EGNYTE CONNECT℠

Whitepaper

Egnyte Security Architecture

A Comprehensive Approach to Security

TABLE OF CONTENTS

ABOUT EGNYTE

Egnyte transforms business through smarter content allowing organizations to connect, protect,and unlock value from all their content. Our Content Intelligence platform delivers smart content collaboration and governance in the cloud or on-premises to thousands of businesses around the world even the most regulated industries. Founded in 2007, Egnyte is privately held and headquartered in Mountain View, CA. Investors include venture capital firms, such as Google Ventures and Kleiner Perkins Caufield & Byers, as well as technology partners, such as CenturyLink and Seagate Technology.

CONTACT SALES: 1-877-7EGNYTE

INTRODUCTION – THE NEED FOR A SOLUTION MADE FOR THE ENTERPRISE

While ready access to information fuels a company's ability to collaborate, innovate and grow, exfiltration and compromises to that information can have devastating effects on the company's ability to succeed. Safeguarding sensitive information, regulated data, and intellectual property is crucial to protecting the reputation, ongoing operations, compliance and productivity of the business.

The only way to ensure that data is simultaneously available and secure is with a file sync and share solution that has been architected to meet these potentially competing demands for the enterprise. Freemium, consumer-oriented solutions, which have been developed to foster rapid user-base growth, do not have the built-in controls required by enterprises to mitigate the risks posed by all the services/applications and devices (BYOD) being used to access, share and store corporate information. In fact, the use of consumer-based cloud apps within enterprises (shadow IT) can create huge blind spots within IT's operations that place the overall business at risk.

Organizations need a solution that puts their interests first, which means they need a solution that has been purpose-built to give them complete control over how their data can be accessed and shared by different users (both inside and outside the organization), with different devices. To ensure adoption, however, the solution needs to also support the requirements of users, making it easy and convenient for them to work with the service to get work done, without putting corporate data at risk.

Egnyte Connect secure file sharing solution was architected keeping in mind the needs for an enterprise. It enables businesses to regain control over their corporate data, with a platform that gives IT teams the comprehensive data visibility and protection they require, and users the ability to work with any application or device they want to easily and securely access and share information, with colleagues, both inside and outside the business.

The unique enterprise architecture from Egnyte Connect provides the end-to-end data protection needed to enable companies to confidently support collaboration, while addressing compliance and security requirements. This white paper reviews how Egnyte Connect delivers that comprehensive, world-class data security, privacy and control to organizations at every layer.

> "Egnyte Connect secure file sharing solution was architected keeping in mind the needs for an enterprise."

SECURE DEPLOYMENT OPTIONS

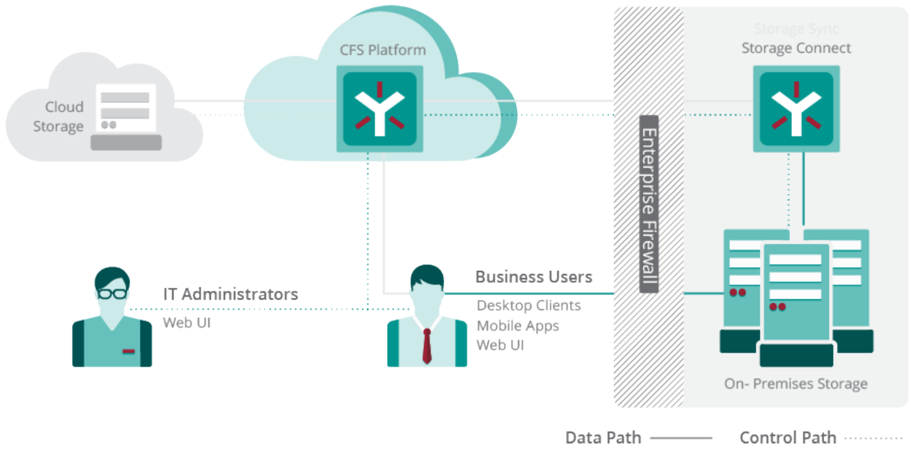
Cloud, On-Premises, and Hybrid

The first step to securing an enterprise's data, is determining where the data is going to be stored. Organizations need to understand the value different information has to their business and classify it accordingly, based on its security and privacy needs. Some data is governed by regulations and regional requirements that dictate where it must reside. For example, there are a host of industry-specific regulations that cover how data must be protected. In addition, many countries have their own data restrictions and laws that require the company to maintain data sovereignty and residency (often within a defined country border).

Egnyte Connect is the only file sharing platform that offers multiple storage deployment models and a completely storage agnostic solution, to enable customers to choose the secure, storage options they need to meet all their compliance and business requirements. Customers can store and manage data within Egnyte's secure cloud infrastructure, their own enterprise data center ,or use popular public cloud platforms. Egnyte Connect allows customers to use any combination to meet their unique needs.

This support for multiple deployment options allows IT to keep data where it belongs, and ensure its security and privacy.

"Egnyte has local data centers in the regions in which it operates to support compliance with data sovereignty and residency laws."



Secure File Storage in the Cloud

When enterprises move to the cloud, they need to trust the cloud vendor has deployed all appropriate measures to effectively protect their information. Since Egnyte purpose-built its solution for the enterprise, customers can be confident it delivers all the enterprise-grade security they require. Egnyte has local data centers in the regions in which it operates to support compliance with data sovereignty and residency laws. It implements industry best practices, providing a fully encrypted, fully redundant cloud storage solution to meet an enterprise's security and availability requirements.

