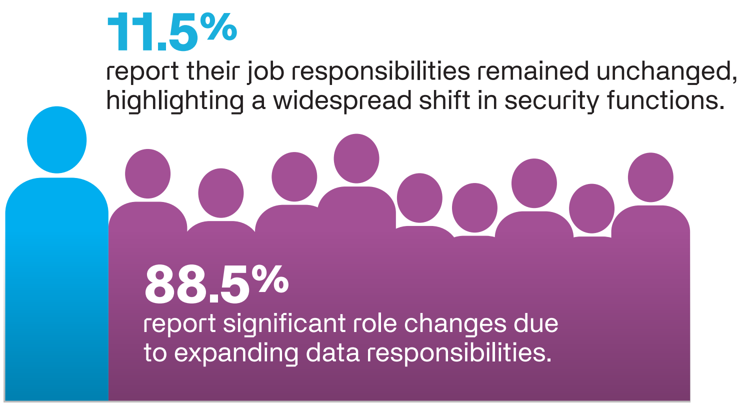
Security Team Role Evolution

9 Have your security responsibilities expanded due to AI adoption?


AI
54% manage AI training data governance.
59% have new AI data discovery duties

IMPACT: Expanded responsibilities without additional support stretch security resources thin, creating vulnerabilities through operational gaps. Clear, consolidated processes are needed to effectively manage growing AI data responsibilities.

10 Have security roles evolved beyond traditional boundaries in the past year?



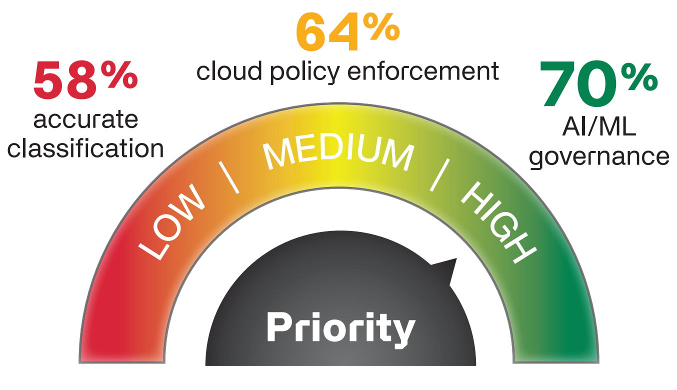
11.5% report their job responsibilities remained unchanged, highlighting a widespread shift in security functions.

88.5% report significant role changes due to expanding data responsibilities.

IMPACT: Expanded responsibilities without sufficient resources or automation can create security blind spots and operational bottlenecks, increasing the likelihood of data breaches and compliance failures.

2025 Security Focus Areas

11 What are your top data security priorities for 2025?



IMPACT: Prioritizing AI governance, cloud policy enforcement, accurate data classification, and data-aware security tools illustrates a strategic shift toward proactive, data-centric security approaches to reduce risk and ensure compliance.

Survey Methodology

- 530 security and IT professionals participated.
- Respondents included CISOs, IT Security Managers, Security Engineers, GRC professionals, and Data Managers.
- Organizations ranged from 1,000 to 50,000+ employees across multiple industries

About Bedrock Security

Bedrock Security, the ubiquitous data security and management company, accelerates enterprises' ability to harness data as a strategic asset while minimizing risk. Its industry-first metadata lake technology and AI-driven automation enable continuous visibility into data location, sensitivity, access and usage across distributed environments. Bedrock's platform continuously catalogs data, enabling security, governance and data teams to proactively identify risks, enforce policies and optimize data usage — without disrupting operations or driving up costs. Trusted by leading financial institutions, healthcare providers and Fortune 1000 companies, Bedrock Security empowers organizations to improve data security posture management (DSPM), confidently deliver Responsible AI initiatives, and manage the exponential data growth. Learn more at **www.bedrocksecurity.com**