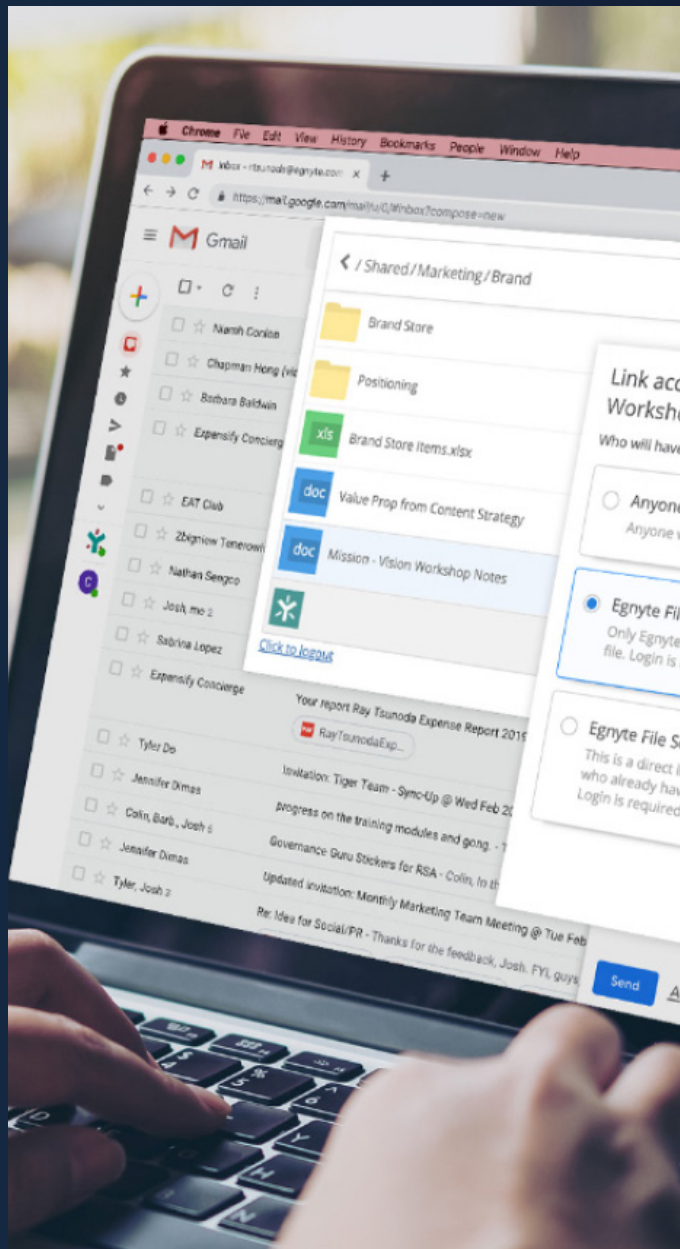
EGNYTE Google Cloud

Data Security in the Cloud Made Easy

Reduce Complexity, Cost, and Cybercrime

Egnyte and Google Cloud walk through modern data sprawl challenges in the cloud and protecting your company from sensitive data breach risks



A single data breach costs a company an average of $9.44 million in the United States, the highest of any country.

A 2023 Cybersecurity Ventures report predicts global cybercrime damages will exceed $10.5 trillion by 2025.

Is Your Company Under Threat?

Companies store data across countless locations. Workers can share it from home, on the road, on job sites, across offices, and with outside contractors, suppliers, and clients.

Your data comes from many sources and is constantly shared. How do you truly know where sensitive information is held, who's accessing it, how they're using it, and who they're sharing it with?

Amid surging cybersecurity attacks and increasing regulatory demands, organizations must enact strict controls around sensitive, regulated, and proprietary information – now.

Google Cloud and Egnyte have outlined the risks and challenges that companies of all sizes face today around data security.

These cloud security experts also outline solutions to those challenges and the results you can expect from tightening your company's security controls.

93%

of IT leaders believe new threats will drive increased security demands requiring a deeper level of access control and inspection[1]

[1]NTT, 2021 Global Workplace Survey

The IT Challenge

IT teams are tasked with protecting exponentially expanding amounts of data and meeting complicated, evolving compliance requirements. They're often asked to do this without intuitive, automated tools or large, dedicated teams.