Support for 3rd Party Cloud Storage

Egnyte Connect offers enterprises a choice. If customers want to leverage an existing investment they have made in a cloud storage provider, they are free to use that cloud storage solution. Egnyte supports all major third party cloud storage providers, such as Amazon AWS, Google Cloud, Microsoft Azure, or any other S3 compatible cloud storage, ensuring enterprises can design a solution that best meets their unique needs.

Secure File Storage in the Datacenter

For customers who want to keep their data on-premises, Egnyte Connect enables secure access to files stored behind the firewall with no files or metadata every touching the cloud. This option still meets an organization's strict regulatory and security requirements, while delivering VPN-less access to authorized users both internal and external to the organization.

Keep Data "In Place"

Unlike cloud-only solutions that require businesses to move vast amounts of data into the public cloud, Egnyte Storage Connect is designed to deliver access and sharing to data stores "in place", without transferring and storing data online. Storage Connect can leverage any existing storage platform and file access protocol, without requiring additional proprietary file system protocols.

Support Remote, VPN-Less Access

Egnyte Connect allows enterprises to link any number of storage systems with any number of access devices (smartphone, tablet, computer) to enable users to securely access all their files stored on any on-premises storage, anywhere in the world, without the need of a VPN. Egnyte Storage Connect separates the control plane from the storage plane to provide mobile and remote VPN-less access to any local storage, without files or file metadata passing through the cloud. This enables users to securely share and access private files from any device, anywhere in the world, while data remains stored behind the corporate firewall - free from privacy risks and in compliance with regulatory data residency requirements.

Secure Hybrid File Storage

Egnyte Connect provides the flexibility to deploy a solution that automatically syncs files stored in the cloud with multiple on-premises locations to ensure users always have access to the latest documents, wherever they are located. In addition, Egnyte can synchronize content between sites to improve availability at remote locations that have unreliable connectivity or limited bandwidth. This protects against disruptions from network outages, enhancing the overall availability and performance of an organization's data. For example, if the WAN goes down or the on-premises storage becomes unavailable, user at the affected location maintain seamless access to their files.

PHYSICAL SECURITY

Datacenter Security

For data stored in Egnyte's datacenters, Egnyte protects the servers where the data resides, housing our application and storage in industry-leading Tier III, SSAE 16 compliant co-location facilities that feature 24-hour manned security, biometric access control, and video surveillance. All servers reside in private cages that require physical keys to open. All datacenters hosting these servers are audited regularly for potential risks and limitations.

Egnyte Connect datacenters are set up to protect company data from hardware and environmental risks. Datacenter servers are maintained in a strictly controlled atmosphere to ensure optimal performance and protection. They are also designed to withstand natural disasters including fires and earthquakes up to an 8.0 magnitude. To ensure uninterrupted accessibility of data, servers are equipped with redundant electrical supplies, protecting against unforeseen power outages and electrical surges. Power is drawn from two separate power grids, while the facilities house redundant UPS modules and a generator to protect from wider power outages.

> "Egnyte datacenters are set up to protect company data from hardware and environmental risks."

System and network performance is continually monitored by Egnyte and datacenter operations to ensure continuous data availability. To learn more about Egnyte's datacenters, please contact Egnyte for the Datacenter Protection Document.

Application Resiliency

Even under the most secured environments, data is still at risk due to unexpected hardware failures. Hard drives, servers, even the datacenter itself can endure natural wear and tear that can lead to data corruption. Egnyte takes several steps to protect customer data, files, and business rules from all these potential risks across the entire Engyte instance.

To protect from equipment failure, we ensure all files are continuously replicated across the storage cluster and off-site locations to protect against larger failures. Data stored on these servers is continually monitored to protect against bit decay that threatens the integrity of files at rest

Egnyte Connect ensures a fully redundant application setup that is resilient to hardware and network failure, and it all starts with the patented Egnyte Object Store (EOS). EOS utilizes a fully redundant architecture to provide application and storage resiliency. To accomplish this, EOS incorporates a resilient active-active design that continuously monitors the status of the solution and can automatically transition to a backup storage cluster or datacenter in the event of a hardware, software, or network outage.

> "Egnyte ensures a fully redundant application setup that is resilient to hardware and network failure, and it all starts with the patented Egnyte Object Store."

TRANSMISSION SECURITY

Encryption

Transferring files online from one network to the next can leave the data vulnerable to data interception. Companies and international government agencies alike have recognized this security risk. To make sure customers transmit their data to/from Egnyte services via secure, encrypted channel, Egnyte keeps its TLS/HTTPS configurations up to date with the latest security standards.

Egnyte Connect has adopted TLS 1.2 as the primary transmission protocol that is used by the most secure institutions in the world. Egnyte uses 256-bit AES encryption to encrypt data during transmission. 256-bit AES encryption is one of the strictest standards applied by the US Government for TOP SECRET documentation and ensures that, even if company data were intercepted, it would be impossible to decipher. Egnyte's encryption system can also be utilized to share files externally with clients, versus sending unsafe email attachments. This allows businesses of any size to leverage data encryption to secure all file sharing and collaborative efforts.

NETWORK SECURITY

Intrusion Detection

Data stored in even the most secure locations must be guarded against network intrusions. This is true for data stored on local company servers, as well as data stored in remote datacenters. While many companies struggle to update their infrastructure to defend against the latest intrusion risks, Egnyte takes away that burden by using cutting-edge technology and working with leading industry experts to ensure unrivaled data protection.

