EGNYTE

Egnyte Security Framework

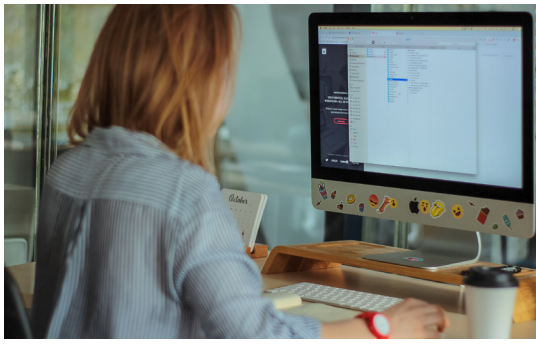
Collaboration, Privacy, Compliance.

Security in the age of Unstructured Data

Unstructured content is the largest source of data growth for modern businesses. The documents, PDFs, spreadsheets, images, and other files that enterprise users create, store, and share represent an ever-expanding portion of vital business data. But as data grows, so too does risk, turning these valuable data assets into liabilities.

In this era of unchecked growth, protecting sensitive content from data leaks caused by malicious or careless insiders, poor data hygiene, and bad actors has become harder. As more jurisdictions pass regulations that govern the privacy of personal data, such as the E.U.'s General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) there is a greater burden on companies to safeguard this information. With an average small-to-medium sized business (SMB) housing nearly seven million files, just understanding where that sensitive data is, and who has access to it, can be a herculean task.

The stakes are high. Data breaches and compliance violations can cost companies millions in fines and reputational damage. SMBs aren't immune: in 2018, a survey by EMA revealed that 60% of SMBs reported increases in the severity and sophistication of cyberattacks. Yet, 85% of those same organizations are hesitant to deploy protections for fear that it will impact user experience.



"SMBs aren't immune: in 2018, a survey by EMA revealed that 60% of SMBs reported increases in the severity and sophistication of cyberattacks. Yet, 85% of those same organizations are hesitant to deploy protections for fear that it will impact user experience."

Deconflicting Security and Productivity

Amid unprecedented unstructured data growth, emerging global privacy regulations, and increased threat of cyberattacks, a heightened focus on data security is no longer optional. Like any other business asset, securing high value data can't be an afterthought. Adding bulky security layers on top of content repositories adds complexity and cost in an environment where ease and productivity is paramount. Rather, businesses must deploy an end-to-end solution that protects data integrity without slowing users down.

Egnyte's secure content framework integrates data governance, compliance, and administrative control into all phases of the content lifecycle, from the day it is created to the day it is deleted, and every day in between. This allows users to securely create and share the files they need, while administrators maintain visibility and control through analysis and optimization of the data environment.

Create

Egnyte's hybrid infrastructure offers a secure environment for users to create and store files in the cloud. Data is housed in secured, SOC2-certified datacenters and can be augmented by on-premises infrastructure to maintain continuity of access in low-bandwidth environments. Users can access files via web, mobile, or desktop app, without the need for added VPN, while administrators can enforce security through strong password requirements, two-factor authentication, encryption key management, and mobile device controls. All the while, data is held in compliance-friendly datacenters that meet requirements under GDPR, HIPAA, FINRA and other regulations.

Share

Egnyte is built to make it easy for users to securely share content with internal and external groups. Rather than send insecure email attachments or rely on consumer-grade web apps to exchange files, users send links to the content they want to share directly in Egnyte. Client-facing organizations can use Egnyte to create secure customer portals or project workspaces that keep shared content under IT control.

Egnyte offers granular permissions down to the folder and file level and makes it easy to continuously monitor who in the organization has access to sensitive or regulated data. Administrators can apply global security standards for any content that travels outside the organization and can also quickly disable links to shut off access to sensitive files.

Analyze

Sustainable data governance is built on an understanding of how risky data is used (and by whom) and how it moves inside and outside the organization. In order to keep enterprise data safe, there are three fundamental questions every business needs to be able to answer:

1. What kinds of sensitive or regulated data do I have?
2. Where is it?
3. Who has access to it?

With millions of files in storage, automated data classification is the only way to do this at scale. Egnyte offers the fastest data classification engine in the industry, scanning the content of each document, spreadsheet, PDF and dozens more file types to locate more than 400 kinds of sensitive data in over 30 languages. Once sensitive content is surfaced, administrators can monitor where that data is housed and who has access to it, and quickly address issues from a central dashboard.