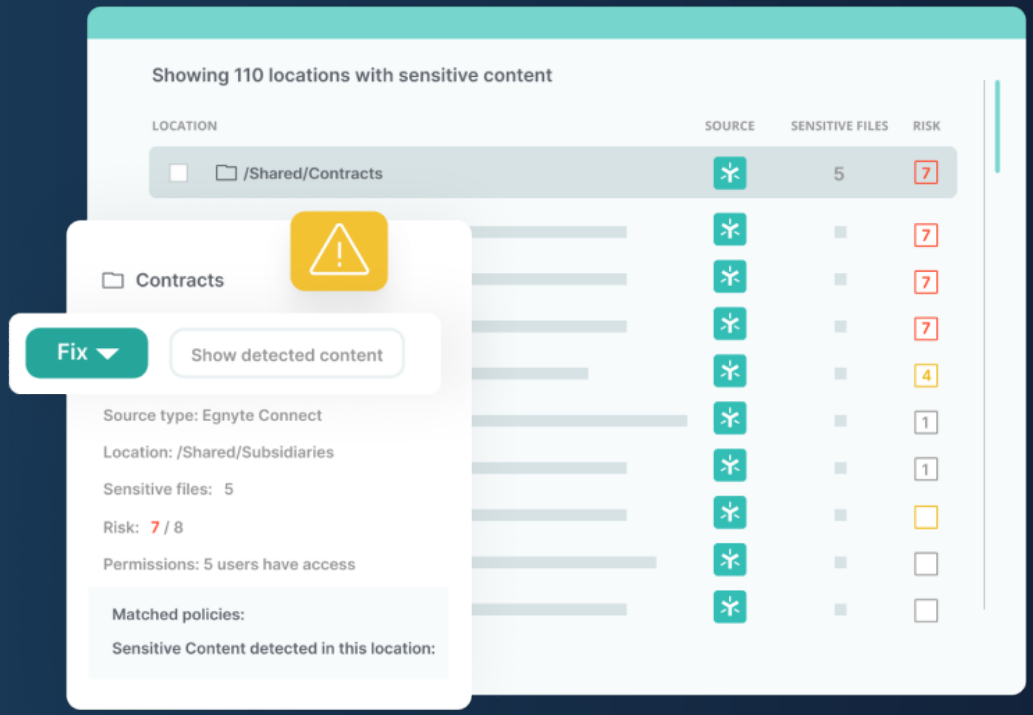
Processes are regularly manual and flawed, leading to inevitable security gaps and resulting in security breaches.

Security gaps occur when:

- Complex IT environments lead to petabytes of unregulated, unsecured, and unchecked data.
- New users and applications (such as SaaS apps) are added, removed, modified, or duplicated.
- Organizations with small IT teams – or no dedicated IT team – must secure expanding environments with limited resources and time.
- Companies still use manual, legacy data security and monitoring tools that require constant, time-consuming manual intervention and updates.

51% of surveyed companies manage **10+ data repositories**[2]

43% of IT professionals report adding a new SaaS app that **stores sensitive data** in the past 12 months. **42%** cite **difficulties in securing SaaS data**[3]



[2] Egnyte, Cybersecurity Trends for Mid-Sized Organizations
[3] Better Cloud, 2023 State of SaaSOps

EGNYTE Google Cloud

The Startling Ease of Exposing Sensitive Data

What are people sharing?

It's remarkably simple to misstep when sharing sensitive information and data. It's equally as easy to accidentally leave it exposed for curious eyes to find or cybercriminals to exploit.

These real-world examples give insight into how easy an oversight can be.

Activision data breach (2023)

- Exposed employee data, including emails, cell phone numbers, salaries, and work locations.
- Cause: Phishing attack on an HR employee.

Radiant Systems data breach (2022)

- Exposed personal information of over 100 million Radiant Systems patients, including names, addresses, and medical records.
- Cause: Employee accidentally left a hard drive containing sensitive data unencrypted in public.

T-Mobile data breach (2021)

- Exposed personal information of over 50 million customers, including names, addresses, and Social Security numbers.
- Cause: Employee accidentally left a laptop containing sensitive data unencrypted in a public place.
- T-Mobile suffered a second breach in 2023.

Capital One data breach (2019):

- Exposed the personal information of over 100 million customers, including Social Security numbers, credit card numbers, and bank account numbers.
- Cause: Employee clicked on a phishing link.

Data breaches can have severe consequences, including:

- Company closures
- Fines
- Lost consumer trust
- Denial of service
- Stolen proprietary or private customer data
- Lost time and productivity
- Insecure collaboration

[4] Verizon, 2023 Data Breach Investigations Report

Can your company afford to lose trust and clients?