In order to police traffic between public networks and the servers where company data resides, Egnyte employs ICSA-certified firewalls. These firewalls are built to recognize and handle multiple synchronous threats (e.g. DDoS attacks), without performance degradation. The network uses TLS/SSL encryption and a Network Intrusion Prevention System that monitors and blocks hackers, worms, phishing, and other infiltration methods. Any attempts to infiltrate the system produces an automatic alert, which Egnyte's trained security team immediately investigates and remediates. In addition to the network firewalls, the datacenter uses separate local firewalls to provide an additional layer of data protection.

Even with these defenses, Egnyte recognizes that hackers are continually becoming more sophisticated in their intrusion attempts. To keep up with the latest security measures, Egnyte employs a multi-pronged strategy to protect against threats, which will be described in the next section. Egnyte also retain logs and performs real-time analysis to proactively monitor network activities.

Egnyte Connect takes additional measures to protect uptime by implementing network hardware redundancies to ensure company data is not only safe, but also readily available. All Egnyte Connect servers are hosted on redundant local area networks that are linked to Tier-1 carriers through multiple fiber-optic lines. To learn more, please contact Egnyte for the Datacenter Protection Document and the Third-Party Security and Penetration Test Document.

> "Data stored in even the most secure locations must be guarded against network intrusions."

DATA SECURITY

Data at Rest

Even with every door blocked and every entrance guarded, Egnyte Connect takes no chances with customer data. Egnyte recognizes that any file system can have unforeseen risks that could threaten data integrity. That's why Egnyte takes an additional step to encrypt data at rest. All the data stored on Egnyte's servers is automatically encrypted using AES 256-bit encryption, so that if someone were to gain access to data on the servers, it would be impossible to read. The encryption key is stored in a secure key vault, which is a separate database accessible only to the two executive heads of Egnyte's Security Council. Additionally, data is stored in a hashed structure that can only be navigated through the Egnyte proprietary system software.

Egnyte Connect Object Store

Egnyte Connect has built its own, patented storage management system, called Egnyte Connect Object Store (EOS). EOS was developed to support enterprise-class security and scalability, enabling higher performance and flexibility with dynamic unstructured data. This distributed model stores data within independent silos (based on client domains), so data of one client domain is never cross-contaminated or de-duped with others. Independent silos also enable clients to efficiently encrypt data on private storage and manage their own keys. Egnyte can also support third party object stores from all major third party cloud storage providers, such as Amazon AWS, Google Cloud, Microsoft Azure, or any other S3 compatible cloud storage solutions.

> “For customers that want more control, they elect to manage their own keys.”

File Encryption and Key Management

As a system default, Egnyte Connect uses AES, with 256-Bit encryption, which is what the U.S. government uses for their most sensitive documents, to encrypt data. In line with industry best practices, Egnyte uses a hardware security module (HSM) to encrypt and decrypt files, as well as manage and secure the cryptographic keys.

Object Store/ Storage	Egnyte Connect Managed Key	Customer Managed Keys		
		AWS CloudHSM	Azure Key Vault	SafeNet HSM
Egnyte Cloud	✓	✓	✓	✓
Google Cloud	✓	✓	✓	✓
Amazon AWS	✓	✓	✓	✓
Microsoft Azure	✓	✓	✓	✓
S3-compliant Object Storage	✓	✓	✓	✓
CIFS Storage	N/A	N/A	N/A	✓

For customers that want more control, they elect to manage their own keys using Amazon AWS CloudHSM or Microsoft Azure Key Vault cloud-based services, or they can deploy a SafeNet HSM in their own datacenter. No other vendor offers this level of flexibility.

Digital Rights Management

Egnyte Connect offers robust digital rights management (DRM) capabilities that deliver granular file controls for sensitive materials, such as legal documents and intellectual property. With Egnyte, customers can use preview only links that prevent downloads, printing and copying; they can secure named distribution, as well as take advantage of detailed tracking for complete visibility into the activity surrounding these files.

Data Leakage Prevention

While Egnyte's visibility and controls protect against data leakage, customers can also choose to add layers of data leakage prevention with Egnyte's out-of-box integrations with solutions from leading security vendors. More information on Egnyte's security partners can be found here at the Egnyte partner showcase page.

Application/Data Vulnerability Detection

Egnyte has a multi-pronged strategy to detect and remove vulnerabilities to keep customer data safe. Egnyte's in-house security team is continuously monitoring the applications and infrastructure, conducting regular penetration tests, security audits and code reviews, both automatically and manually, in line with the highest standards of Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). Egnyte also provides security training to all product and engineering teams to ensure security is built into the Software Development Life Cycle (SDLC), from the design phase to the implementation, testing and deployment of the solution.

Egnyte uses a 3rd party enterprise application security platform to continuously monitor the live production site and identify any vulnerabilities in the web application. This platform assesses all the critical classes of technical vulnerabilities, including the Open Web Application Security Project's (OWASP) Top 10 list. In addition, all clients undergo a manual security audit, which is conducted on a periodic basis.

Egynte's unique Smart Reporting also uncovers risks to data that can support quick mitigation. Customers receive reports on data, user and device activity, as well as overall storage utilization, that can be used to optimize and strengthen the enterprise's security. Egnyte monitors and analyzes an enterprise's overall application/data usage, highlighting any changes that could indicate a breach or potential issue that needs to be investigated and remediated.

> "Engyte delivers the visibility and controls enterprises need to support their data retention, archival and discovery activities."