"Once sensitive content is surfaced, administrators can monitor where that data is housed and who has access to it, and quickly address issues from a central dashboard. "

Egnyte's analysis goes beyond the content of the files to learn how users behave on the file system, and alert administrators to unusual activity such as a rogue employee downloading or deleting large amounts of data. Egnyte also includes built-in ransomware detection, scanning for known ransomware signatures *and* zero-day events, to help prevent one of the most devastating kinds of attacks on your business.

Optimize

Corporate data is an asset, but also a liability; one that is vulnerable to hacks, insider threats, and regulatory penalties. To limit the risk posed by out-of-control data growth, companies must retire old or stale data, remove data that is no longer useful, and take steps to reduce their overall data footprint. Egnyte's content lifecycle management tools allow companies to retain content that is required under the law, while archiving or deleting content that isn't used. Using content-driven policies, companies can automate much of this process to protect themselves. After all, content that isn't there cannot be leaked or stolen.

The following Security Framework offers a detailed breakdown of the protections embedded in the Egnyte Secure Content Platform throughout the data lifecycle.

Table of Contents

Secure Collaboration

User Authentication

IT administrators know the most vulnerable point of any infrastructure is 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. Customers can use their existing corporate identity management systems, such as Active Directory (AD), LDAP or SAML 2.0, to authenticate users and ensure consistent policy enforcement.

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.

Two-step Login Verification

Egnyte's Two-Step Login Verification enables administrators to 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, SMS message, or authenticator app to create a double check for every authentication. By enforcing an additional 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, alerting on any suspicious activity, so system administrators can investigate.

In order to protect login credentials, user passwords are protected via one-way hashing. Only Egnyte's proprietary software can detect which hashed credentials belong to which user.

Egnyte implements multiple measures to prevent unauthorized access after a user has logged in, issuing a session time outs, and alerting admins when Egnyte is accessed from unexpected geo-locations that may indicate an insider threat.

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.

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 third-party apps) they can access and use. Customers 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.

Egnyte enables customers to define a user's role and then determine exactly what they can access and do, regardless of whether they are internal or external to the business. 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 employees.
- **Standard Users:** usually made up of non-employees, such as consultants and contractors, who are extensions of the company and need secure access to internal files to conduct business. A standard user allows authenticated and managed access to company content.
- **Anonymous External Users:** typically, business partners and others who need to exchange documents with the company but do not need authenticated access to files.

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

Access Permissions

Egnyte allows permissions to be easily set for an entire team (Group) within a company. Groups can include any combination of employees and business partners to meet the unique collaboration needs of the business. For example, a group can be created for the entire finance team.

Users and groups can be granted view, edit, full or owner access - administrators can set granular folder and sub-folder permissions for each individual user (e.g. none, read only, read/write, read/write/delete).

Permissions can be set for each folder and sub-folder, across all connected repositories, to prevent over-sharing and unnecessary access to sensitive information. For example, some folders can be set to preview only links that prevent users from downloading, printing, and copying files. Customers can also secure named distribution, as well as take advantage of detailed tracking for complete visibility into the activity surrounding their user activity and files.

These advanced access controls are critical to the implementation of the data's structure and hierarchy. Access permissions are always uniformly enforced, irrespective of location and access method (web browser, desktop app, secure FTP, mobile app).

Encryption in Transit

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 protect the integrity and privacy of transmissions, Egnyte uses HTTPS and secure FTP protocols to create a protected, encrypted channel.

To encrypt the data during transmission, Egnyte uses 256-bit AES, which is one of the strictest standards available. Egnyte's encryption system can not only be used to protect data to and from Egnyte services, but also to protect files shared externally, so users no longer need to send unsafe email attachments. This allows businesses of any size to leverage data encryption to secure all their file sharing and collaborative efforts.

"Customers who want more control can elect to manage their own keys."

Encryption at Rest

Even with every door blocked and every entrance guarded, Egnyte 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 if someone were to gain access to data on the servers, it would be impossible to read. Encryption keys, which are unique to each customer, are stored in a secure key vault, which is accessed only by the Egnyte Object store software. Additionally, data is stored in a hashed structure that can only be navigated through Egnyte's proprietary platform software.

Egnyte Object Store

Egnyte has built its own, patented storage management system, called Egnyte 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.

File Encryption and Key Management

Files uploaded to Egnyte are encrypted by default, using 256-bit AES encryption with a key that is unique to each customer. Egnyte manages this encryption key and follows best practices to secure, store, and manage these keys for customers. If a customer would like to control their keys they can manage, rotate, and store their encryption keys themselves.