The three leading causes of error-related data breaches are:

43%

Misdelivering sensitive content to the wrong recipient

23%

Showing proprietary data to the wrong audience

21%

Misconfiguration[4]

Do You Need a New Approach to Protecting Data?

Ensure that your company uses best-of-breed data security to help protect your business

Does your team struggle to:

- Detect and classify sensitive information?
- Enforce data-safeguarding policies?
- Better manage retention, archival, and deletion?
- Restore snapshots of large file and folder structures with minimal effort?
- Detect unusual user behavior?

To assess your current secure data protection tools and strategies, **Google Cloud and Egnyte** recommend you ask your teams these ten questions:

1. Are we aware of all the sensitive content types stored in our technology ecosystem?
2. Where exactly is our sensitive content stored?
3. Who's accessing it? What are their typical work patterns (locations, times of day, devices, etc.)?
4. Who are they sharing it with? Are they using secure means?
5. Do the right people have the correct permissions to the right data?
6. Can IT secure our data without having direct access to it, such as board documents?
7. How old is our sensitive data? Do we have automated data governance to manage and archive it properly?
8. Are our data security measures up to date with current regulations?
9. Are we prepared for future regulatory or contracting needs?
10. Do our current data protection tools hamper collaboration and productivity?

If your teams are unsure of these answers, it's time for a change.

EGNYTE Google Cloud

Egnyte on Google Cloud simplifies how you manage, secure, and govern content wherever work happens. Egnyte layers Google Cloud's advanced security technologies and rock-solid, scalable infrastructure with additional automated discovery, security, and control measures. With seamless Google Workspace integration, employees can keep working with the tools they like, even within content stored in secure enclaves.

What Data Types Must Be Safeguarded?

Personally identifiable information (PII)

Credit card data (PCI-DSS)

Protected Health Information (PHI)

Regulated financial information (FINRA, SOX)

Life sciences research and other data (GxP)

Controlled Unclassified Information (CUI) and Federal Contract Information (FCI)

Board and executive communication

Human resources documentation

Securing Your Sensitive Data: Do It the Right Way

With Egnyte and Google Cloud, organizations can take a multi-layer approach to secure sensitive data

Organizations across multiple verticals rely on Egnyte and Google Cloud to help users collaborate on protected files while meeting stringent regulatory requirements, including:

- **HIPAA:** Health information privacy and security.
- **GDPR:** Personal data privacy in the European Union.
- **ECCPA:** Personal privacy data in California.
- **SOX:** Investor protection from fraud.
- **PCI DSS:** Credit card data protection.

