# Egnyte for Private Equity Firms



Funds managed by Private Equity (PE) firms and the sensitive information they possess make them a frequent target of cyber criminals. These malicious adversaries have ample opportunities for attacks, such as targeted phishing, spoofing and digital impersonation, where large amounts of money could be siphoned during the course of a complex deal. According to a recent study by Performance Improvement Partners, PE firms are under constant attack.

- Phishing scams happen **up to 50 times per day per employee**.

- The average firm experiences **2 to 3 cyber incidents per month**.

- It is estimated that an average of **1 in 4 middle market firms will suffer a cyber breach each year**.

Unfortunately, security practices adapted to the complexity and regulations of the PE industry and the intensity of financial deals are often seen as a blocker rather than an enabler for the business.

> ...80% of private equity houses have had a breach in the last 12 months and the time it took for them to discover that they had been breached was 8 months.
>
> **— Neil Hampson |** Partner, UK Cyber Security Leader, PwC

# Address Data Risk with Egnyte's Unique Approach

Egnyte assists more than 100 PE/VC customers with a simple yet powerful solution to manage and secure data flows for sensitive and deal-critical information. Ideal for small and mid-sized PE organizations that conduct highly-sensitive transactions with a larger number of advisors, the solution minimizes risk in reputational and regulatory damage.

Egnyte provides a simple, unified platform to protect, govern, and share sensitive data with advisors, employees and clients. It's rapid to deploy, easy to use and purpose-built with features that support sensitive transactions, such as deal activities, bidding, and contract negotiations.

### Locate & Classify Sensitive Data

Automatically identify and inventory sensitive data wherever it resides using hundreds of built-in data patterns, supported by proprietary AI. A governance risk dashboard displays where risk is present, allowing IT teams to remediate issues quickly.

### Securely Share Sensitive Documents

Share and access sensitive data with financial partners on any device, in a controlled, secure manner, using encrypted file delivery, digital watermarking and view-only and preview-links, ensuring that only authorized recipients have access to edit and download rights.

### Detect & Recover From Threats

Least-privilege, granular permissioning models reduce the attack surface. Ransomware detection combines machine learning-based behavioral analytics with artifact-based protection to identify malicious and anomalous activity like renaming, deletions, downloads and changes in file entropy.

For a detailed overview of Egnyte's capabilities, **sign up for Egnyte's Data Governance Test Drive.**

---

## EGNYTE

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multicloud businesses. More than 17,000 organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere. Investors include GV (formerly Google Ventures), Kleiner Perkins, Caufield & Byers and Goldman Sachs. For more information, visit **www.egnyte.com.**

### CONTACT US

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