Egnyte Key Management (EKM) allows customers to manage their keys, using a third-party cloud service or their own on-premises infrastructure. Egnyte currently integrates with the following external key management systems: Microsoft Azure Key Vault, and Amazon AWS CloudHSM.

Application & Data Vulnerability Detection

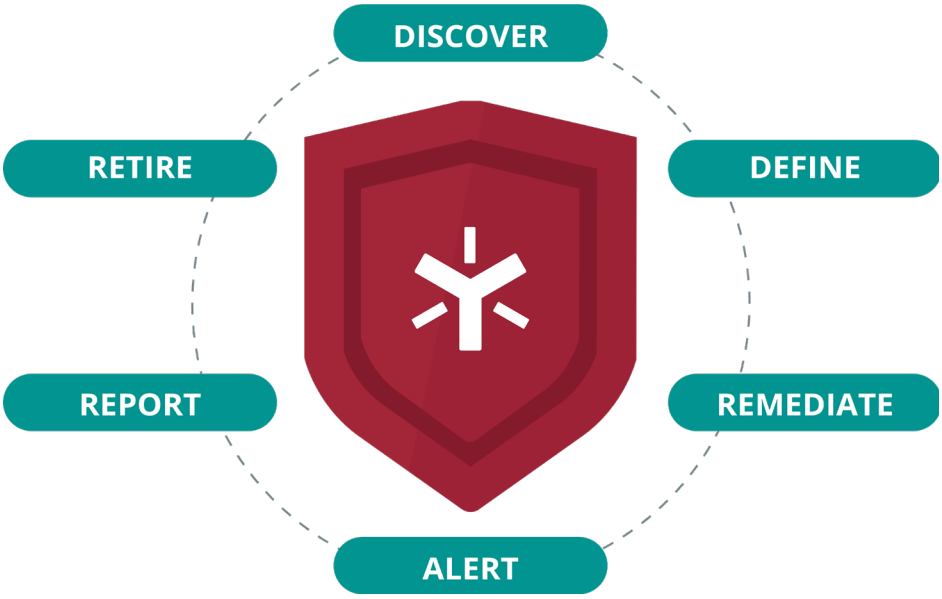
Egnyte has a multi-pronged strategy to detect and remove vulnerabilities to keep customer data safe. Egnyte's in-house security team is continuously monitoring the applications and infrastructure, conducting regular penetration tests, security audits, and code reviews, both automatically and manually, 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 design to implementation, testing, and solution deployment. Egnyte embraces the DevSecOps principles for all software deployment.

Egnyte uses a third-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. 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. To learn more, please contact Egnyte for the Third-Party Security and Penetration Document.

Egnyte'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 a business' overall application and data usage, highlighting any changes that could indicate a breach or potential issue that needs to be investigated and remediated.

Compliance, Governance, and Privacy

Strong governance is the foundation of a sustained data privacy and security posture. In order to comply with regulations, protect IP and customer information, and keep files safe from data leaks, Egnyte builds visibility and control into the entire content lifecycle. This allows administrators to make informed, data-driven choices about their content. A data lifecycle approach makes it easy for businesses to manage their files and control who has access, from the day they are created to the day they are deleted. Egnyte's data governance workflow covers all stages of the content lifecycle: Discover, Define, Remediate, Alert, Report, and Retire.



Discover

Automate Sensitive Data Classification

You can't secure your most sensitive data if you don't know where it is.

Egnyte scans the content of the files in all linked repositories to identify sensitive content, such as credit card numbers, addresses, dates of birth, social security numbers, and health-related information (e.g. patient ID numbers). Egnyte's classification engine comes more than 400 patterns of Personally Identifiable Information (PII) and content types built-in, in multiple languages (including those for all EU member nations).

Customers can use any of Egnyte's out-of-the-box data governance configurations that lay the groundwork for compliance with global data use regulations (HIPAA, GDPR, etc.) or choose custom parameters that are unique to the business, such as keywords (e.g. client names), patterns, file properties and document templates, to scan more than 50 file types. Egnyte's dynamic classification back-end makes it easy to add or modify classification policies as the business changes, automatically applying updates. As Egnyte develops new classification templates to match international data privacy regulations, these policies are immediately available to Egnyte customers.