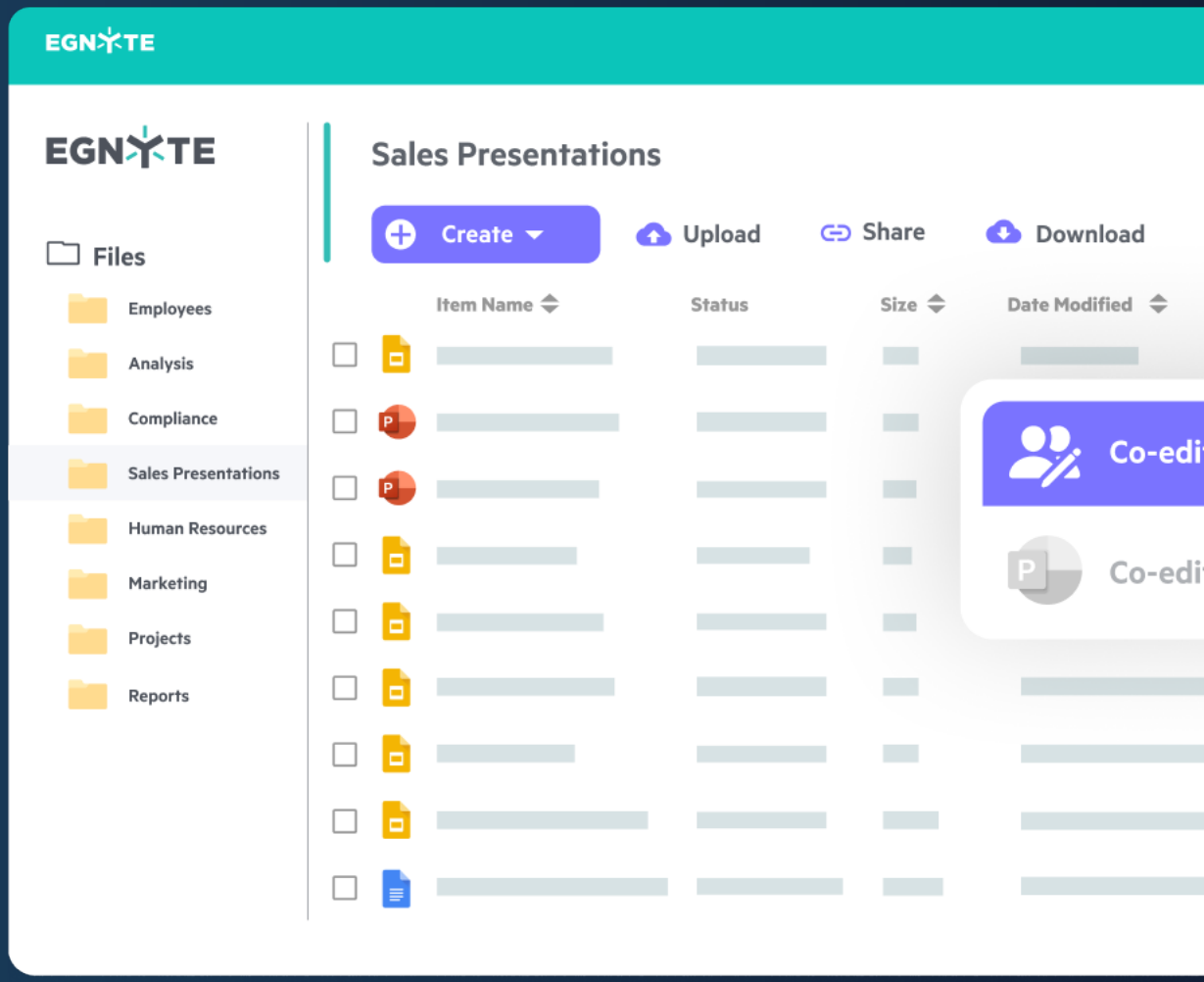
Egnyte and Google Cloud are compliant with all of these regulations and requirements.

Egnyte on Google Cloud simplifies how you manage, secure, and govern content wherever work happens. Egnyte layers Google Cloud's advanced security technologies and rock-solid, scalable infrastructure with additional automated discovery, security, and control measures. With seamless integration with Google Workspace, employees can keep working with the tools they like, even within content stored in secure enclaves.

The partnership also offer features to help organizations comply with data privacy regulations, such as:

- **Data encryption:** Encrypt data both at rest and in transit to help protect it from unauthorized access.
- **Audit trails:** Keep detailed audit trails of all user activity to help organizations track and investigate data breaches.
- **Role-based access control (RBAC):** Organizations can define fine-grained access controls for users and groups to help restrict access to sensitive data.
- **Data loss prevention (DLP):** These features can help organizations prevent sensitive data from being accidentally or maliciously shared.

Egnyte enhances Google Cloud's Zero Trust core security capabilities. The partnership enables discovery and rule-based access controls for documents across Google Workspace, Google Cloud Storage, and other third-party data repositories and clouds.



Building Better Ways to Work - From the Ground Up

The Egnyte and Google Cloud partnership offers exceptional benefits

Let's dive into how the collaboration between Egnyte and Google Cloud will benefit your business.

- **Enhanced security**
  Egnyte's security features, such as granular permissions, auditing, and encryption, combine with Google Cloud's infrastructure security to provide comprehensive security.

- **Improved compliance**
  Egnyte's compliance features, including data loss prevention (DLP) and eDiscovery, combine with Google Cloud's compliance offerings to help organizations meet regulatory requirements.

- **Increased productivity**
  Egnyte's collaboration features, such as real-time file sharing and co-editing, combine with Google Cloud's productivity tools to help teams work more efficiently. These tools include Google Docs, Sheets, and Slides.

- **Simplified IT management**
  Egnyte's cloud-based platform and Google Cloud's managed services make it easy for IT teams to manage and deploy the solution.

- **Collaboration features**
  Egnyte and Google Cloud offer many collaboration features, such as real-time file sharing, version control, and commenting. Teams can efficiently work together on documents and other files, regardless of location.

- **Global reach**
  Deploy the solution to users anywhere in the world.

- **Scalability**
  Easily add users or storage as needed.

- **Reliability**
  Be confident that your data is secure and accessible.

- **A single platform for all your content**
  Store, manage, and collaborate on all content, regardless of format or location.