Data Retention, Archival and Discovery

Engyte delivers the visibility and controls enterprises need to support their data retention, archival and discovery activities. With Egnyte, customers have the ability to drive centralized policies around how and when data should be retained and managed. As opposed to consumer-based, cloud-only solutions that were designed to meet the needs of the individual user, Egnyte was built from the ground up to address enterprise requirements. As such, Egnyte provides centralized visibility and control over trash folders, allowing configurable retention and API access. As a result, customers can enforce enterprise-wide retention and versioning policies. They can also create and manage archive instances in support of custom searches for e-discovery.

Data Removal

For all Egnyte Connect's accounts, deleted files are automatically sent to the Trash folder, which only Administrators can access. Administrators can restore files from the Trash folder to reverse accidental deletions. After files have been in the Trash folder for the designated and configurable period, they are emptied and completely removed from Egnyte's system. Administrators may request to be notified before the content in the Trash folder is emptied. To ensure compliance with data removal, Egnyte overwrites company data with random patterns of information to render the data unrecoverable. The following removal process is followed:

1. The original data and all file versions are removed from Egnyte servers.
2. Replicated backup copies on local storage are removed.

3. Replicated backup copies on secondary datacenters are removed.
4. The removal process deletes all metadata associated with the removed files, including notes, access history, thumbnails, and indexing content used in searches.

Egnyte maintains an audit trail of all data removed, which can be viewed by account administrators through their audit reports. Egnyte also has a robust trash management API for customers that desire additional flexibility and control, via external applications.

> "Egnyte maintains an audit trail of all data removed, which can be viewed by account administrators through their audit reports."

ACCESS CONTROL

The centralized management of Egnyte makes it easy for IT to see and control exactly who can do what with corporate data, both inside and outside the organization.

Roles-Based Administration

Enterprises can set up granular access policies based on a user's role in the organization, giving IT full control over the types of applications (including 3rd party apps) they can access and use. Enterprises can create multiple user roles to accommodate different access needs. For example, a department assistant can be allowed to add and remove users within that department and an operations manager can run usage reports.

User Types

Egnyte enables enterprises to define a user's role and then determine exactly what they can do. As a result, Egnyte enables organizations to fully control what users can access and do, regardless of whether they are internal or external to the enterprise. In general, there are the following types of users:

- **Administrators:** employees assigned to manage and perform administrative functions. There are typically only a few Administrators and they are usually part of the IT team
- **Power Users:** typically, full-time employees.
- **Standard Users:** typically made up of non-employees, such as consultants and contractors, that are extensions of the company and need secure access to internal files to conduct business. A standard user allows authenticated and managed access to enterprise content.
- **Anonymous External Users:** typically, business partners and others, who need to collaborate with the company but do not need authenticated access to files.

For each type of user, IT can determine what they can access and do:

User Type	Access Methods	Administrative Capabilities	Functional Capabilities
Administrators	Web UI Mobile Apps Desktop Apps Mapped Drive	Manage all content, users, devices and policies	Create Content Share Content Edit Content Private Folder Access
Power	Web UI Mobile Apps Desktop Apps Mapped Drive	Can optionally manage users, groups, run reports, administer retention policy/trash etc.	Create Content Share Content Edit Content Private Folder Access
Standard	Web UI Mobile Apps	N/A	Access files from shared folders Upload/modify/delete files*
Anonymous External Users	Web Browser on Laptop or Phone/Tablet	N/A	Download files shared using link Upload files from a shared upload link

*With appropriate permissions

"Most of the security threats today are a result of compromised user credentials."

User Authentication

IT administrators know the most vulnerable point of any infrastructure is on the login screen. This is why Egnyte enables strict user authentication and permission enforcement at every access point, ensuring only users with the right credentials can access company data. Enterprises can use their existing corporate identity management systems, such as AD, LDAP or SAML 2.0, to authenticate users and ensure consistent policy enforcement.

Two-step Login Verification

Most of the security threats today are a result of compromised user credentials. With Egnyte's Two-Step Login Verification, administrators can require an extra login credential as part of the user authentication process. The additional login step requires users to verify their identity through a phone call or SMS message, creating a double check for every authentication. By enforcing an additional phone-based verification upon user login, Egnyte customers can prevent account breaches, even when user credentials are compromised.

Login Credentials

Within the company domain, all users are required to enter their username and password. Administrators can set user password complexity and length. Additionally, Egnyte monitors and logs all access attempts to customer domains; any suspicious activity alerts the system administrators who then can investigate the issue.

In order to protect login credentials, user passwords are hashed using Bcrypt. This one-way hash function cannot revert to the original password. Even when two identical passwords from different users are stored in the server, the hashed passwords appear different, making it impossible for anyone to decipher the original characters. As an additional precaution, only Egnyte's proprietary software can detect which hashed credentials belong to which user.

Even without knowing the login information, unauthorized users can still find ways to access company data by piggy-backing on the user's computer while they are logged into the platform. This is true for any web application, whether accessing a bank account website or personal email. Egnyte is fully aware of these attempts and takes multiple steps to prevent unauthorized access after a user has logged in, issuing a session-specific cookie that keeps users logged into their account for a limited time only. This cookie expires after a certain period of inactivity, which is set by the account administrator, requiring users to log in again.

Password Policy Management

Egnyte Password Policy Management allows IT administrators to set mandatory employee password rotations and leverage account lockouts after failed logins. Mandatory password rotations greatly reduce the exploitation of default and guessable employee credentials. Account lockouts prevent brute force password attacks, by immediately locking out the access point after multiple failed login attempts. Once set up, Administrators can monitor password change histories. These best practice access controls allow IT to enforce stringent business policies, adding an extra layer of password protection against unauthorized use and unwanted intrusions.