Define

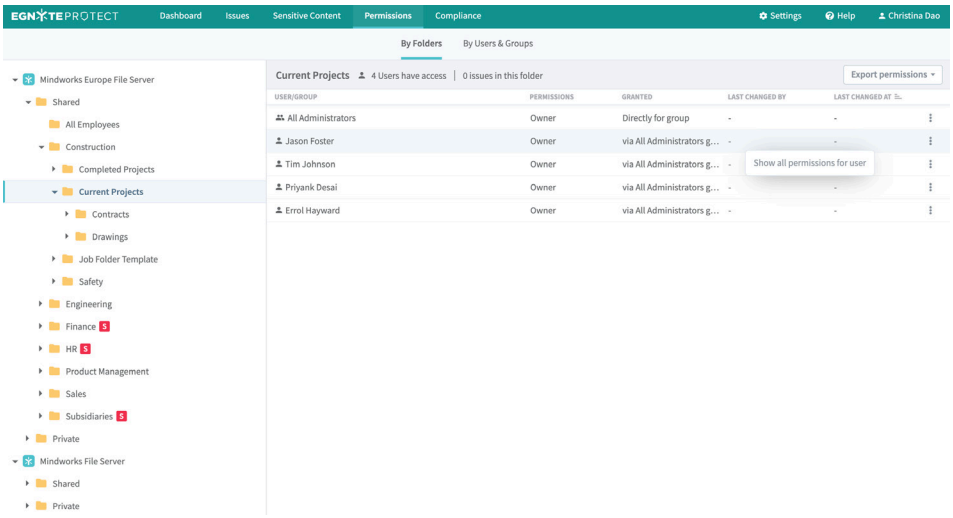
Access & Content Sharing Controls

Egnyte offers robust access controls and digital rights management (DRM) capabilities that empower organizations to protect their critical data, such as legal documents, intellectual property, and sensitive, regulated information.

Egnyte Protect surfaces sensitive data found under chosen classification policies and displays it in a central dashboard, giving businesses visibility into all their content repositories to see where sensitive content is, who has access to it, and whether it is being shared. It provides a window into exposure points, like unsecured public links or files being shared with external parties or unprivileged groups. Admins can remediate issues to effectively restrict access to content, in accordance with the law, as well as their other corporate and security objectives.

Permissions Browser

Egnyte's Permissions browser makes it easy to audit who has access to your sensitive data and how that access was granted, so permissions can be adjusted, as needed, to mitigate risks.



Content Safeguards

Content Safeguards protect your repository from data leaks by restricting public links to sensitive files. Administrators can create Content Safeguards policies that restrict links to a minimum security level, based on sensitive content matching, risk score, and location. These policies are then enforced in the Connect repository.

Remediate

Address and Resolve Issues

Customers can remediate issues by disabling links to content in Egnyte that contains sensitive data, taking action on compromised accounts, forcing password resets, adding user exceptions, deleting empty or unused groups, or moving or deleting sensitive content that is being shared too broadly or stored in unauthorized locations. With Egnyte, organizations also have the visibility and insights needed to address broader issues, such as a sprawling, anything-goes folder structure or employees who consistently mishandle sensitive information, that could put the business at risk.

Egnyte uses location-based rules to flag suspicious access indicating a potential compromise. By default, the platform restricts access from countries that appear on the US State Department's export control list, including China, Russia and North Korea. Administrators can easily remove individual countries from the restricted list to suit their business needs. Egnyte also detects and alerts admins to 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.

Ransomware

When an authorized user solicits content from an unlicensed, external party, that content is scanned for malware signatures upon upload, including known bad file extensions. Egnyte's signature-based ransomware detection runs a deep scan of all content in Egnyte and Windows File Server to detect known patterns of ransomware such as the presence of "ransom notes" in your content.

Signature-based ransomware is excellent at detecting known file types associated with ransomware. It is a great first line of defense. But what about ransomware that has never been seen before? Egnyte also includes behavior-based ransomware detection, which helps find previously unknown types of ransomware that can ravage your system. A proprietary machine learning model looks for patterns of user activity associated with ransomware such the rate of file rename, creation, and deletion, and encryption, and alerts you to potential threats.

Egnyte alerts administrators to accounts have potentially been compromised and prompts action before attackers can gain access to sensitive documents. Administrators can then lock down access to the file and quickly disable compromised accounts. In the event that loose credentials lead to a ransomware attack, Egnyte can help identify affected files and roll back to the last good version.

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

Behavioral Analytics

Egnyte integrates behavioral analytics to understand the typical behavior of a business' users and what their usual patterns of data consumption are. The platform develops a fingerprint of how users consume data, creating a snapshot that becomes more high-resolution over time, as more behavior can be analyzed. Egnyte will alert on behavior that is abnormal, empowering administrators to determine whether it's acceptable or take action, as appropriate.

The Issues tab provides quick remediation options for disabling their account to stop the theft in its tracks or allowing the exception. Administrators can also set a detection threshold for unusual activity in their organization, which can be adjusted for greater or lesser sensitivity to anomalous behavior.