- **A future-proof solution**
  Egnyte and Google Cloud are committed to innovation, so you can be confident that your solution will stay up-to-date with the latest technologies.

- **Cost-effectiveness**
  Egnyte's cloud-based solution eliminates the need for organizations to invest in and maintain their infrastructure. Egnyte leverages Google Cloud's economies of scale and offers several features to help organizations reduce costs.

EGNYTE Google Cloud

Why Egnyte and Google Cloud?

Learn how easy it can be to protect your organization's most sensitive data

Automation for always-on content compliance and management

Every piece of content needs to be evaluated, scrutinized, and controlled to help your business stay compliant and reduce the risk of breaches. No company has the staffing resources to perform this work manually at the pace or volume required. Intelligent automation is critical for keeping up.

With Egnyte and Google Cloud, you can take advantage of automation at every step of the content management process while meeting compliance expectations and best practices.

Egnyte on Google Cloud provides:

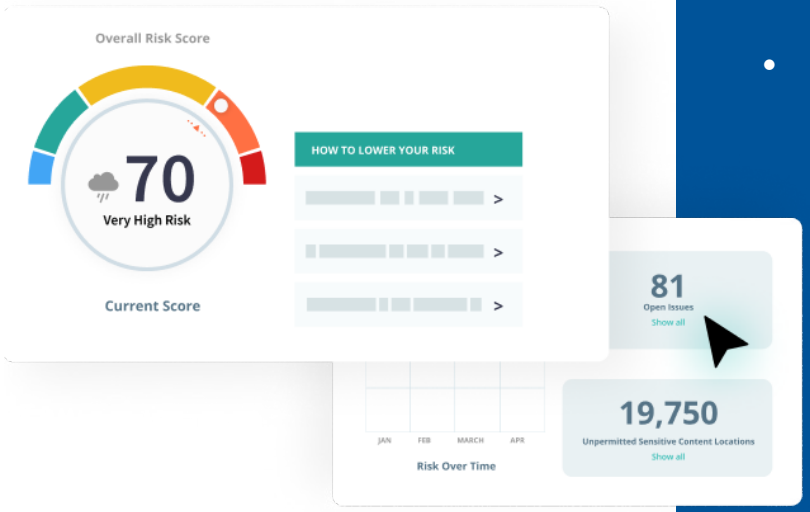
- **Content discovery:** Take advantage of hands-off and always-on content discovery in hybrid and multi-cloud environments as soon as data is created. Easily locate PII, PHI, CUI, GxP (for life sciences), payment card information, and other sensitive data.
- **Secure enclaves:** Egnyte creates secure enclaves for your data. With these enclaves, you can still give the right users seamless access via Google Workspace tools like Docs, Sheets, Slides, Gmail, and Drive.
- **Abnormal behavior detection:** Rely on machine learning-powered, behavior-based detection that can spot abnormal behaviors. These behaviors may indicate a ransomware attack or unusual amounts of file movement and encryption.
- **Access safeguards:** Automatically restrict sensitive content access to minimum security levels based on content matching, risk score, storage location, and other variables.

Easier to Manage, Easier to Work

Ensure data security is no longer a burden

Work moves fast these days. Egnyte and Google Cloud care just as much about smooth collaboration as they do data security — and it strikes the perfect balance.

At the same time, it's simple to manage. One IT staff member can handle it, freeing your team's time for other priorities.



Your end users will benefit from:

- Access controls that remove the guesswork and burden from working compliantly.
- Sensitive data-sharing alerts embedded in daily workflows, r einforcing best practices without impeding work.
- Seamless collaboration and access using Google Workspace and Google Cloud, no matter where data is stored.
- The ability to maintain familiar letter folder structures, easing the transition to working in the cloud.
- Support for on-site, multi-location, and field data access needs, including extensive file access and syncing without VPN.

Your IT staff will benefit from:

- A single command point with visibility. See where sensitive data is located, how it's being shared, real-time threats and anomalies, and benchmarks for measuring progress.
- Automated, purpose-built secure enclaves with preconfigured settings for standard regulations and purposes.
- Granular file-level controls and automated rule enforcement.
- Threat prioritization, automated actions, and recommended mitigations.
- Audit-ready access tracking.
- Snapshot recovery for ransomware attacks or accidental deletion.
- Supported integration with leading security information and event management, security operations center, and identity management systems.
- Rules-based automated data governance, including retention, archiving, and deletion, to reduce attack surfaces and support legal compliance.