Active Directory/LDAP/Single Sign On Integration

Large organizations with existing authentication systems in place can choose to integrate their Egnyte account directly with their Active Directory (AD) deployment. This allows companies to embrace the cloud without decentralizing user management. As users are created and deleted from Active Directory, they can be automatically granted or denied access to Egnyte's Adaptive File Services. The full range of password and lockout policies set in Active Directory are enforced across all Egnyte access points. (E.g. after three failed login attempts within a 15-minute window, the user account is locked out).

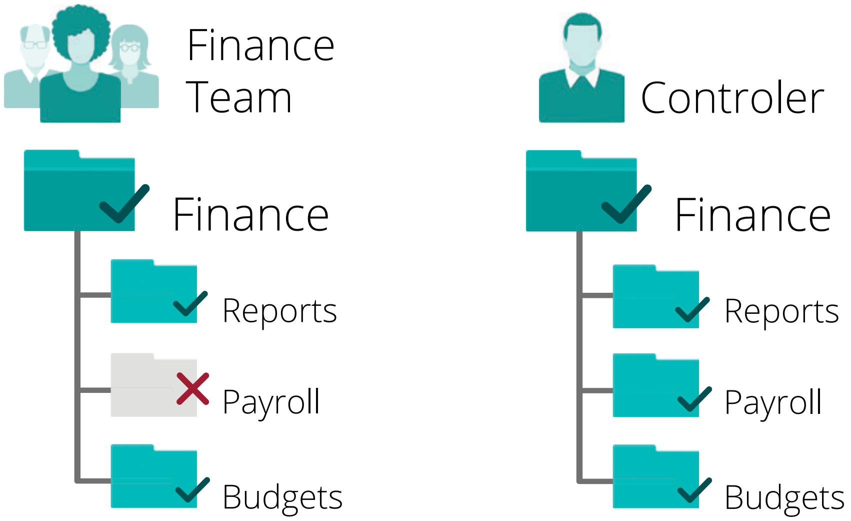
Egnyte also supports OpenLDAP, Single Sign On (SSO) through SAML 2.0, and partner integrations with a host of leading identity management solutions. This allows businesses to seamlessly integrate Egnyte into their existing workflows.

Permission Controls

Egnyte provides advanced access controls Administrators can use to assign and manage folder and sub-folder permissions. These access controls are critical to the implementation of the data's structure and hierarchy. Administrators have the ability to set granular folder and sub-folder permissions for each individual user (none, read only, read/write, read/write/delete). Access permissions are always uniformly enforced, irrespective of location and access method (web browser, mapped drive, secure FTP, desktop sync, mobile/tablet app).

> "Egnyte provides advanced access controls Administrators can use to assign and manage folder and sub-folder permissions."

Folder and sub-folder permissions can be broken down into three categories: inheritance, exclusion and group.



> “Egnyte Connect provides group management functionality, allowing permissions to be easily set for an entire team within a company.”

Inheritance

- Folder permissions set at the parent levels in a hierarchy are automatically inherited by any sub-folders.
- Example: The Corporate Controller has access to the Finance parent folder, which also means they have access to the sub-folders within Finance.

Exclusion

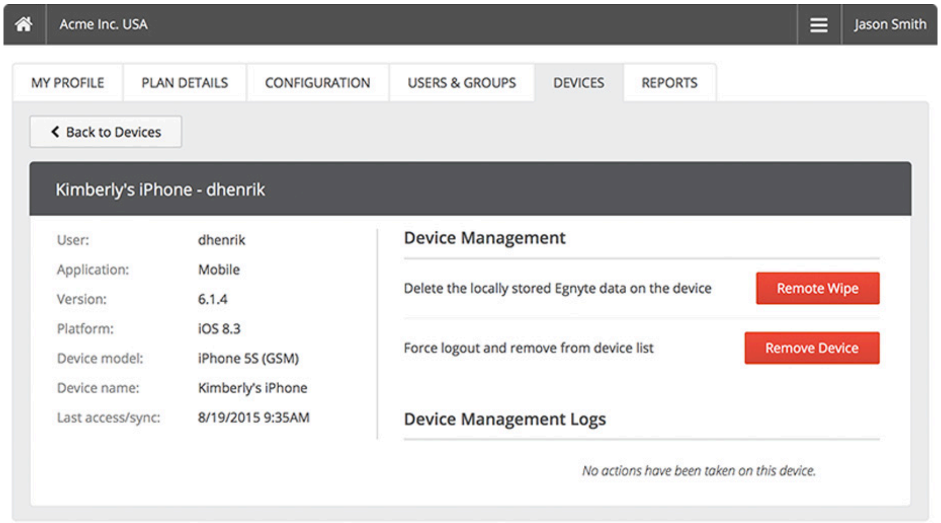
- Permissions can be excluded at any level of a deep folder hierarchy.
- Example: The Finance parent folder has 3 sub-folders: Budgets, reports and payables. The entire finance team needs access to the Finance folder, with the exception of the budgets sub-folder. The budgets sub-folder should only be accessible by the Corporate Controller.

Group Management

- Egnyte provides group management functionality, allowing permissions to be easily set for an entire team within a company. Groups can include any combination of employees and business partners to meet the collaboration needs of the department.
- Example: A group can be created for the entire finance team.