Alert

Stay on Top of Issues

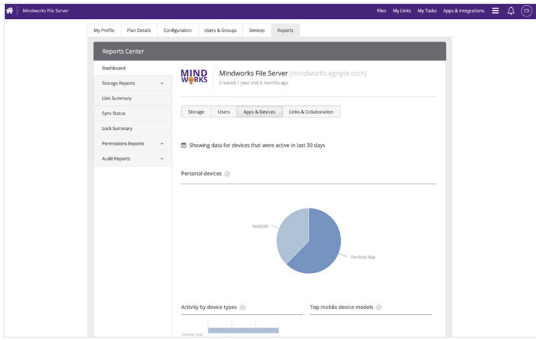
Egnyte flags unusual activity or issues that arise that could represent risky configurations, insider threats or malicious actions. Businesses can customize alerts based on recipient, issue type, sensitive content type, level of severity. Egnyte leverages machine learning to become better at alerting as it learns more about typical data behavior inside your organization. From Egnyte's Issues tab, businesses can identify problems, including:

- **Unusual Access**: Uses machine learning to flag users downloading or deleting unusually large amounts of data to help prevent data theft and loss.
- **Compromised Accounts:** Flags users who appear to be logging in with compromised credentials.
- **Ransomware Infection:** Detects suspected ransomware affecting a user account.
- **Public Link:** Detects files and folders accessible via public links. These are any links that do not require a password and are not limited to domain users (i.e. they are open to the public).
- **Open Access:** Detects folders that are permitted to groups containing many users, which may mean they are accessible by many more people than intended.
- **External Sharing:** Detects files and folders that contain sensitive content that are accessible by people outside your organization.
- I**ndividual Permission:** Detects folders that are directly permitted to individual users, rather than to groups. It is a general security best practice to grant permissions to groups of users rather than individuals.
- **Empty Group:** Detects groups that do not contain any users. This rule helps keep data repositories clean, so they are easier to manage. Removing empty groups means users are less likely to grant permissions to the wrong people.
- **Unused Group:** Detects groups not used to grant any folder permissions. This rule helps keep data repositories clean, so they are easier to manage. Removing unused groups means users are less likely to grant permissions to the wrong people.
- **Sensitive Content Alerts:** Alerts you to locations where regulated or personal data is known to be.

Egnyte allows administrators to set sensitivity thresholds for alerting on certain kinds of issues (for example, HIPAA content) to reduce the amount of noise and get alerted only to the most critical issues.

Report

Share Progress & Support Regulatory Compliance



Egnyte gives customers comprehensive dashboards of analytics around content, users, devices, applications, and more to help identify potential threats and support compliance across the file environment. Egnyte allows lists of access issues and sensitive content locations to be exported from the platform to be shared with relevant business units and stakeholders.

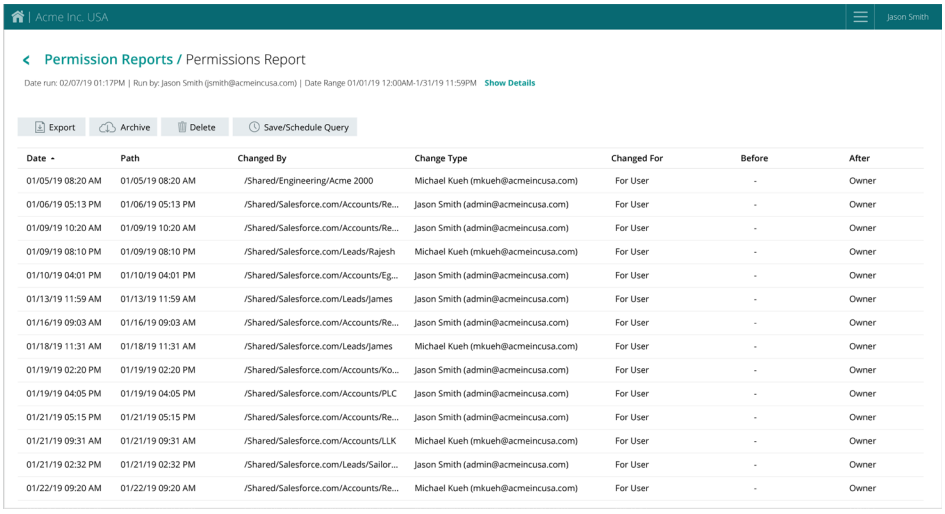
Customers have access to unique insights about user, file, and device activity that can be harmful to their organization. This information enables them to take appropriate measures to strengthen their security or eliminate a threat. In addition, Egnyte includes reporting functionality for data breach responses to maintain compliance with data privacy laws.

