



Egnyte Technical Overview

Winter 2023 Edition



Table of Contents

Introduction	3
Architecture	4
File Sharing & Collaboration	6
Ad Hoc Collaboration	6
Sustained Collaboration	9
Access Governance	16
Discovery & Classification	23
Lifecycle Management	26
Data Controls	29
Threat Management	31
Privacy & Compliance	39

Introduction

An organization's unstructured content, including product plans, customer data, and other IP, contains not only the most valuable form of data for most companies, but also represents the most difficult to secure and govern. It accounts for the vast majority of corporate data created (>80%), accessed and shared by end-users, and therefore poses a more significant risk, because the systems where it is stored (public email folders, collaboration systems, cloud storage services) are not easily integrated.

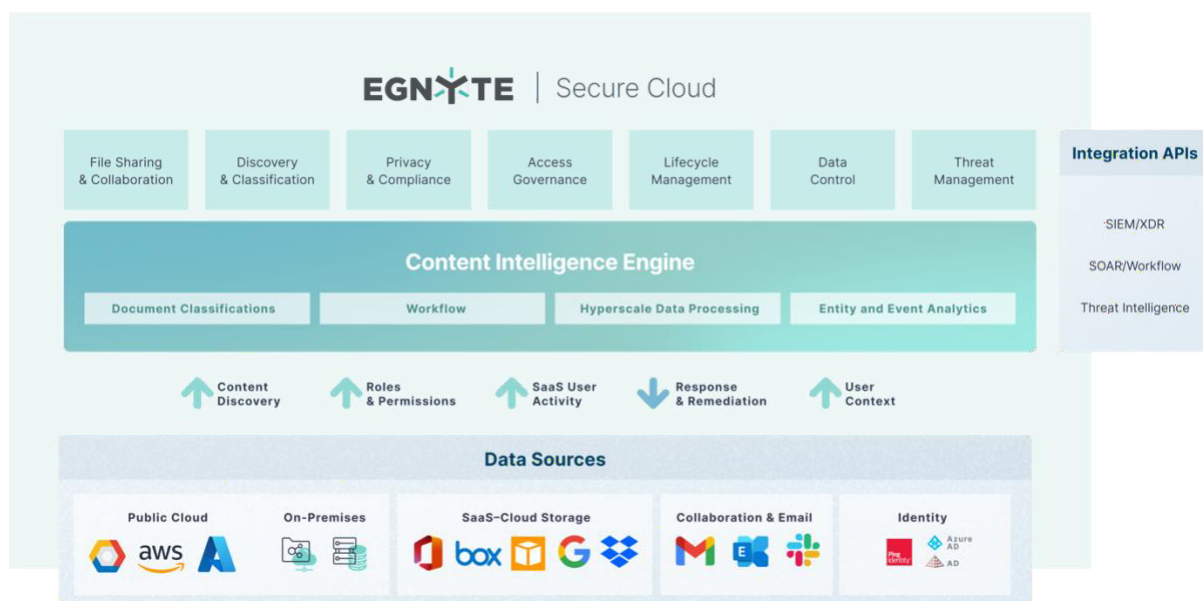
There are many solutions on the market today, ranging from free-to-use consumer tools to expensive and complex enterprise offerings. The former often lack centralized controls and adequate reporting, while the latter can overwhelm overcommitted IT organizations and understaffed security and risk teams. For thousands of companies, Egnyte's platform provides an ideal middle ground – protecting content from multiple vectors without compromising employee productivity.

As a unified solution, Egnyte provides the power of many tools in one: intelligent data discovery and classification, lifecycle management, access governance, threat management and secure file sharing and collaboration – to name a few. Simple to deploy and manage, Egnyte enables organizations of all sizes and industries to work faster, smarter, and safer.

Architecture

Egnyte provides organizations with a platform for identifying, classifying, managing, sharing, and securing sensitive data. Data can be stored in Egnyte applications for full control, in existing 3rd-party applications like Box, OneDrive, SharePoint, and Gmail, or in a combination of Egnyte and 3rd-party applications. Users can access data through existing 3rd-party apps and cloud services and Egnyte's web, desktop, mobile, and tablet apps.

Egnyte's integrations with over 170 popular applications allow users to use the business solutions they are accustomed to while organizations can manage, track, and protect data that flows through those applications.



Egnyte Object Store

Egnyte Object Store (EOS) is a patented storage management system that supports 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 from one client domain is never cross contaminated with another.

Independent silos also enable clients to efficiently encrypt data on private storage and manage encryption keys. Egnyte also supports 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.

Application Security

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

Vulnerability Management

Egnyte uses a third-party enterprise application security platform to continuously monitor its 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. The assessment also includes a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). In addition, all clients undergo a manual security audit, which is conducted on a periodic basis.

File Sharing & Collaboration

Good organizations encourage members to work together and contribute expertise for the benefit of a shared objective. Before networks, employees would circulate paper copies of documents and mark them up by hand. Later, as networking emerged, the same process was replicated by attaching documents to emails to be edited and returned. However, this method is still inefficient, error-prone, and slow - especially if multiple people are collaborating on a complex document or group of documents. The concept of collaboration itself needed to be revised.

Egnyte supports two fundamental types of advanced collaboration. The simplest is Ad-Hoc collaboration, in which users can share links to files rather than the files themselves. The advantages to this approach include compatibility with any media (not just email), reduced bandwidth, and the ability for the sender to continue working on the file, knowing the recipient will always see the latest version. The second model is “Sustained Collaboration” where work teams to share a common workspace environment for long term collaboration on complex projects. This requires advanced and scalable permissions. Both models require flexibility while still intelligently securing sensitive information, and both are well supported by Egnyte.

Ad Hoc Collaboration

For Ad Hoc collaboration, Egnyte provides a simple, secure, and efficient means for sharing files and collaborating between employees, partners, and vendors. It allows users to manage file access and share sensitive information securely while maintaining control of future downstream data use or resharing.

File Links

While users and administrators can allow access to folders through permissions, Egnyte also provides the ability to share files through links. This is useful when sharing large files that might trigger a size limit, such as an email attachment, or when sharing sensitive data requiring more stringent security controls.

Secure Delivery

Egnyte allows sensitive files to be shared in an encrypted form, accepting decryption only by recipients who have installed the Egnyte FileGuard client (available for PC and Mac) and confirmed their identity by responding to an email to the email address with which the file was shared. Once the link expires or is revoked, PC recipients will no longer have access to the shared file, even if they

Private link for "Client Presentation.pdf"

Who will have access?

Specific Recipients

Allow downloads?

Yes, encrypted

☒ Link expires

on date

Dec 10, 2021

When link expires, access to file will be automatically revoked

☒ Notify me when link is clicked

☒ Include file name in link

☒ Always show the most recent version of the file

downloaded it.

Preview-only Links

Preview-only links allow users to control a recipient's use of a file. The preview-only option prevents recipients from downloading or printing a shared file, as well as copy/pasting a file's contents.

Email-validated Sharing

When sharing sensitive content via email, it is critical that those receiving the data are the *intended* recipients and not someone with a similar email address, even more critical when using public email domains like Gmail. Egnyte supports this by validating email recipients when creating recipient-specific links.

When creating a Shared link, the recipients will be authenticated via email when they first access the link. If they access the link again in the future, they will be emailed an authorization code to unlock the shared content. With recipient-specific links, only the recipients indicated will be able to view the content, even if the link is forwarded to others.

Public link for "Client Presentation.pdf"

Who will have access?
Anyone

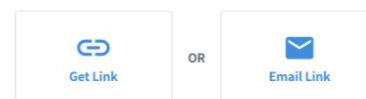
Allow downloads?
Yes

☒ Link expires
on date Dec 10, 2021

☒ Notify me when link is clicked

☒ Include file name in link

☒ Always show the most recent version of the file



Upload Links

Users can provide a link to allow non-authenticated recipients to upload files to a folder. The non-authenticated recipient is not allowed to see anything else in the folder.

Folder Links

In addition to links to share individual files, Egnyte also provides the ability to share folder links to recipients. This allows the sharing of large numbers of files with a single link.

Co-editing

Users can edit documents simultaneously using online tools from Google Workspace or Microsoft 365 Online. This is helpful for live editing sessions in conjunction with video conference software. In addition, users can edit online documents using a desktop application while the desktop client manages file synchronization behind the scenes. In this case, the file can be automatically locked during editing to avoid conflicting edits from different users.

File Versioning

As documents are often shared among a group of users, to ensure a record of changes and prevent unauthorized changes, Egnyte provides automatic file versioning. Users can revert to a previous version if a file is accidentally or erroneously overwritten. This feature can also be used to recover individual files in the event of malicious behavior or ransomware.

Versions

Download History

Every time somebody uploads a file, a new version is created. This server stores a maximum of 100 versions per file. Deleted versions are moved to the trash.