DEVICE CONTROLS

Egnyte provides IT with a centralized dashboard to control and monitor all employee devices. Within the device control panel, administrators can enforce additional security settings to manage desktops, laptops, mobile phones and tablets. Egnyte can integrate with enterprise mobile management (EMM) and mobile device management (MDM) containers to ensure consistency in controls; Egnyte can also use their mass deployment capabilities to securely download the Desktop Sync client (for those customers who want local, high speed access/offline access to their files), with SCCM.



Kimberly's iPhone - dhenrik

User:	dhenrik
Application:	Mobile
Version:	6.1.4
Platform:	iOS 8.3
Device model:	iPhone 5S (GSM)
Device name:	Kimberly's iPhone
Last access/sync:	8/19/2015 9:35AM

Device Management

Delete the locally stored Egnyte data on the device

Force logout and remove from device list

Device Management Logs

No actions have been taken on this device.

> “In case an employee device is lost or stolen, saved files can be instantly erased by the administrator or device owner.”

Enterprise Mobility Management (EMM) Integration

Egnyte seamlessly integrates with EMM platforms allowing businesses to install and manage the Egnyte mobile applications within a broader set of mobile policies defined for the enterprise. Egnyte’s mobile apps can be deployed from an enterprise app store, managed with the EMM platform and remotely wiped in the case of a lost device.

However many enterprises are yet to implement an EMM solution. For such customers Egnyte provides a host of native device control capabilities outlined below.

Mobile Passcode Lock

Businesses can minimize security risks in the event employee mobile devices are lost or stolen. Administrators can set mandatory passcode locks, requiring users to enter their pin after they login or their device is idle. As an additional safety precaution, locally stored mobile files can be automatically wiped after a set number of incorrect passcode attempts.

Offline Access Controls

Administrators can control whether employees can download files locally on their mobile devices and how often local files are periodically deleted. By turning off local downloads, documents can only be viewed online, preventing offline access of sensitive data.

Remote Wipe

In case an employee device is lost or stolen, saved files can be instantly erased by the administrator or device owner. Administrators or device owners can quickly initiate wipes of Egnyte files on mobile apps and Desktop Sync clients from a web UI, which provides a central view of all end-user devices. Regardless of the device (Windows, Mac, iOS or Android), administrators and device owners can remotely erase Egnyte content stored on that mobile client to prevent unauthorized access to files.

Local Encryption

When using Egnyte, files are protected during transmission and at rest through government-grade 256-bit AES encryption. For customers looking for additional mobile security, local file encryption is available for smartphones and tablets. This provides complete end-point encryption, so even in the event of data leaks or device theft, customer files are always encrypted.

> “Files are protected during transmission and at rest through government-grade 256-bit AES encryption.”

OPERATIONAL SECURITY

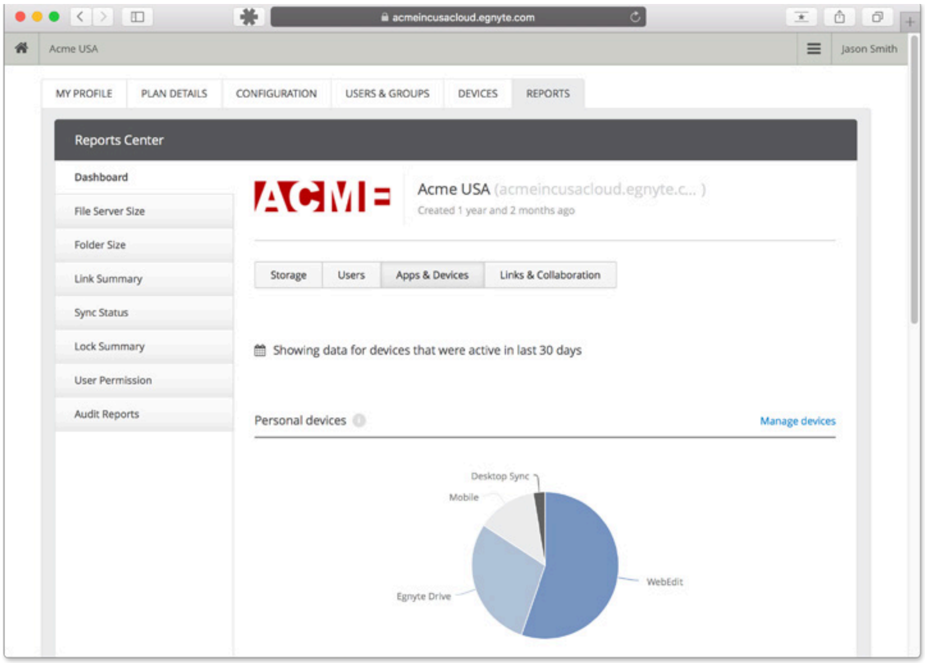
Administrative Access Controls

Only a few designated Egnyte Operations Administrators have the clearance level to access Egnyte’s datacenter (for inspection, maintenance, etc.). These key members undergo third-party background checks and stringent security training. This team only has the access required to perform scheduled hardware maintenance. Any operational activity, including facility access, replacing hardware components and removable media is monitored and audited.

Other members of the Operations team that are System and Application administrators must meet stringent requirements before being granted the appropriate privileges to perform regular system maintenance tasks. Egnyte continually monitors access logs to ensure that at no time can external sources access customer data.

Smart Reporting and Auditing

Egnyte Connect gives organizations comprehensive dashboards of system-wide analytics around content, users, devices, applications and more to help identify potential threats within the environment. The first service of its kind, Egnyte gives Administrators unprecedented visibility and control across an organization’s entire content lifecycle, so they can make informed, data-driven choices around their content.