Audit Reports

Egnyte helps businesses streamline compliance with data privacy regulations that require audit reports on usage and access. Audit reports help businesses track key actions taken in the platform, such as users logging in, allowing or disallowing sensitive content in specific locations, moving or deleting files, and viewing sensitive content. The reports provide a 360-degree view of all activities, allowing administrators to view all:

- User access activities, such as login, logout, and password resets, with specific IP address origination and device information.
- File activities, including uploads, downloads, deletes, links shared, etc..
- Access permission changes. For example, new permissions granted or revoked from folders.
- Make note of the Egnyte Protect dashboard.

These auditing capabilities, combined with Egnyte's central administration, provides administrators the full suite of enterprise controls they need to manage data across all their on-premises and cloud repositories. This level of control and visibility is critical to ensure compliance to regulatory requirements, especially in industries such as healthcare and financial services.



Date	Path	Changed By	Change Type	Changed For	Before	After
01/05/19 08:20 AM	01/05/19 08:20 AM	/Shared/Engineering/Acme 2000	Michael Kueh (mkueh@acmeincusa.com)	For User	-	Owner
01/06/19 05:13 PM	01/06/19 05:13 PM	/Shared/Salesforce.com/Accounts/Re...	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/09/19 10:20 AM	01/09/19 10:20 AM	/Shared/Salesforce.com/Accounts/Re...	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/09/19 08:10 PM	01/09/19 08:10 PM	/Shared/Salesforce.com/Leads/Rajesh	Michael Kueh (mkueh@acmeincusa.com)	For User	-	Owner
01/10/19 04:01 PM	01/10/19 04:01 PM	/Shared/Salesforce.com/Accounts/Eg...	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/13/19 11:59 AM	01/13/19 11:59 AM	/Shared/Salesforce.com/Leads/James	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/16/19 09:03 AM	01/16/19 09:03 AM	/Shared/Salesforce.com/Accounts/Re...	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/18/19 11:31 AM	01/18/19 11:31 AM	/Shared/Salesforce.com/Leads/James	Michael Kueh (mkueh@acmeincusa.com)	For User	-	Owner
01/19/19 02:20 PM	01/19/19 02:20 PM	/Shared/Salesforce.com/Accounts/Ko...	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/19/19 04:05 PM	01/19/19 04:05 PM	/Shared/Salesforce.com/Accounts/PLC	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/21/19 05:15 PM	01/21/19 05:15 PM	/Shared/Salesforce.com/Accounts/Re...	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/21/19 09:31 AM	01/21/19 09:31 AM	/Shared/Salesforce.com/Accounts/LLK	Michael Kueh (mkueh@acmeincusa.com)	For User	-	Owner
01/21/19 02:32 PM	01/21/19 02:32 PM	/Shared/Salesforce.com/Leads/Sailor...	Jason Smith (admin@acmeincusa.com)	For User	-	Owner
01/22/19 09:20 AM	01/22/19 09:20 AM	/Shared/Salesforce.com/Accounts/Re...	Michael Kueh (mkueh@acmeincusa.com)	For User	-	Owner

Responding to Requests for Personal Data

Egnyte makes it easy for organizations to quickly search for a user's personal data and export pre-formatted reports to respond to data subject access requests, which they must complete in order to comply with regulations like GDPR and CCPA. With Egnyte, it is easy to:

- Collect all the personal data about the requestor across the organization's repositories
- and archives. Note, organizations can also create and manage archive instances in support of custom searches for e-discovery.
- Verify the data to ensure that it is the right personal data for the right person. For example, if the business has two individuals with the same name and only one of them requests "to be forgotten," the business must be able to verify they've collected and deleted the data for the correct individual, while leaving the data for the other undisturbed.
- Identify specific files containing the data subject's personal data, so they can delete or dispatch them.

Retire

Delete or Archive Stale Data

Whether for contractual or legal reasons, many companies must retain certain kinds of content for specified periods of time. But holding content that is no longer being used can clutter the file environment and impact productivity, as well as pose a risk. The more content you house, the more can be stolen or leaked.

Egnyte helps customers minimize these risks through policy-driven retention, archiving, and deletion. Egnyte, customers can define retention periods based on location or data classification rules, and automatically and securely purge or archive that content once the retention period has expired. Content marked with retention periods can be deleted from folders, enabling users to effectively manage their work, but won't be purged from the underlying repository until the defined retention period has expired. Retention policies can be locked to prevent accidental or intentional overrides and ensure compliance with regulations as well as peace of mind.

