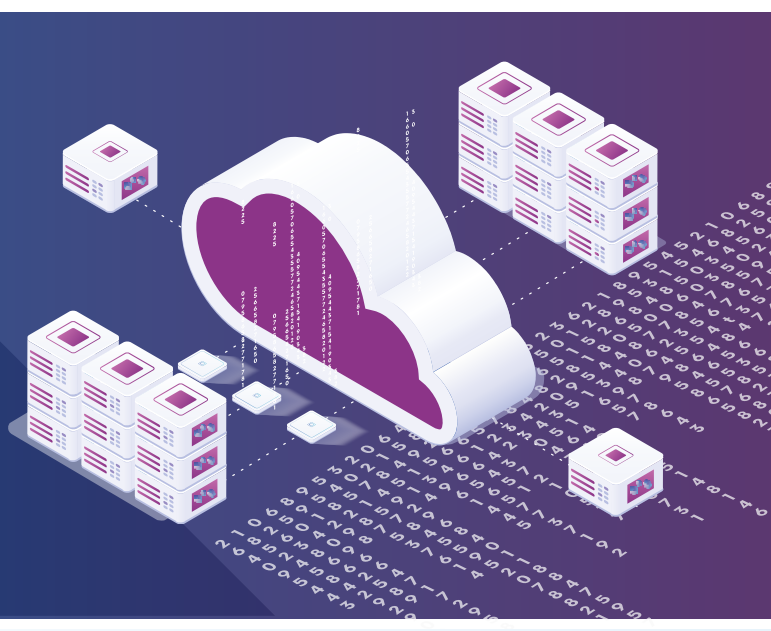
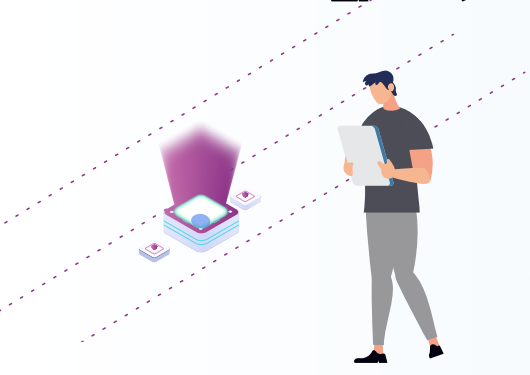
Identity-First Cloud Security Is Essential



An IDC infographic, sponsored by Ermetic

Demand for cloud infrastructure and applications is skyrocketing. But as more users and services access sensitive data in the cloud, the risk of breaches is growing. Organizations are increasing spending on cloud security but continue to struggle with visibility and access control. Ermetic and IDC's State of the Cloud 2021 Survey indicates organizations should consider a new approach to protecting their data.



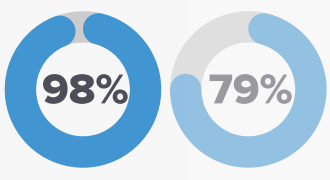
70%

of organizations surveyed spend more than $10 million per year to grow their cloud infrastructures.

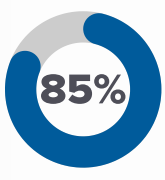
85%

of organizations expect to increase their security spending this year. 38% of those with large cloud footprints anticipate a budget increase of more than 10%.

Sensitive Data Is Being Exposed



98% of organizations experienced at least one cloud data breach in the past 18 months — up from 79% in the 2020 survey.



of organizations with large cloud footprints said their sensitive data has been exposed in the cloud.

Identity and Access Are Leading Risk Factors

of large enterprises cited access vulnerabilities as a primary root cause of their cloud data breaches.

Nearly

of organizations spend 25+ hours a week on Identity and Access Management (IAM) in cloud infrastructure.

Yet ...

More than

of organizations said lack of visibility and inadequate IAM security are major threats to their cloud infrastructures.

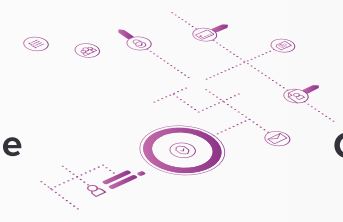
Top 5 Security Priorities for CISOs and Other Security Decision Makers

#1
Compliance Monitoring

#2
Security Governance and Management

#3
Addressing Data Privacy Issues

#4
Access Risk in the Cloud



#5
Cloud Infrastructure Security

Survey findings indicate the need for an approach to cloud infrastructure security that addresses access risks holistically and applies automation and remediation across the life cycle of identities, entitlements, and configurations.

Identity First

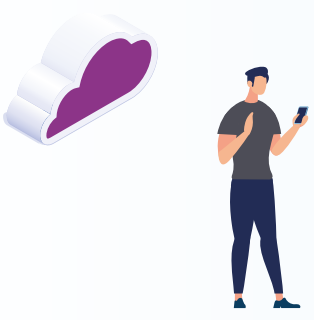
An identity-first approach is essential to tackling one of the leading security risks to cloud infrastructure: identities. Proactive and reactive security practices need to be built into the earliest stages of IT and application development.

Automation

Multi-cloud environments are the new, increasingly complex reality for organizations. Automation is the only way to stay on top. Automation offers unified visibility, prioritization and remediation — and least privilege guardrails.

Continuous Lifecycle

The dynamic nature of the cloud calls for continuously eliminating risky access by combining smart technology with IT and business processes. Collaboration across security stakeholders — IT, DevOps, and executive management — is crucial.



Survey Methodology
n=200 in the United States

Industry Verticals:

Software | Retail | Healthcare | Finance | Pharma | Manufacturing

https://idc.com