MODIFIED		UPLOADED	SIZE				
Oct 26, 2021	CURRENT	Oct 26, 2021 1:52 PM by Trevor J...	21 KB	Download	Preview	Delete	
Oct 25, 2021		Oct 25, 2021 2:52 PM by Trevor J...	28 KB	Download	Preview	Delete	Refresh
Oct 25, 2021		Oct 25, 2021 2:39 PM by Trevor J...	27 KB	Download	Preview	Delete	Refresh
Oct 25, 2021		Oct 25, 2021 2:28 PM by Trevor J...	26 KB	Download	Preview	Delete	Refresh
Oct 25, 2021		Oct 25, 2021 2:18 PM by Trevor J...	25 KB	Download	Preview	Delete	Refresh

Workflows

Users can add workflows to accompany documents stored in Egnyte. “To Do, Approval, and Review and Approval” workflows will automatically generate emails and track the next step in the process. Due dates can be assigned for individual steps, and signatures completed for approval. Documents are automatically locked while waiting for approval.

Commenting

In addition to traditional document commenting in Office 365 and Google Workspace, Egnyte supports native commenting which is visible to authorized users on the preview page for each document. This is helpful for discussions during the development of a document and to clarify steps in a review and approval workflow.

Custom Metadata

Administrators can allow users to add and edit metadata for files and folders within the Web UI. Metadata properties are displayed in the sidebar folder details pane to make finding related folders and files even easier. In addition, Egnyte preserves and can support external metadata such as Microsoft sensitivity labels through integrations with Microsoft Information Protection.

Search and Recent Files

Egnyte provides AI-driven search tools to help users find specific information across large folder structures in either files or folders. Recently accessed files are highlighted to help users find the latest information.

File Preview

Egnyte provides a preview capability to display the contents of a file in a browser window without having to open an editor. Many different types of file formats are supported including the most common word processing, spreadsheets, presentations, images, audio, and video formats. In addition, Egnyte supports “Preview-Only” links which only allow the recipient to preview, but not download or edit a file.

Sustained Collaboration

As stated previously, sustained collaboration is used by teams to share workspaces and resources. For sustained collaboration, work teams need additional tools to be able to access and work on the same documents together. Not only do they need the collaboration tools, but they also need an advanced permissions schema that scales while remaining manageable. Egnyte provides this capability with Folder permissions, Users, and Roles.

Project Folders

Egnyte supports project folders for those companies that organize work around projects. Project folders can be used as templates to start a new project, and equally importantly, are recognized by the system so that retention policies can be set up to automatically clean-up and archive associated documents after a project is closed.

Connected Folders

Connected folders sync folders stored on an end-user computer with specified folders in the cloud. Particularly useful for linking library folders such as Desktop, Documents, Pictures, and Downloads, this feature provides increased performance when working with large files. Any changes between the folder on the hard drive or the corresponding folders in the cloud are kept in sync in real-time and allow access to files when offline.

Video Transcoding

The video preview function converts flv, mp3, mp4, m4a, ogv, webm, wav, mov, avi, wmv, m4v, and mpeg type files and displays them appropriately. Viewing video in preview mode allows the user to watch a video immediately without having to wait for the entire file to download. It can also be used to protect the contents of the file.

Audit Reporting

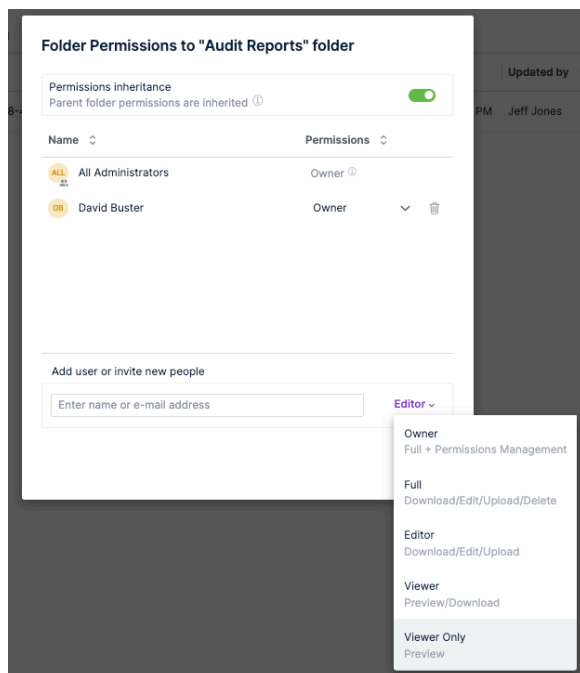
Egnyte provides a series of audit reports that summarize important insights for administrators. These include reports on: Files, Permissions, Logins, User Provisioning, Group Provisioning, Configuration Settings, Workflow Audits, and Saved/Scheduled queries.

Single Source of Truth

Because Egnyte creates a layer of abstraction between users and their data, significant flexibility is provided. A user can use the desktop app for simple “drive letter” access, browser access to the Egnyte domain, and a mobile app for remote access. Therefore, files can reside in multiple places, but the single source of truth is the Egnyte domain while the others are kept in sync.

Non-inherited Folder Permissions

Within Egnyte, permissions for folders are controlled by the data owner, relieving the burden from the IT team. This person can add or delete individual permissions to access the contents of the folder. Permissions for folders in competing systems are inherited from the folder above. However, this is not always preferred and can often lead to inadvertent exposure of sensitive information. Egnyte allows the data owner to over-ride inheritance and change the permissions on sub-folders to match business needs. This can often reduce the need to create separate folders inside and outside a folder structure.



As shown, individual permissions can be granted from very limited access all the way up to full ownership status. As permission levels increase, additive capabilities include Preview, Download, Upload, Delete, and permissions management itself. These permissions can be extended to both individuals and groups as needed.

User Types

Egnyte provides various default User types to deal with general business document access situations. The default configuration includes 3 main user types- Admin, Power User, and Standard User. Generally, these user types break down as follows. “Admin” users can configure the system and are therefore usually limited to trusted IT staff only. “Power Users” are typically active, full-time employees who need access to all features and capabilities of the system. Finally, “Standard

Users” are typically contractors, partners, or part-time employees who only need a limited set of capabilities. In each case, the individual capabilities of these user types can be modified to meet organization needs per the example screen below.

User Types

Roles

Power Users

can use Desktop Sync	Enabled	
can use the Desktop App	Enabled	
can view Users & Groups in Settings	Enabled	
can see all non-default groups	Enabled	
can invite Standard Users	Enabled	
receive folder notification emails	never	☒ users can override this setting
can receive the Egnyte newsletter	Enabled	
can view Activity in folders	Enabled	

Standard Users

receive folder notification emails	never	☒ users can override this setting
can receive the Egnyte newsletter	Enabled	
can view Activity in folders	Enabled	

User Roles

User Roles can be used to fine tune these capabilities even further. An admin can create custom User Roles based on the needs of the organization. Often, these are used to confer unusual capabilities to specific groups of people. For example, Senior executives, trusted contractors, or even team leaders can be given additional capabilities. In the example below, the “CIO Role” has been created to provide additional capabilities to the CIO.

User Types

Roles

Roles

Role Name ^	Users
CIO	0
contractor	0
Default	13
DevOps	0
HR Manager	0
Security Admin	0
Team Lead	3

"CIO" Role

Administrative Capabilities

can manage all Standard Users	Disabled
can manage Power Users	Disabled
can manage all groups	Disabled
can manage billing	Enabled
can change account configuration	Enabled
can manage custom metadata settings	Enabled

User Groups

One concern many IT teams have is the ability to scale the management of permissions across thousands of users and millions of files. Although user accounts can be automatically added to Egnyte (typically through integration with Active Directory), manual assignment of folder permissions is still difficult. Therefore, Egnyte uses the concept of “User Groups” to scale up permissions for hundreds or thousands of users. User Groups can be created, and employees added to them as needed. Then as folders are created and populated, User Groups can be added rather than adding individual users. In most businesses, User Groups are created to correspond to work teams, departments, and entire organizations. An individual may be a member of several groups, and groups can be members of other groups. In this way, permissions can scale by simply adding the appropriate groups. Likewise, large numbers of permissions can be withdrawn by simply deleting a group permission. In the configuration screen below, you can see typical examples of User Groups.

Group Name ^	Owners	Users
Americas-all	Jeff Jones	9
Building Maintenance	Dave Buster	1
Construction Managers-EU	Jeff Jones	2
Construction Managers-US	Jeff Jones	2
Contractors	Dave Buster	0
EU-all	Jeff Jones	5
Field Engineering	Jeff Jones	3
Finance	Jeff Jones	3
HR Consultants	Jeff Jones	2
HR Managers	Jeff Jones	1
IT	Jeff Jones	3

Permissions Browser

Egnyte’s Permissions Browser gives visibility to the permissions structure for each folder across connected repositories, allowing administrators to audit permissions and enforce access controls. The Permissions Browser displays permissions for individuals or groups, including how each user derives their permission to view specific content (e.g., as a member of an entitled group or through direct permission from the owner), as well as whether they have view, edit, full, or owner access.