When files are deleted they are automatically sent to the Trash folder, which can be configured to restrict access only to Administrators. If needed, Administrators, or Power Users, if configured with this permission, 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 platform. 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:

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

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 indexed content used in searches.

Egnyte produces audit reports that provide account administrators an audit trail of all data that has been removed from the platform. Egnyte also has a robust trash management API for customers who desire additional flexibility and control, via external applications.

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

Minimize Your Data, Minimize Your Risk

By automatically removing old, stale or risky content in accordance with policy, you reduce your overall data footprint, limiting the attack surface and lowering your overall risk in the event of a breach. Egnyte's Data Minimization Dashboard provides file analytics that allow admins to visualize where risky, redundant, or stale data lives, and optimize the data environment to reduce risk.

Secure Deployment Options

The first step to securing business 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 industry and government regulations that dictate where certain sensitive information must reside and how it must be protected. For example, the European Union's General Data Protection Regulation (GDPR) institutes strict controls around how personally identifiable information (PII) can be used and where it must be processed and stored (within an EU country's borders). Egnyte is storage agnostic, offering multiple storage deployment models to enable customers to choose the secure, storage options they need to meet all their compliance and business requirements.

Egnyte Secure File Cloud Storage

Customers can store and manage their data within Egnyte's global, secure cloud infrastructure. This infrastructure was purpose-built to meet a business' security and availability requirements, implementing industry best practices to deliver a fully encrypted, fully redundant cloud storage solution.

Support for Third-Party Cloud Storage

If a customer needs to comply with specific data residency requirements, they can utilize an in-region third-party cloud provider. Egnyte supports all major third-party cloud storage providers, such as Amazon AWS, Google Cloud, Microsoft Azure, or any other S3-compatible cloud storage provider, to ensure customers can design a solution that best meets their unique needs.

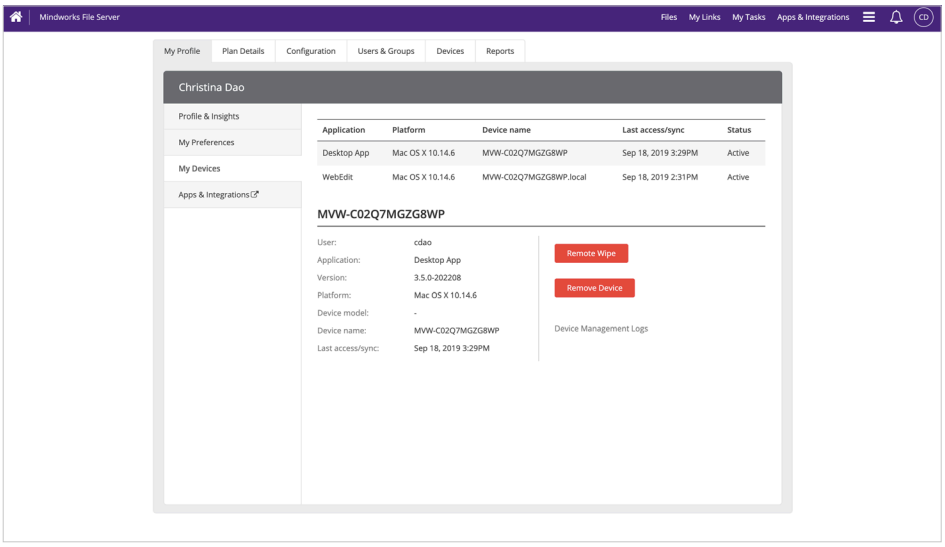
Secure Hybrid File Storage

Egnyte gives customers the ability 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. Egnyte's storage sync complies with the Center for Internet Security (CIS) Level 1 hardening guidelines for optimal data protection. The ability to automatically sync files minimizes any disruptions from network outages and enhances the overall availability and performance of an organization's data. For example, if the WAN goes down or the on-premises storage becomes unavailable, users at the affected location will still have access to their files.

"Once sensitive content is surfaced, administrators can monitor where that data is housed and who has access to it, and quickly address issues from a central dashboard. "

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.



Enterprise Mobility Management (EMM) & Mobile Device Management Integration

Egnyte can integrate with enterprise mobile management (EMM) and mobile device management (MDM) containers to allow customers to install and manage the Egnyte mobile applications with a broader set of mobile policies to deliver consistent 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). 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 solutions, Egnyte provides a host of native device control capabilities outlined below.