Acme USA (acmeincusacloud.egnyte.c...)
Created 1 year and 2 months ago

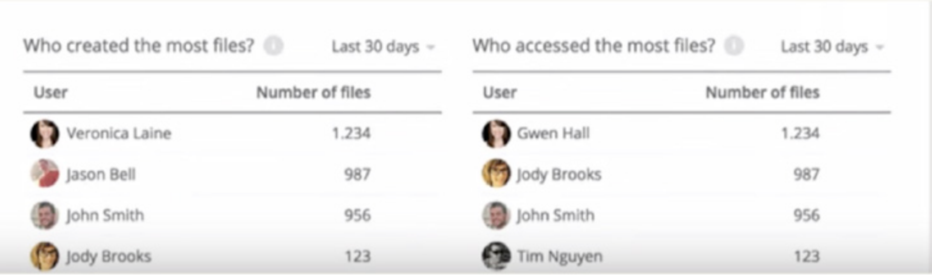
Showing data for devices that were active in last 30 days

IT leaders are provided access to unique insights about user, file, and device activity that can be harmful to their organization, so they can take appropriate measures to strengthen their security or eliminate the threat. The Smart Reporting and Auditing service generates preventative alerts that notify IT about suspicious activities, internally and externally, to help the business maintain security and compliance.

> “Smart Reporting and Auditing service generates preventative alerts that notify IT about suspicious activities, internally and externally.”

For instance, Administrators can see the number of logins by device type that have taken place over the last month. If there is a large number of mobile user logins, when normally most logins are via a desktop, it may be indicative of a stolen credential or compromised device. Armed with this information, the company can investigate to understand what is really going on; based on what they find, they may move to quickly contain and remediate a breach, institute training to improve awareness around mobile threats, or develop a mobile permissions policy that aligns with their security requirements, etc.

Another example, the Smart Report below shows the number of files both created and downloaded. The top user has downloaded ten times more files than the fourth highest ranked user. Abnormal behaviors, such as this one, can point to potential security breaches, such as an employee leaving the company or a recently hacked account. This information alerts companies to a potential issue, so they can dig deeper — and if necessary — be proactive and take immediate action.



Who created the most files? Last 30 days

User	Number of files
Veronica Laine	1.234
Jason Bell	987
John Smith	956
Jody Brooks	123

Who accessed the most files? Last 30 days

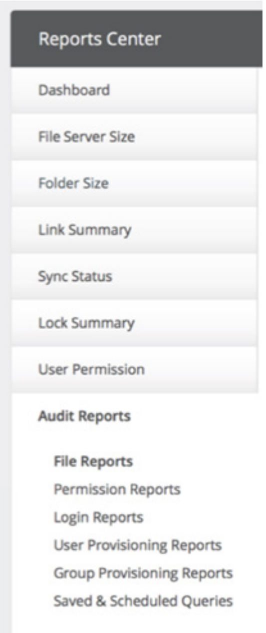
User	Number of files
Gwen Hall	1.234
Jody Brooks	987
John Smith	956
Tim Nguyen	123

Comprehensive Auditing and Reporting

Egnyte Audit Reporting helps IT proactively understand usage and behavior and audit their account for security risks. Egnyte offers administrators a wide range of real-time reporting tools to provide complete visibility of users, devices and data.

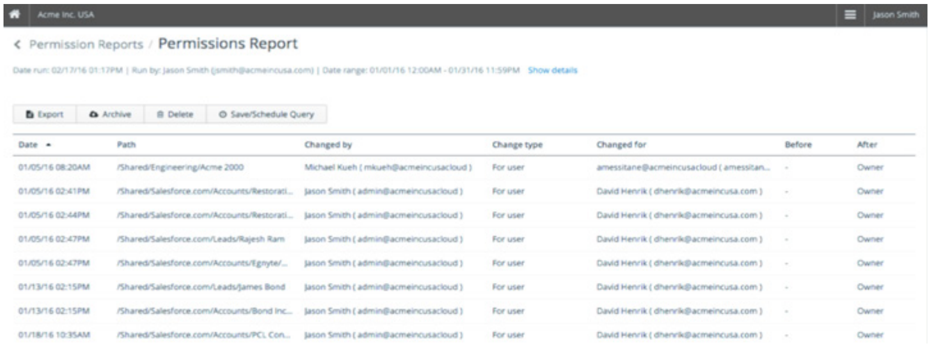
The audit reports provide a 360-degree view of all activities. Administrators can view all:

- User access activities (login, logout, password resets etc.) with specific IP address origination and device information.
- File activities (uploads, downloads, deletes, links shared etc.).
- Access permission changes (such as permissions granted or revoked from folders).



These auditing capabilities, combined with Egnyte's central administration, provides Administrators the full suite of enterprise controls they need to manage their account. This level of control and visibility is critical to ensure compliance to regulatory requirements, especially in industries such as healthcare and financial services.

> "Egnyte offers a FINRA compliant online storage solution, with end-to-end data protection."