EGNYTE

Secure & Govern

Dashboard

Issues

Sensitive Content

Permissions

Compliance

By Folders

By Users & Groups

Filters

SOURCES

☐ Governor File Server

DATA OWNERS

☒ Show all folders

☐ Only folders with Data Owner assigned

☐ Only folders without Data Owner assigned

REVIEWS

☒ Show all folders

☐ Permission Review pending for anyone

☐ Permission Review pending for you

☐ Permission Review requested by you

Governor File Server

Shared

Audit Reports

Building Management

Documents

Finance

Bank info

Budgets

Forms

Reports

Human Resources

Marketing

Mortgage Documents

Templates

Bank info

Add permissions

Export permissions

1 Group • 14 Users • 1 Deactivated User • 0 issues

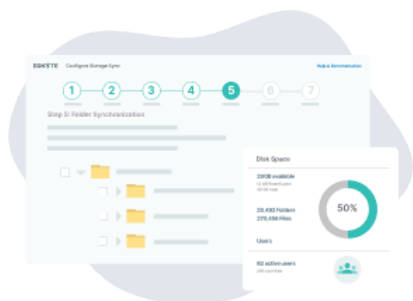
☒ Show Deactivated Users

USER/GROUP	PERMISSIONS	GRANTED	LAST CHANGED BY	LAST CHANGE...
All Administrators	Owner	Directly for gr...	-	-
Brian Harmony	Owner	via All Admini...	-	-
Dave Buster	Owner	via All Admini...	-	-
Governance Access	Owner	via All Admini...	-	-
James Schmidt	Owner	via All Admini...	-	-
Jeff Jones	Owner	via All Admini...	-	-
Kevin Washington	Owner	via All Admini...	-	-
Matt Bromiley	Owner	via All Admini...	-	-
Mike Pittenger	Owner	via All Admini...	-	-
MSP Partner	Owner	via All Admini...	-	-

If permissions appear incorrect, the administrator can request a review by the data owner.

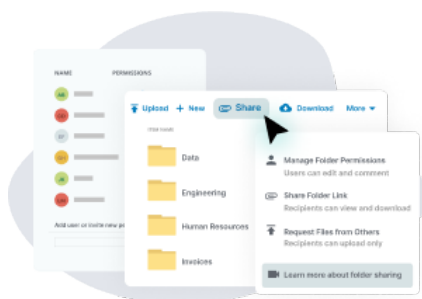
User Access Summary

Egnyte allows users in distributed workforce settings to access content through a desktop application, web browser, native applications, and via a mobile app. It also provides users and administrators a variety of options for storing and accessing data:



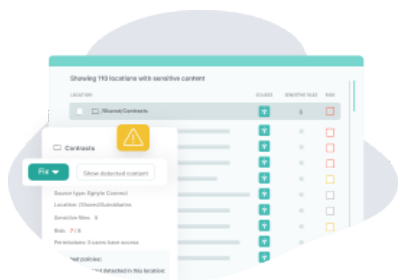
01 | Local caching of large files

When permissions allow, files can be stored on-premises to eliminate internet bandwidth and latency concerns.



02 | Desktop and mobile device

When local access is required (no, slow, or untrusted internet, travel, etc.) Egnyte enables users to synchronize data from Egnyte with desktop folders.



03 | Differential synchronization

Egnyte provides differential synchronization to update only the parts of a file that have changes to improve performance.



04 | File compression

Many file types can be compressed prior to upload or download when bandwidth is an issue.

Smart Cache

Smart Cache is Egnyte's next generation hybrid technology. It works with the Egnyte Desktop App so that files are available from a single drive letter on a user's device. When users are at home, Egnyte Desktop App automatically connects to the cloud. When users are present in an office, Egnyte Desktop App connects to the device if there is one deployed in their Local Area Network. Smart Cache supports Global File Locking, so that when a file is opened for editing, the file is locked and is not editable by any other user. With Smart Cache, users who travel between different offices can continue to use the Desktop App to access files stored in Smart Cache devices at each location (if they are authorized to access the Smart Cache device). The Desktop App discovers the nearest device based on certain network tests (bandwidth and latency checks) and connects to the appropriate device or the cloud. This way, users can easily move between offices and still access their files in the most optimal manner.

File Protocol Support

To support general user collaboration, users connect through the Desktop App to Smart Cache over secure REST APIs. Egnyte also supports direct Server Message Block (SMB) protocol for organizations using back-end capabilities like scanners, machinery, and custom programs as well as FTP, SFTP, WebDAV and other common protocols. This provides the flexibility to connect to on-premises file systems in addition to cloud repositories. (Note: Because some versions of SMB are vulnerable to attack, it is not recommended to use SMB outside of a local LAN segment for security reasons.)

User Authentication

Egnyte enables strict user authentication and permission enforcement at every access point, ensuring only users with appropriate credentials can access company data. Organizations can use existing corporate identity management systems, such as Active Directory, LDAP and the Google Identity Platform (using SAML IdP), to authenticate users and ensure consistent policy enforcement. Egnyte supports Single Sign On (SSO) through SAML 2.0, and partner integrations with leading identity management solutions such as Okta. Egnyte also offers its own access system which includes multifactor authentication.

Egnyte also implements multiple measures to prevent unauthorized access after a user has logged in, issuing session timeouts and alerting administrators when Egnyte is accessed from unexpected geo-locations that may indicate a potential threat.

Access Governance

Egnyte allows folder access permissions to be easily set for an individual or groups of users. Groups can include both employees and external users, as required by the business. For example, groups can be created for the entire finance department, procurement and specific suppliers, marketing and external contractors, or executive team only. Permissions can be set for each folder and sub-folder or across a repository to prevent over-sharing and unnecessary access to sensitive information.

Permissions

Typically Folder permissions are set by the data owner and always uniformly enforced, irrespective of location and access method (web browser, desktop app, secure FTP, mobile app). Users and groups can be granted different access levels:

- Viewer Only
- Viewer
- Editor
- Full
- Owner

And administrators can set granular folder and sub-folder permissions for each individual user (e.g., none, read-only, read/write, read/write/delete).

Permissions for each folder and sub-folder are flexible. For example, folders can be set to preview-only, which prevent users from downloading, printing, and copying files. Customers can also leverage recipient-specific distribution (described below) and detailed tracking for complete visibility into the activity surrounding their users' activity and files. These advanced access controls are critical to the implementation of data structure and hierarchy.

Documents are typically shared among a group of users. To ensure a record of changes and to prevent unauthorized changes, Egnyte provides *automatic file versioning* – allowing users to revert to a previous version if a file is accidentally or erroneously overwritten – and *automatic global file locking* to avoid version conflicts or prevent simultaneous editing by multiple users.

Folder Permissions to "Client share" folder

Permissions inheritance
Parent folder permissions are inherited 

NAME ^	PERMISSIONS ^
 All Administrators	Owner 
 Betty Johnson NON-EMPLOYEE	Viewer  x
 Eric Bishop NON-EMPLOYEE	Full  x

Add user or invite new people

Editor 

Done

User Types and Roles

As stated previously, Egnyte supports User Types and Roles. However, it's important to point out that these functions are supported separately on the collaboration side and the Secure & Govern side of the platform.

First, the Collaboration (file sharing) side of the platform supports 3 standard roles: Power Users, Standard Users, and Admins. The default settings are sufficient for most organizations, but within these roles, you can configure the specific capabilities allowed. Typically, Power Users are full time employees who need full access to all the capabilities of the collaboration environment, while Standard Users are more often occasional users, contractors, or partners who need limited access to be able to collaborate on specific projects. Admins manage the system. The specific capabilities of the Power User and Standard User types can be set in the Configuration Settings screen as shown here:

The screenshot shows the 'Configuration Settings' interface with two tabs: 'User Types' and 'Roles'. The 'User Types' tab is active, displaying settings for 'Power Users' and 'Standard Users'.

Power Users	
can use Desktop Sync	Enabled ☐
can use the Desktop App	Enabled ☐
can view Users & Groups in Settings	Enabled ☐
can see all non-default groups	Enabled ☐
can invite Standard Users	Enabled ☐
receive folder notification emails	never ☐
can receive the Egnyte newsletter	Enabled ☐
can view Activity in folders	Enabled ☐

Standard Users	
receive folder notification emails	never ☐
can receive the Egnyte newsletter	Enabled ☐
can view Activity in folders	Enabled ☐

In addition, the collaboration platform also includes a default role for an admin which includes a broad range of capabilities to configure and manage the system. However, many larger organizations choose to delegate certain portions of that responsibility others. This is done by creating additional roles. For example, a role can be created within the finance team to be able to manage account billing, or within the IT team to manage storage allocations. Some organizations prefer to have the security team manage devices. Example roles and capabilities are shown in the configuration screen below.

