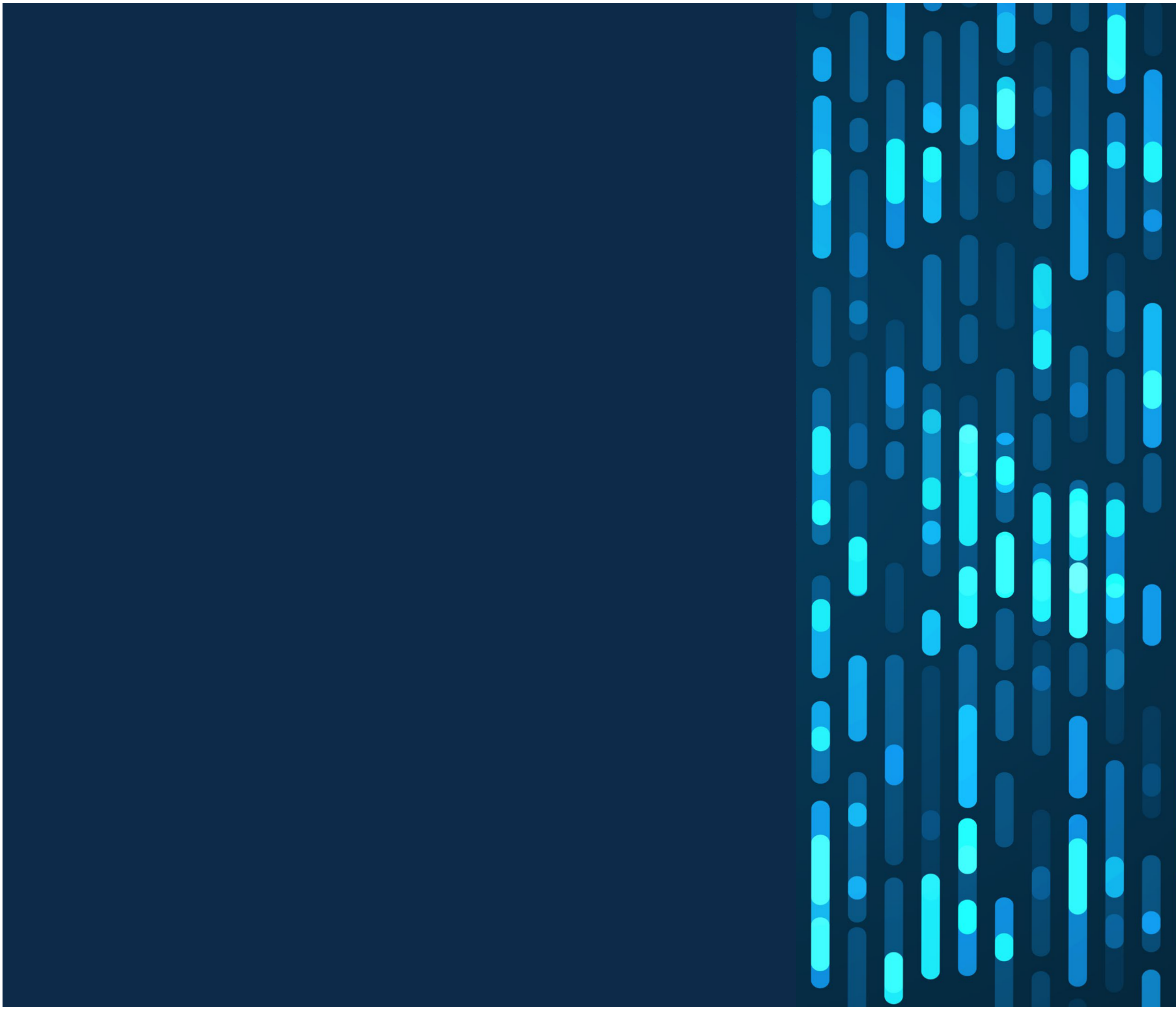
Security Framework

Table Of Contents

DOCUMENT OVERVIEW 3
FAQs 4
CLOUD DATACENTER SECURITY 5
USER DATA SECURITY AND ISOLATION 7
EMPLOYEE SECURITY 8
SECURITY PROCESSES 10
CUSTOMER SOLUTION SECURITY 12
REGULATORY COMPLIANCE CERTIFICATIONS 14
CONNECT WITH OUR SECURITY TEAM 15



DOCUMENT Disclaimer

This whitepaper describes the current state of Egnyte's security as of January 2023, which is subject to change with future feature and product launches. We understand that a good security program requires ongoing efforts, constant evaluation, and updates to improve infrastructure and cloud offerings. Therefore, we regularly conduct internal and external assessments and perpetually update and improve our policies so that existing controls comply with the highest security, privacy, and compliance standards. Consequently, some parts of this document may become obsolete without notice. Egnyte makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information in this document. Egnyte shall not be liable for any loss or damage arising from or in connection with the use of this document or any part thereof.

Frequently Asked Questions

FAQs

What is Egnyte?