Permission Reports / Permissions Report

Date run: 02/17/16 01:17PM | Run by: Jason Smith (jsmith@acmeincusa.com) | Date range: 01/01/16 12:00AM - 01/31/16 11:59PM

Date	Path	Changed by	Change type	Changed for	Before	After
01/05/16 08:20AM	/Shared/Engineering/Acme 2000	Michael Kueh (mkueh@acmeincusacloud)	For user	amessitane@acmeincusacloud (amessitan...	-	Owner
01/05/16 02:41PM	/Shared/Salesforce.com/Accounts/Restorati...	Jason Smith (admin@acmeincusacloud)	For user	David Henrik (dhenrik@acmeincusa.com)	-	Owner
01/05/16 02:44PM	/Shared/Salesforce.com/Accounts/Restorati...	Jason Smith (admin@acmeincusacloud)	For user	David Henrik (dhenrik@acmeincusa.com)	-	Owner
01/05/16 02:47PM	/Shared/Salesforce.com/Leads/Rajesh Ram	Jason Smith (admin@acmeincusacloud)	For user	David Henrik (dhenrik@acmeincusa.com)	-	Owner
01/05/16 02:47PM	/Shared/Salesforce.com/Accounts/Egnyte/...	Jason Smith (admin@acmeincusacloud)	For user	David Henrik (dhenrik@acmeincusa.com)	-	Owner
01/13/16 02:15PM	/Shared/Salesforce.com/Leads/James Bond	Jason Smith (admin@acmeincusacloud)	For user	David Henrik (dhenrik@acmeincusa.com)	-	Owner
01/13/16 02:15PM	/Shared/Salesforce.com/Accounts/Bond Inc...	Jason Smith (admin@acmeincusacloud)	For user	David Henrik (dhenrik@acmeincusa.com)	-	Owner
01/18/16 10:35AM	/Shared/Salesforce.com/Accounts/PCL Con...	Jason Smith (admin@acmeincusacloud)	For user	David Henrik (dhenrik@acmeincusa.com)	-	Owner

COMPLIANCE

Information Security Management System
ISO 27001
Certified
SOC3
SSAE 16
CERTIFIED
TYPE II
CSA
cloud security alliance®
HIPAA
Health Insurance Portability and Accountability Act
FDA
21 CFR Part 11
FINRA
SKYHIGH
ENTERPRISE-READY

ISO27001

Egnyte is ISO/IEC 27001:2013 certified. This is the leading information security standard around the world, and provides the requirements for an Information Security Management System (ISMS). The ISMS establishes the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed. This certification validates that Egnyte products, supporting infrastructure, people and processes operates within the best practices established by ISO/IEC 27001.

Financial Services

Egnyte offers a FINRA compliant online storage solution, with end-to-end data protection. Egnyte enables full compliance under SEC 17a-4, 31a, 204 and recordkeeping regulations for confidential data storage, retention, digitalization and accessibility. Egnyte is fully compliant with SOC 1 (SSAE 16 Type 2), SOC 2, SOC 3, as well as ISO 27001:2013; Egnyte has also received the highest rating from the Cloud Security Alliance (CSA).

Healthcare

Egnyte understands the importance of the confidentiality and security of an individual's Protected Health Information (PHI). Egnyte's comprehensive data security enables HIPAA/HITECH compliance for Payer, Provider, pharmaceutical and biomedical businesses. In addition, Egnyte is fully compliance with FDA 21 CFR Part 11, as well as the aforementioned SOC, ISO and CSA regulations.

EU Customers

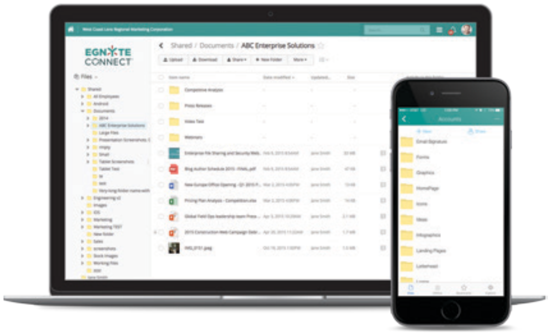
Egnyte complies with the European Union Data Protection Directive (EUDPD). The EUDPD was enacted to provide a consistent data protection framework with EU-level enforcement, and a baseline of security around information storage, transmittal, and processing. Egnyte stores all European customers' data and metadata in its European datacenter in Amsterdam. Data never leaves the EU; even when a customer opens a support ticket, it is handled by a European support team.

> "Egnyte stores all European customers' data and metadata in its European datacenter in Amsterdam."

European
Commission

SUMMARY

With the recent advancements in consumer-grade rogue file sharing solutions, IT is struggling with visibility and control over company data, users and devices. Egnyte puts IT back in control by providing market-leading Enterprise File Services with Egnyte Connect. It delivers end-to-end data protection, including storage, physical, transmission, network and data security, as well as access, device and operational controls. Egnyte empowers IT with the visibility they need to spot and stop potential problems and strengthen their overall data security, while maximizing their users' productivity. As the only file sharing solution that supports multiple deployment options, with cloud, on-premises and a hybrid solution, Egnyte provides flexibility and control needed to address the security, compliance and collaboration needs of the most demanding organizations around the world.



READY TO TRY EGNYTE CONNECT?

Start a free trial online, or contact our sales team today.

15-DAY FREE TRIAL

EGNYTE | Smart Content Collaboration & Governance

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

Egnyte transforms business through smarter content allowing organizations to connect, protect,and unlock value from all their content. Our Content Intelligence platform delivers smart content collaboration and governance in the cloud or on-premises to thousands of businesses around the world even the most regulated industries. Founded in 2007, Egnyte is privately held and headquartered in Mountain View, CA. Investors include venture capital firms, such as Google Ventures and Kleiner Perkins Caufield & Byers, as well as technology partners, such as CenturyLink and Seagate Technology.