Roles

Role Name ^

CIO
contractor
Default
DevOps
HR Manager
Security Admin
Team Lead

"Security Admin" Role

Administrative Capabilities

can manage all Standard Users	Enabled	
can manage Power Users	Enabled	
can manage all groups	Enabled	
can manage billing	Disabled	
can change account configuration	Enabled	
can manage custom metadata settings	Enabled	
can manage personal devices	Enabled	
can manage storage devices	Enabled	
can manage trash	Disabled	
can create top-level folders	Disabled	
can run reports	Enabled	
can manage Document Rooms	Disabled	

The Secure & Govern side of the platform has a similar model to manage Users and Roles for governance of data. In this case, each user has one or more roles which determine the level of authority they have. When a user is added, one or more roles can be selected as shown below. Here, we see the 4 built-in roles that have been provided. They are Admin, Basic User, Basic Viewer, and Data Owner. In this case, 2 roles have also been created and added as possible roles. They are "Contractors" and IT Jr Analyst".

Roles

One user can have multiple roles. Effective user permissions are the sum of all their role permissions.

Add role

NAME	USERS WITH ROLE	
Admin BUILT IN	9	>
Basic User BUILT IN	1	>
Basic Viewer BUILT IN	0	>
Data Owner BUILT IN	4	>
Contractors	0	>
IT JR Analyst	1	>

The responsibilities of each of these roles can be configured as needed. For example, here is a screen configuring the Basic User Role.

Role details
Delete role
Save role

Role name: Basic Viewer **BUILT IN**
Description: Built in Basic viewer role

Role Settings
Users with this Role

ON
Issues

Users see: Issues they are assigned
Users can: ☐ Manage issues (fix, dismiss, reopen and delegate)
Settings: ☐ View Analysis Rules settings
☐ Manage Analysis Rules settings

OFF Sensitive Content
OFF Permissions
OFF Content Lifecycle
OFF Legal Holds
OFF Compliance
OFF Content Safeguard
Others

In addition to roles and users, Egnyte supports the concept of groups, which provides tools to manage thousands of user permissions. Groups can be created which can be assigned access permissions, and then users added to the group in bulk. The concept of groups provides a powerful tool to manage permissions across large numbers of users. To prevent misuse, Egnyte provides alerts to inform administrators of empty groups (groups with no members) and unused groups (which have not been given access).

Users
Groups
Import Groups
Export All Groups
+ Add Group

Groups
Search groups

Group Name	Owners	Users
Group name Add Group Cancel		
Americas-all	Jeff Jones	9
Building Maintenance	Dave Buster	1
Construction Managers-EU	Jeff Jones	2
Construction Managers-US	Jeff Jones	2
Contractors	Dave Buster	0
EU-all	Jeff Jones	5
Field Engineering	Jeff Jones	3
Finance	Jeff Jones	3
HR Consultants	Jeff Jones	3



Login Credentials

Egnyte administrators set password length and complexity requirements, as well as mandatory password rotations, and enable account lockouts after failed logins. Egnyte monitors and logs all access attempts and generates alerts for suspicious activity. Login credentials are protected via one-way hashing.

Multi-Factor Authentication

Egnyte's Two-Step Login Verification enables administrators to require users to verify their identity through a phone call, SMS message, or authenticator app. Egnyte also supports two-factor authentication through FIDO2/WebAuthn.

Device Controls

Egnyte provides a centralized dashboard to control and monitor all employee devices. Within the device control panel, administrators can enforce additional security settings to manage Egnyte content on desktops, laptops, mobile phones, and tablets. This includes the ability to allow or prevent data synchronization under specific conditions, prevent specific file types from synching, and requiring passcode locks on mobile devices.

Personal Devices

Storage Devices

Export All Personal Devices

Personal Devices

Any Username

Any Status

Any App

Username	Application	Software Version	Device Platform	Device Name	Last access/sync	Device Status
dbuster	Desktop App	3.14.1-202444	macOS 11.6	admin's MacBook Pro	Dec 7, 2021 1:38 PM	
tjohnson	Desktop App	3.14.1-202444	macOS 11.5.2	Tim's MacBook Pro	Dec 7, 2021 1:32 PM	
tjohnson	WebEdit	2.4.5.24	Mac OS X 11.5.2	Tims-MacBook-Pro-2.local	Dec 7, 2021 9:47 AM	
bsanders	WebEdit	2.4.5.24	Mac OS X 11.5.2	Tims-MacBook-Pro-2.local	Dec 7, 2021 9:47 AM	
bcarambio	WebEdit	2.4.2.90	Mac OS X 10.16	brittanys-mbp.lan	Dec 7, 2021 7:40 AM	
tjohnson	Desktop App	3.12.0.107	Win 10	DESKTOP-J39433C	Oct 13, 2021 7:39 PM	

Enterprise Mobility Management and Mobile Device Management

Egnyte can integrate with enterprise mobile management (EMM) and mobile device management (MDM) containers to allow customers to install and manage Egnyte's applications with a broader set of mobile policies to deliver consistent controls.

Egnyte can also use mass deployment capabilities to securely download the Desktop App client, for those customers who want local, high-speed access, or offline access to files.

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.

For customers who do not have an EMM or MDM solution, Egnyte provides a host of native device control capabilities outlined below. As with the mobile application, the Egnyte desktop application also provides a remote wipe capability.

Mobile Passcode Lock

Egnyte allows organizations to minimize security risks if employees' mobile devices are lost or stolen. Administrators can set mandatory passcode locks, requiring users to enter a PIN after login or an extended idle time. As an additional safety precaution, locally stored mobile files can be automatically wiped after a set number of incorrect passcode attempts.

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 to sensitive data.



Remote Wipe

Administrators or device owners can quickly initiate remote wipes of Egnyte files on mobile apps and Desktop Sync clients from a web interface that provides a centralized view of all end- user devices.

Device Entitlement

Administrators can manage which mobile devices are allowed to use the Egnyte mobile app. Likewise, similar capability is provided with the desktop application. This prevents the application from being installed on unmanaged endpoints.

Mobile File 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, file encryption is available for offline files stored on a device. This provides complete endpoint encryption, so even in the event of data leaks or device theft, customers' files are always encrypted.

Discovery & Classification

Egnyte continuously scans all governed repositories to discover and classify sensitive data. This includes unstructured data from email and messaging applications, commercial and custom applications, corporate and personal devices, SaaS applications, and public and private clouds.

Data Classification

Since not every piece of data is subject to the same security and regulatory policies, the millions of files and terabytes of information that are identified must be categorized or *classified* for sensitivity. Manual classification by end-users is inconsistent and does not scale to millions of documents. Instead, Egnyte automatically classifies data to flag sensitive information as each repository is scanned. This includes unstructured data from office documents and files, local and remote file servers, corporate email, messaging applications, and other business applications.

The complex process of data classification requires artificial intelligence and machine learning, provided by Egnyte's Content Intelligence Engine. For example, in a document, a string of digits may be a sensitive Social Security number, or a part number. The Egnyte system scans the surrounding information for context before deciding whether data is sensitive. Occasionally, an administrator will receive a message asking if the data detected is indeed sensitive, and the system then uses these human confirmations to learn.

A typical Egnyte deployment scans and classifies 7 million files, and 3 terabytes of data in less than a week using content-based and contextual classification rules. Egnyte then continuously scans each repository for data that is added or changed and classifies it in real-time.

Content-based Classification

Egnyte automatically identifies and classifies sensitive information like credit card numbers, addresses, dates of birth, social security numbers, and health-related information (such as patient ID numbers and diagnostic codes). Classification parameters are pre-configured for

The screenshot shows the 'Identify sensitive content' configuration page. It includes a 'Find folders with sensitive files' section with a 'Sensitive Content' tab. Below this is a 'Within which jurisdictions must you comply?' section with a dropdown menu showing 'United States, United Kingdom, European Union, Canada'. The 'What should be treated as sensitive content?' section contains a 'BUILT-IN POLICIES' table with columns for policy name, description, and selection status. The table lists several policies: 'Regulatory Compliance Policies' (23/29 SELECTED), 'Finance' (4/4 SELECTED), and 'General Privacy' (14/22 SELECTED). Under 'General Privacy', there are four checked policies: 'DPA' (Data Protection Act), 'PIPEDA' (Personal Information Protection and Electronic Documents Act), 'GDPR' (General Data Protection Regulation), and 'UKGDPR' (UK General Data Privacy Regulations). Each policy has a description and an 'Application mode' dropdown menu.