Mobile Passcode Lock

Organizations 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 for Mobile Devices

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

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.

Mobile File Encryption

As already noted, 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, customer files are always encrypted.

Datacenter Security

For data stored in Egnyte's datacenters, Egnyte protects the servers where the data resides, 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's 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. All Egnyte servers are hosted on redundant local area networks and the servers themselves are equipped with redundant electrical supplies to protect against unforeseen power outages and electrical surges and ensure the uninterrupted accessibility of data.

Only a few designated Egnyte Operations Administrators have the clearance level to access Egnyte's datacenter to perform their jobs. These administrators undergo third-party background checks and stringent security training. This team only has the access required to perform scheduled hardware inspections and maintenance. Any operational activity, including facility access, replacing hardware components, and removing media is strictly monitored and audited.

To protect against attacks aimed at the equipment and data housed in the datacenters, Egnyte employs state-of-the-art security technologies. Egnyte uses ICSA-certified firewalls to police traffic between public networks and the servers where company data resides, as well as separate local firewalls to provide an additional layer of data protection. In addition, Egnyte uses network intrusion prevention systems (IPSes) to monitor and block hackers, worms, phishing, and other infiltration methods.

To learn more about Egnyte's datacenters, please **contact Egnyte** for the Datacenter Protection Document.

Egnyte Compliance Certifications

SOC 2

Egnyte is SOC 2 SSAE 18 Type 2 compliant, ensuring that data is securely managed and the interests of customers and the privacy of all clients is protected. Egnyte's compliance is supported by a SOC 2 attestation report issued by an independent auditor, whose role is to assess vendor compliance within selected Trust Services categories.

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 to give confidence to interested parties that risks are adequately managed. This certification validates that Egnyte products, supporting infrastructure, people, and processes operate 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

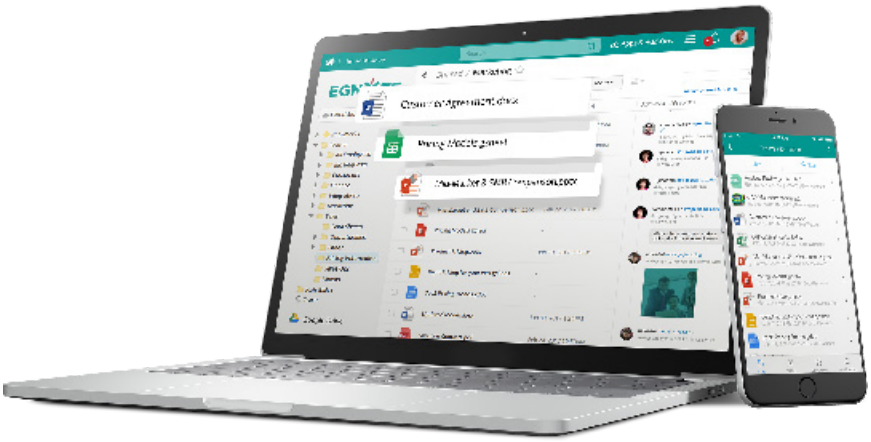
Egnyte understands the importance of the confidentiality and security of an individual's Protected Health Information (PHI). Egnyte's comprehensive data security enables HIPAA/HITECH compliance for Payer, Provider, pharmaceutical, and biomedical businesses. In addition, Egnyte is in full compliance with FDA 21 CFR Part 11, as well as the aforementioned SOC 2, ISO, and CSA regulations.

EU Customers

Egnyte complies with the requirements of the General Data Protection Regulation (GDPR), helping organizations meet data privacy obligations across the globe. In addition to GDPR compliance, Egnyte supports data sovereignty, ensuring compliance to the laws and standards of any location where data resides. Egnyte stores all European customers' data and metadata in its European datacenter. The data does not leave the EU. When a customer opens a support ticket, it is handled by a European support team.

Summary

Egnyte delivers the visibility, control and protection businesses need quickly discover, manage, and safeguard the content that matters most to support their security and compliance objectives. Egnyte is simple to use, quick to deploy, and requires almost no training for administrators or end users. It centralizes data access policies and eliminates end user data classification, time-intensive scanning methods, and burdensome incident response processes. Egnyte jumpstarts your governance and compliance efforts by addressing some of the most complex unstructured data problems within an enterprise. With Egnyte, companies have 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 and hybrid solutions, Egnyte provides the flexibility and control needed to address the security, compliance, and collaboration needs of the most demanding organizations around the world.



READY TO TRY EGNYTE ?

1-877-734-6983

EGNYTE

Smart Content Collaboration & Governance