Data Governance in a Multi-Cloud Environment

All organizations have sensitive data that needs to be protected from internal and external threats, in order to avoid business disruption. However, as data creation and consumption rates continue to skyrocket, so does the risk to the company. Reducing that risk becomes even more challenging when company data spreads across multiple cloud sources and users lose track of which files contain sensitive data and which ones do not.

> *When a client suffers a data breach or compliance violation, the impact is not only felt by the client but also by their provider*

Egnyte's Unique Approach

Finding and classifying sensitive data

Automatically Identify and inventory sensitive data across multi-cloud environments using hundreds of built-in data patterns, supported by proprietary AI.

Securing and controlling access to shared files

Access and share sensitive data on any device, in a controlled, secure manner, using advanced sharing controls and encrypted file delivery so that only authorized recipients have access to edit and download rights.

Detecting and recovering from threats

Detect malicious and anomalous activity using machine learning-based behavioral analytics with artifact-based protection and respond using snapshot and individual file-based recovery options.

Capability Details

Content Intelligence

- Sensitive data discovery across sources
- Document classification by type such as resumes, budgets, and more
- Content-aware lifecycle management
- Content-aware safeguards

Threat Detection

- Risk score identification
- Snapshot-based file recovery
- Suspicious login detection
- Unusual user behavior detection
- Multivariate anomaly detection

Multi-Cloud Support[1]

- Egnyte cloud repository
- Microsoft Office 365, Exchange Online, Windows file server
- Google Workspace, Gmail
- SharePoint Online/OneDrive, Box, Dropbox
- Amazon S3, Azure Storage, Google Cloud Storage

Ransomware Detection & Recovery

- Risk summary dashboard
- Snapshot-based file recovery
- Zero-day behavior-based detection
- Artifact-based detection and blocking
- Issue alerting
- File version recovery
- Assisted recovery services

Data Privacy & Compliance

- Pre-programmed compliance policies
- Audit and breach reporting
- Legal hold
- Data subject access requests (DSARs)
- GDPR EU data residency

Access Governance

- Two-factor authentication
- Strong password policy enforcement
- Global file access policies
- Granular sub-folder permissions

Take the next step: Learn more at egnyte.com/msp

[1] Not all capabilities are available on all sources

EGNYTE | PARTNER PROGRAM

Egnyte fuels business growth by enabling content-rich business processes, while also providing organizations with visibility and control over their content. Egnyte's cloud-native content platform leverages the industry-leading content AI engine to deliver a simple, secure, and vendor-neutral foundation for managing content across business applications and storage repositories

CONTACT US

+1-650-968-4018
1350 W. Middlefield Rd.
Mountain View, CA 94043, USA
egnyte.com/msp