BUILT-IN POLICIES		
Search for Policy		
Regulatory Compliance Policies	Personal information used by organisations, businesses or the government in the UK	23/29 SELECTED
Finance	Personal information collected by Canadian private sector organizations in the course of commercial business	4/4 SELECTED
General Privacy	Personal information related to a European Union resident	14/22 SELECTED
Application mode: Broad		
DPA	Data Protection Act	Personal information used by organisations, businesses or the government in the UK
PIPEDA	Personal Information Protection and Electronic Documents Act	Personal information collected by Canadian private sector organizations in the course of commercial business
GDPR	General Data Protection Regulation	Personal information related to a European Union resident
Application mode: Broad		
UKGDPR	UK General Data Privacy Regulations	Personal data of UK residents collected by businesses and organizations
Application mode: Narrow		

major regulatory standards and geographies, as outlined in the Regulatory Compliance section of this document.

Administrators can also add custom classifications for parameters unique to their organizations, including keywords, patterns, file properties, document templates, file types, and metadata. In the case of graphics files (.png, etc.), the Egnyte system automatically uses Optical Character Recognition (OCR) to derive text from the image that it can then use to classify sensitive data. This helps Egnyte classify photos of sensitive records such as driver's licenses and social security cards.

For many text documents, Egnyte also detects document types based on the format and structure of the document itself. Documents such as resumes, invoices, and contracts can be detected (and subsequently protected) this way. In addition, if your organization has unique (custom) document types for sensitive information (departmental reports, designs, specification, etc.), you can submit samples of those documents to the Egnyte Machine Learning Engine to learn. Within a few minutes, the Egnyte AI can begin detecting your unique document types.

Below is a table listing some of the various file types that Egnyte display using the preview feature (by simply clicking on a file in the browser interface). A full listing is here: <https://helpdesk.egnyte.com/hc/en-us/articles/201637604-Which-Types-of-Files-Work-with-the-File-Previewer->

File type	Extension
Microsoft Office files since Office 2007	.docx .docm .dotx .dotm
	.xlsx .xlsm .xltx .xltm .xlsb
	.pptx .pptm .potx .potm .ppam .ppsm .ppsx .sldx .sldm
Legacy Microsoft Office formats	.doc .docb .doct .dot .xls .xlt .xlm .ppt .pot .pps
Postscript and PDF formats	.ps .pdf
Other spreadsheet formats	.csv .tsv
Email storage formats	.msg .mbox
OpenDocument formats	.odt .ods .odp
Rich text and simple text formats	.rtf .txt
Compressed archives (non-encrypted)	.zip .7z .bz2 .cpio .jar .rar .tar .gz .xz .tgz
Image files	.jpg .jpeg .png .tif .tiff .bmp
Google Suite files	.gsheet .gdoc .gslides
Other file types	.epub .html .xml .xhtml .ooxml .odf

Contextual Classification



Certain data, including video, audio, images, and drawings, cannot be “read” for sensitive information. In those cases, Egnyte can classify data based on configurable settings such as data store, author, file type, or file folder.

Lifecycle Management

In most organizations, content expands exponentially. Not only is new content created, but old content gets copied and replicated across multiple repositories. As old content accumulates, it creates potential problems for the organization, including:

- Legal liabilities when retention policies are not documented and followed
- Expanded target surface for attackers to mine for sensitive information
- Difficulty for employees to find the information they need to do their job
- Additional costs for active storage of unneeded data

Egnyte helps address these problems with tools for Lifecycle Management.

Lifecycle Policy Creation Engine

Administrators can write their own policies to automatically retain, archive, or even delete old data based on when it was created, folder locations, or classification. These policies can be as simple or as complex as necessary to fit business needs. Overlapping policies are managed according to the following rules:

Retention

Files covered by multiple retention policies are retained according to the policy with the most extended retention period. This provides the best protection for critical information.

Edit Content Retention Policy [Cancel] [Save policy]

This content retention policy applies to new and existing file versions. Files will be prevented from being purged according to the policy settings below.

Created by: Dave Buster
Created date: 10/21/2021
Last modified: 10/21/2021

Policy name: Accounting Archive
Description: Historical accounting records

Apply policy to: ☒ Files ☐ Projects
☒ Retain only latest version of files

Retention period: 10 years after creation

When retention ends: Move file versions to archive domain...
Governor Archive Server Match source paths at destination (for shared folders)

☒ Leave stub files behind to indicate that the files were archived

Retain files that match these criteria:

Policy affects files that: match selected classification policies

Select classification policies
Matches any selected classification policies [Configure]

Archiving

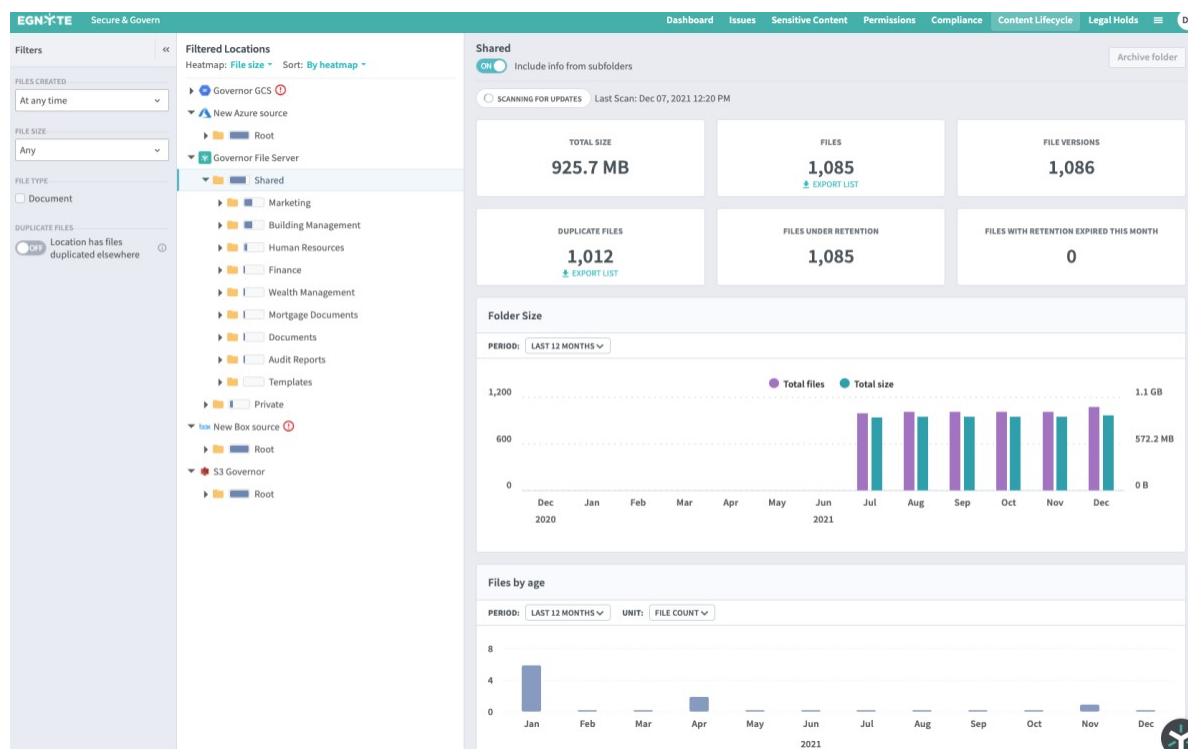
Files covered by multiple archiving policies are archived according to the policy with the shortest archiving period. This saves money by archiving files sooner.

Deletion

Files covered by multiple deletion policies are deleted according to the policy with the shortest deletion period. This saves money by deleting files sooner.

ROTS (Redundant, Obsolete, Trivial, Stale) Data Management

The risk of sensitive data being exposed increases each time a new version of a document is created or shared. At the same time, many organizations are subject to regulatory standards with strict data retention policies. Egnyte's policy templates allow organizations to classify files across repositories and identify redundant, obsolete, trivial, and stale data (ROTS) that can be securely deleted to minimize risk.



Unified Analytics and Reporting

As Egnyte continuously scans, classifies, and monitors content, it surfaces a Lifecycle Management dashboard for admins. An administrator can select any folder structure and review detailed statistics including:

- Number of files
- Number of versions
- Number of duplicate files
- Files under retention
- File ages and activity
- File types
- Folder sizes

It's important to note that Egnyte provides scans of this information for all repositories covered – not just Egnyte. Therefore, the information above is also available for Microsoft, Google, Box, Dropbox, etc. However, based on the API supplied by the provider, not all Retention, Archival, and deletion automated policies can be supported on third party repositories. Check with your Egnyte representative for the latest capabilities for lifecycle management across third party repositories.