EGNYTE Google Cloud

Egnyte on Google Cloud: Data Security Without Limitations

Egnyte is built on Google Cloud's rigorous Zero Trust security and shared-fate model with limitless scalability.

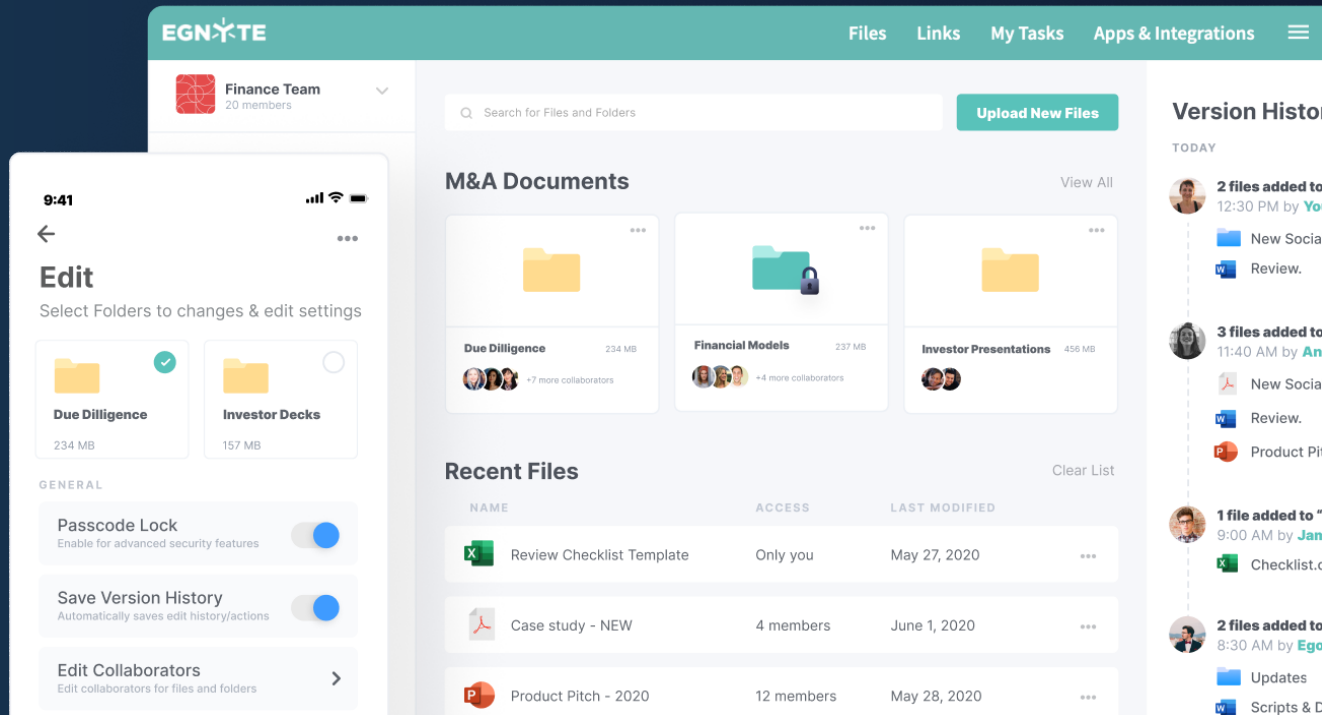
Our secure enclaves reside in Google Cloud Storage, and Kubernetes-based elasticity enables Egnyte to meet the needs of our customers without latency. Your most sensitive content is always protected.

The result?

- Time, resources, and costs savings (and management headaches). Reduce legacy data center hardware with a consolidated tool that provides a cloud file system, data management, and content security.
- Minimizing compliance, regulatory, and security risks, which can be expensive and detrimental to the business.
- Increasing growth opportunities. Expand into such areas as government contracting, large enterprise clients with more stringent security, and regions that require data residency.
- Utilizing Google Cloud commitments to increase efficiency, scalability, and resilience in data and content security and management.
- Efficiently and securely sharing and work with data between teams, systems, and use cases. Improve these efficiencies by leveraging cloud-architected solutions like Egnyte with open APIs, pre-built integrations, a single flexible source of truth, and advanced file sync.
- Relieving overburdened IT teams so they can focus on other valuable and rewarding tasks.

Buy without procurement red tape on **Google Cloud Marketplace** using your credits, or visit **Egnyte.com** for a free trial.

Start Free Trial



EGNYTE Google Cloud