Data Controls

Once sensitive information is identified, Egnyte allows administrators to manage access to content while allowing employees to access relevant data freely and collaborate with each other, customers, and business partners.

Egnyte's Access Control features continuously monitor content sources, in the cloud and on-premises, to automatically:

- Identify issues with permissions and sharing to ensure only authorized individuals have access to sensitive information.
- Eliminate non-secure links and comprehensively review sharing with outside parties.
- Audit and streamline permissions across content repositories for greater control and security.
- Spot unusual user activity to prevent insider data theft and other malicious actions.

Content Safeguards

Egnyte protects governed repositories from data leaks by restricting public links to sensitive files. Content Safeguards use classification policies described previously to determine if a file contains sensitive content. Then, Egnyte applies sharing restrictions when it detects sensitive content in a file. Restrictions can include requiring password file access or limiting external file sharing, or simply warning the user that external sharing is not recommended. In the user warning example, the user is provided an opportunity to override the file sharing restriction with an explanation. Administrators can create Content Safeguard policies to apply a minimum-security level matching, risk score, and/or location.

Edit Content Safeguard Policy Cancel Save policy

Link sharing restrictions will affect files matching 1 sensitive content policy.

Policy name:

Description:

Which files should be restricted?

Policy restricts files that meet: ANY of the following criteria

- Content matching selected classification policies**
1 Content Classification policy selected. Configure
- Any risk score**
No minimum risk score selected. Configure
- At any location**
No specific location selected. Configure

What restrictions should be applied?

Sharing restrictions
Users will be able to share files only using links with increased level of security
Lowest security level for links to files matching this policy:
Private link for specific content source users

Note that Egnyte can scan many types of repositories for sensitive data including Microsoft SharePoint, OneDrive, Google, Box, Dropbox, and others. Sensitive data is discovered, tracked, and access is monitored. However, depending on the APIs provided by the respective providers, Egnyte content safeguards cannot always be applied uniformly across third party repositories. Therefore, it is recommended that employees be encouraged to put the most sensitive information into the Egnyte repository to get the best protection.



Encryption in Transit

Egnyte uses HTTPS and secure FTP protocols to create a protected, encrypted channel and encrypts data in transit using 256-bit AES, including sensitive files shared externally.

Encryption at Rest

All the data stored on Egnyte's servers is automatically encrypted using AES 256-bit encryption and hashed encryption keys that are unique to each account and stored in a secure key vault accessible only by the Egnyte Object store software.

File Encryption and Key Management

Enterprise Key Management (EKM) allows organizations to manage their keys using a third-party cloud service or their own on-premises infrastructure. Egnyte supports Microsoft Azure Key Vault and Amazon AWS CloudHSM.

Threat Management

Issue Detection

Egnyte uses machine learning to detect issues that might result in data loss or non-compliance with privacy regulations. From a centrally located Issues tab, users can identify problems including:

- Empty and unused groups: Detects groups that contain no users and groups with users that lack any folder permissions.
- External sharing: Detects files and folders that have been made accessible to people outside your organization.
- Individual permissions: Detects folders that are directly permitted to individual users rather than to groups.
- Open access: Detects folders that are accessible to Open groups (with very large numbers of users)
- Probable ransomware: Detects user accounts suspected of being compromised by ransomware, either through artifacts or behavior.
- Public link: Detects files and folders accessible by a public link.
- Suspicious login: Detects anomalous login activity that may indicate a compromised account. This includes impossible travel and location.
- Unusual access: Flags users downloading or deleting unusually large amounts of data to help prevent data loss.

← Unusual Access

Detects users who access or delete an unusually large number of files, which may indicate malicious activity.

Total issues detected: 0
Open issues: 0
Ignored issues: 0
Last issue update: ~
Severity of this issue type: 1 to 3

DETECTION THRESHOLD

Select which criteria should be taken into account for issue detection:

- ☒ File access / downloads
Number of files opened or downloaded by user within one day
- ☒ File deletes
Number of files deleted by user within one day
- ☐ Access of sensitive files
Number of files with sensitive content accessed by user within one day
- ☐ Locations
Number of unusual locations accessed by user within one day
- ☐ Time of day
Number of actions taken by user at unusual time of day within one day

Controls how far from their normal usage pattern a user needs to deviate before an anomaly is detected.

Threshold: Low ⓘ

Minimum number of files accessed or deleted by a user in order to trigger an issue: 10

At this threshold, you can expect to detect about 1 anomaly per month.

Issue Alerting

Administrators or other designated alert recipients receive notifications when issues arise, such as when publicly available links to sensitive information are shared, content that's marked sensitive is shared outside of predetermined boundaries, or a compromised account is detected. Customizable alerts can be created in minutes to help avoid “alert fatigue”, common among traditional security solutions. An administrator can select the severity of the alert and then choose to receive emails above the selected threshold. By using (free) third party email/SMS gateways, these emails can also be forwarded as text messages to mobile devices.

Issue Prioritization and Resolution

The Issues tab provides quick remediation and allows administrators to filter issues by severity and set alert thresholds for unusual or anomalous behavior. To simplify issue prioritization, all issues are scored by severity (1–9) based on the type and amount of sensitive content present. This approach also transforms a list of potential issues into actionable tasks, which permit administrators to:

- Disable a compromised user account
- Force password resets or add user exceptions
- Expire public links
- Delete empty or unused groups
- Move, delete, or “whitelist” sensitive content
- Modify permissions

The screenshot shows the 'Issue Details' panel for a specific issue. At the top, it says 'Public Link (#23)' with 'Fix' and 'Ignore' buttons. Below this, the following details are listed: Issue Number: 23; Issue Status: OPEN; Source type: Egnyte; Severity: 7 / 9 (with a red 'S' icon); Sensitive Content: ITAR, CUI (with an eye icon); Location: /Shared/Building Management/Active Projects/Uptown Project/Bid Documents (with a 'Show permissions' link). At the bottom, a summary states 'Issue: 1 public link detected' and 'Folder is accessible via 1 public link', with a 'Show Details' button.

Typically, the system recommends a fix to the issue which is available with one click.

Risk Score

A risk score is calculated when an issue or sensitive content location is detected based on analysis rules and classification policies. The risk score is calculated by analyzing the age and severity of open issues in the repositories, where sensitive content is located, and who has access to it.

An overall risk summary is also displayed in a unified admin dashboard, to allow tracking of risk over time. Organizations can quickly reduce risk scores by remediating high severity open issues, limiting the number of unpermitted high risk sensitive content locations, and limiting the number of users who have access to high-risk content.



Ransomware Detection & Remediation

Egnyte provides ransomware detection capabilities and facilitates recovery from potential attacks. It also reduces the risk of attacks by locking down file access with least-privilege, granular permissions, and applies signature-based protection to block known malware. In the event of an unknown variant, Egnyte's machine learning-based behavioral analytics can recognize file activity that could be indicative of ransomware—such as renaming, deletions, and changes in file entropy—and disable compromised accounts to block attack progression. Egnyte speeds recovery through an audit trail of compromised users, files, and data subjects/sensitive data and the ability to roll back specific files to a pre-attack state.

File Recovery

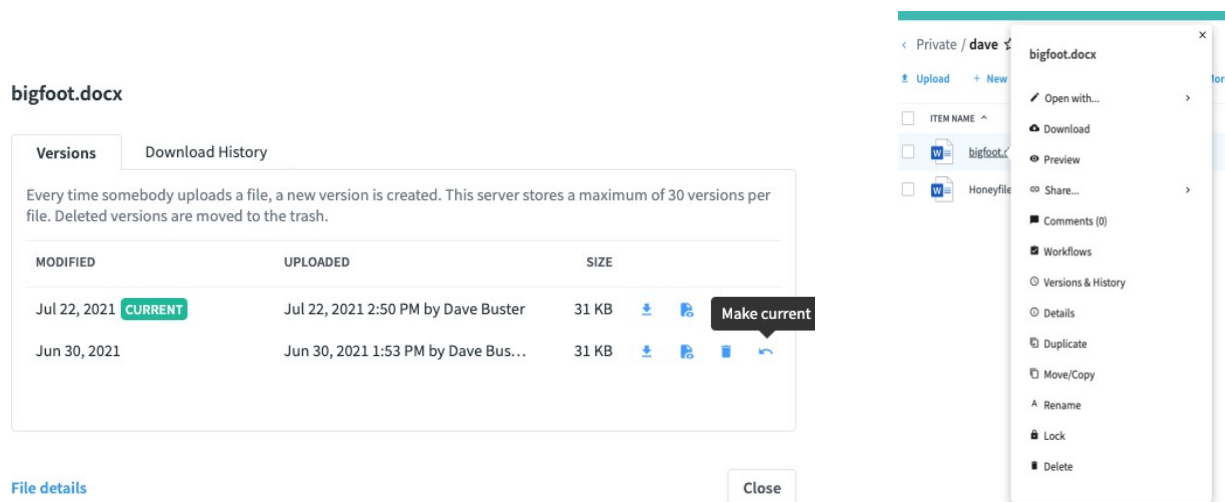
Egnyte offers three different ways to recover files encrypted by ransomware. These are:

- Individual recovery
- Bulk Recovery with Egnyte Professional Services
- Snapshot recovery

Individual File Recovery

For small ransomware events affecting few files, users can recover files directly without IT support, the same way they would recover files that were inadvertently over-written. The user simply selects the file and chooses “Versions & History” from the pop-up menu.

Then, the user simply chooses a previous version of the file and selects “Make current”. Because Egnyte keeps previous file versions online, the file is instantly reverted to a good version with virtually no delay.



If a ransomware attack is confined to a single user, then it's a simple matter to revert affected files back to a previous version. The date and time stamps make it easy to determine which files might have been affected.

Bulk Recovery with Egnyte Professional Services

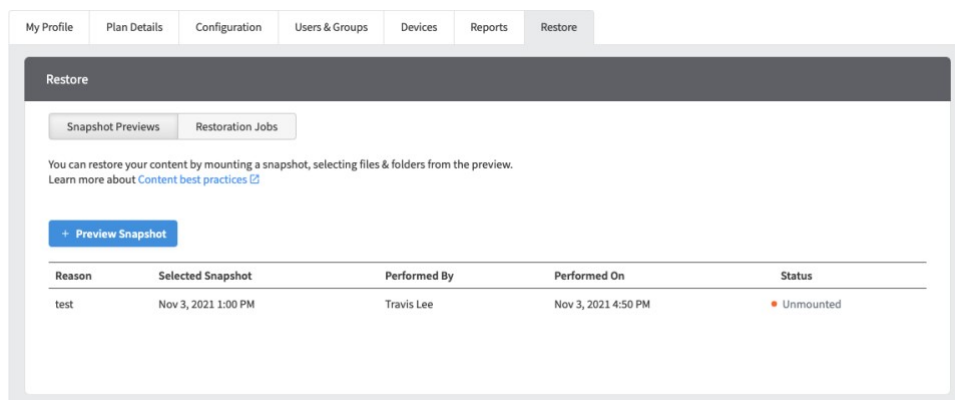
For larger scale attacks that affect large numbers of files and folders, individual file recovery may not be practical. In that case, Egnyte also offers bulk file recovery through the Egnyte Professional Services organization.

Snapshot Recovery

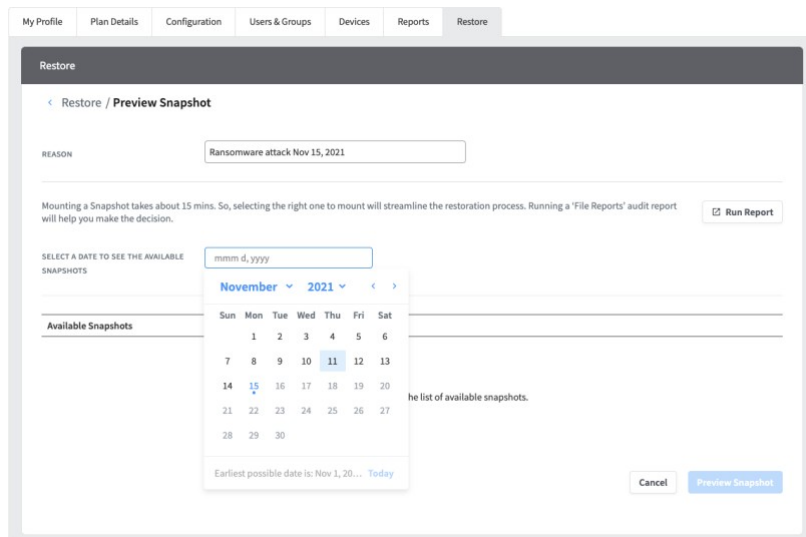
For customers on select platforms, a snapshot bulk recovery tool can be used to recover entire folder structures. Administrators can view a report of snapshots of their folder structure. By scrolling back through time, they can detect when the ransomware attack started and then choose a recovery point just prior to the attack. Full restoration usually takes minutes to a few hours (depending on the scope of the attack). However, in all cases, restoration is much faster than manually copying drives. These steps are outlined in more detail below.

Selecting a Snapshot

An administrator opens the “Restore” tab on the “Settings” page to begin the process.

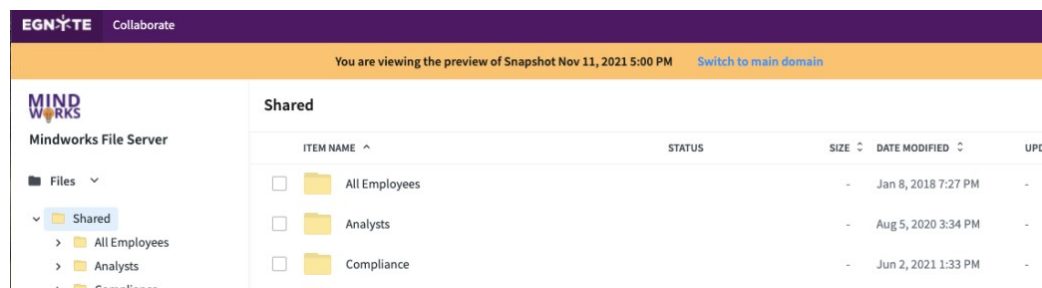


Next, the administrator chooses a date and time and selects a snapshot estimated to be just prior to the ransomware attack. This does not have to be precise, additional snapshots can be added later.



Once a snapshot is selected, it is mounted to be reviewed on a preview screen. Mounting a snapshot can take a few minutes, but status is provided on the page.

After the Snapshot is mounted, the administrator can go into the snapshot preview and verify that the files are intact.



Any individual files or entire folder structures can be selected at this point for restoral by checking the box. Then the restoration process begins.

Restore from Snapshot

JOB NAME:

We discovered some storage and personal devices enabled on your domain. Disable these before restoring your data.

[Go To Settings](#)

You will still see some encrypted files within your file server after the restoration.
[Learn how to delete them](#)

Cancel

Restore

Once the folders have been restored, the user will see the newly restored folders beside the ransomware encrypted folders. Using this process, administrators can restore large folder structures to recover quickly and easily from large ransomware attacks.

Compromised Accounts

Egnyte uses location-based rules to flag suspicious access that indicate a potential compromise. By default, the system restricts access from countries that appear on the US State Department's export control list, including China, Russia, and North Korea.

Administrators can easily add or remove individual countries from the restricted list to match their regulatory and business needs. Egnyte also detects near-simultaneous logins from distant locations. For cases where simultaneous access is expected, per-user exceptions and IP whitelisting allow for shared accounts or access from a VPN.

User Behavior Analytics

Egnyte uses behavioral analytics to baseline and continuously refine patterns of employee behavior and data usage. This improves confidence in the detection of anomalous behavior, such as users downloading or deleting unusually large amounts of data or downloading content that user typically does not access like customer lists or financial reports that might be brought to a competitor.

Issue Reporting

Egnyte's reporting function uncovers risks to data that can support quick mitigation.

Administrators receive reports on data, user, and device activity, and overall storage utilization that can help optimize the enterprise's security. Administrators can monitor and analyze overall application and data usage, highlighting any changes that could indicate a breach or potential issue that warrants investigation.

Audit Reporting

Egnyte provides an audit report of all key actions taken within the system, including:

- Logins
- Viewing sensitive content matches
- Permitting and un-permitting sensitive content in folders
- Moving or deleting files with unpermitted sensitive content
- Ignoring, re-opening, or fixing issues

For each action, the system logs the date and time the action occurred, the user performing the action, the associated content repository, and details such as the file path or a link to the associated issue in Egnyte. All details are stored indefinitely in Egnyte, and administrators can run reports for any period, including from system inception.

Audit Reports

Download an audit report of content lifecycle policy or user actions.

Action type:

Date range:

-

[Download Audit Report](#)

Through integrations with third party SIEM products like Sumo Logic and Splunk, this information can also be integrated into enterprise-wide analytic tools to help correlate Egnyte events and actions with those across other systems in the enterprise.

Privacy & Compliance

Most organizations are obligated to comply with an ever-growing set of regulatory standards. These include privacy regulations like GDPR and CCPA, financial reporting requirements like GLBA and SOX, and regulations covering Protected Health Information like HIPAA and PIPEDA. Egnyte simplifies compliance with regulatory requirements through a variety of capabilities.

Supported Regulatory Standards

The Egnyte Platform includes classification patterns the ability to create data retention policies easily for dozens of global privacy laws, with workflows to support Subject Access Requests (SAR) and Breach Reporting. Some examples of privacy regulations supported include:

Data Privacy Regulations & Compliance Mandates	
• APA - Australian Privacy Act	• ITAR - International Traffic in Arms Regulations
• CCPA - California Consumer Privacy Act	• LFPD - Mexico Federal Law on the Protection of Personal Data
• DPA - Data Protection Act	• LGPD - Brazilian General Personal Data Protection Law
• FCRA - Fair Credit Reporting Act	• NOOL - Nevada Opt-Out Law
• GDPR - General Data Protection Regulation	• NZPA - New Zealand Privacy Act
• GLBA - Gramm-Leach- Bliley Financial Modernization Act	• PCI-DSS - Payment Card Industry Data Security Standard
• HIPAA - Health Insurance Portability and Accountability Act	• PIPEDA - Personal Information Protection and Electronic Documents Act
• IPDP - India Personal Data Protection Bill	• SOX - Sarbanes-Oxley Act

Data Retention Policy Management

Some regulatory standards dictate a retention period for specific data types. Egnyte provides a tool to easily create a data retention policy. Criteria for the policy can include location (by folder) or a match to any of the classification policies (including custom classification policies). Once the data is located, the retention policy can be set to lengths of time varying from 30 days to 30 years, or a custom period. Many organizations use 7 to 10 years, based on regulatory requirements. The retention timer can start at creation or after the last time the file was accessed (evergreen model). Finally, when the retention period expires, the policy can be instructed to do nothing, move files to trash, or archive files. The policy also applies to files in trash to avoid critical files being accidentally or maliciously deleted.

Subject Access Requests (SAR)

Some regulatory standards allow users to request personal data that businesses have collected about them by submitting a Subject Access Request (SAR). These can include:

- **Notification:** Provides the user with the amount and type of personal data collected.
- **Right to be forgotten:** Identifies and securely deletes all information collected on that user.

Egnyte's SAR search and reporting feature quickly identifies and collects all personal data for the requestor across Egnyte, governed repositories, and archives, verifies the data to the correct individual, (optionally) securely deletes the data, and documents all necessary steps.

Through an integration with Truyo, the SAR search and reporting can also be extended across structured data in databases, helping organizations comply with privacy requirements across both structured and unstructured data found in files. To reduce churn cost, the SAR function is not applied on archive domains.

Legal Hold

Egnyte supports Legal Holds to retain content related to a legal matter, securing all files created by selected users (referred to as a

The screenshot shows the 'New Subject Access Request' form. At the top right are 'Cancel' and 'Create request' buttons. The form is divided into sections: 'Subject Access Request Information' with dropdowns for 'Request type' (set to 'Right to be forgotten') and 'Target service time' (set to '45 days'); 'Subject Information' with a note to 'Fill in as much information as you have about the subject to serve the request more effectively.' Below this are input fields for 'First name' (Jeff), 'Middle name/initial' (Optional), 'Last name' (Smith), and 'Passport Number' (1234567). A link '+ Add another identifier' is at the bottom.

The screenshot shows the 'Add a Legal Hold' form. At the top right are 'Cancel' and 'Create Legal Hold' buttons. A descriptive text states: 'A Legal Hold retains content related to a legal matter, securing all files defined in the hold scope that were created, accessed or deleted within a specified date range. These files will be retained until the Legal Hold is closed or cancelled.' The form includes fields for 'Legal Hold Name' (Smith Liability Evidence), 'Description' (Received a Warrant for all info pertaining to Jones), 'Legal Matter' (Smith vs. Jones), and 'Date Range' (12/14/2021 to 02/18/2022). The 'Hold Scope' is set to 'Hold the files matching: ANY of the following criteria'. At the bottom, there are two expandable sections: 'Select custodians' with the text 'Hold files accessed, modified or deleted by selected users (custodians)' and a 'Configure' link; and 'Select folders' with the text 'Files within any selected folders' and a 'Configure' link.

custodians) within the specified date range. Administrators can also place holds on specific folders related to a given project or client. Importantly, Legal hold can be applied using a classification policy, providing much more flexibility and convenience. Typically, legal holds occur when litigation is pending or anticipated, when a company is subject to a government investigation or internal audits, or when another business matter forces a company to hold on to their records.

Breach Response

Breaches occur in even the most diligent organizations, often the result of compromised credentials. Breach reporting in Egnyte automatically prepares breach impact statements in accordance with supported regulations, including a summary report of impacted individuals and counts of sensitive information exposed.

New Breach Report Cancel Create report

Report name:

Description:

Breach date range: -

Target service time:

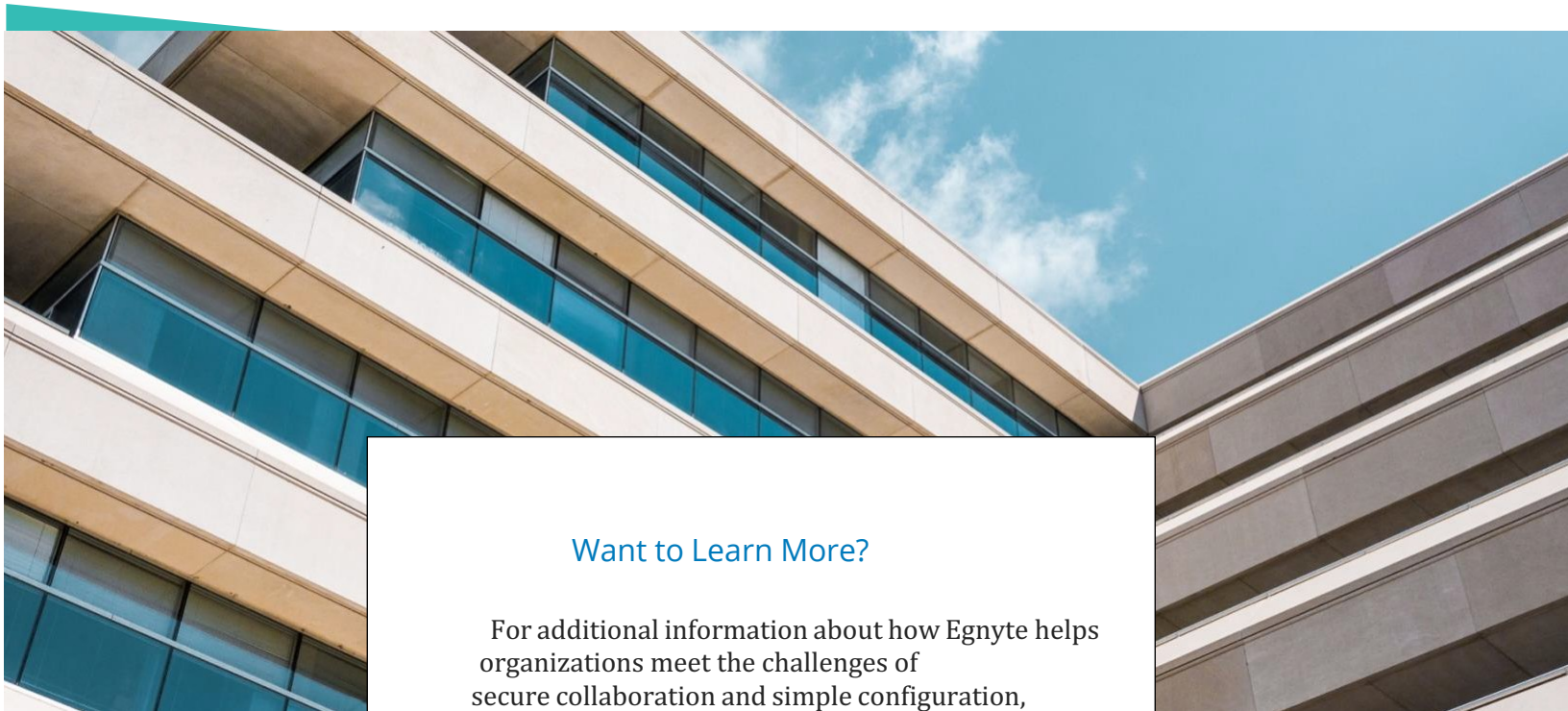
Breached users:

USER	SOURCES INCLUDED
Humberto Darden (hdarden@acme.com)	Sources 1/1 ×
Jessica Clark (jclark@acme.com)	Sources 1/1 ×
Type a name or email...	

Certifications and Audit Reports

The Egnyte platform is compliant with the following standards:

- SOC 2 SSAE 18 Type 2
- ISO 27001:2013
- FINRA
- DFARS
- HIPAA/HITECH
- FDA 21 CFR Part 11
- GDPR



Want to Learn More?

For additional information about how Egnyte helps organizations meet the challenges of secure collaboration and simple configuration, administration, and data management, visit www.egnyte.com to schedule a demonstration of the Egnyte platform.

Contact Us

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.

EGNYTE

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