Egnyte is a SaaS platform designed to provide seamless content collaboration through access and integrations, compliant content governance to proactively protect sensitive data, and a robust modern infrastructure to reduce ownership and operating costs of an on-premises file system architecture. Access to content is available through several clients to provide a native interface to the data. Web portal, drive letters, mobile devices and 3rd party integrations are all ways to access content in the office or on the road.

Is Egnyte SaaS, PaaS, IaaS, hosted on-prem, other?

Egnyte is a cloud-based SaaS platform. Delivery of the platform is owned solely by Egnyte and does not require the customer to own or maintain virtual infrastructure. The content (folders and files) is solely owned by the customer and is not accessible by any Egnyte personnel.

Is our data encrypted?

Egnyte stores customer data in uniquely encrypted client domains. Egnyte encrypts all data in transmission and at rest with 256-bit AES encryption. By default, Egnyte manages customer encryption keys according to industry best practices, including an ISO-27001 compliant Cryptographic and Key Management Policy. Egnyte supports our customers' ability to own and manage their own encryption keys, either using a 3rd party cloud service or their own on-premises infrastructure.

Does Egnyte have access to customer data?

No Egnyte personnel or third parties have any access to customer data.

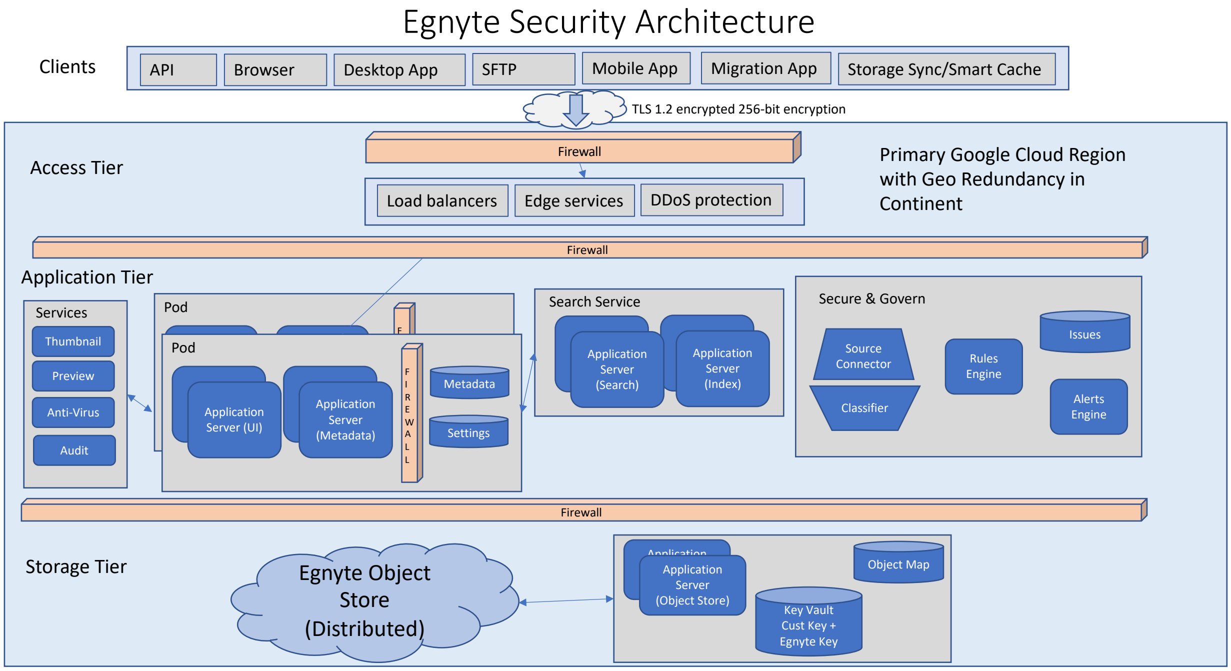
What protections does Egnyte have for ransomware?

In some cases, Egnyte can detect and block the affected user's machine from uploading or syncing files. This prevents rampant spread of the encryption to other files. However, this detection and blocking is not possible in all cases. We are continually enhancing the tools to recover and restore the customer's files as quickly as possible from Crypto encryption.

How we Secure our Environment

CLOUD DATACENTER SECURITY

All hardware and software operate in Google Cloud Services that run in a highly scalable and redundant architecture. Because of the scale and critical nature of these facilities, security is typically at a much more sophisticated level than can be done in an enterprise datacenter. This approach is outlined below.



Physical Security

These data centers are protected with several layers of security to prevent any unauthorized access to data. They feature layered security with custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and laser beam intrusion detection. They are monitored 24/7 by high-resolution cameras that can detect and track intruders. Most importantly, all data is duplicated to other data centers located in separate facilities and geographies within region.

Hardware Security

Hardware infrastructure is purpose-built using custom Titan chips to provide a hardware root-of-trust. End-to-end provenance and attestation reduce the "vendor-in-the-middle" problem. The OS is a stripped down, hardened version of Linux which has been verified, validated, and compiled in a secure environment.

Cloud Network Security

Cloud-to-cloud network security is protected using Virtual Private Cloud (VPC) service to provide connections between centers without using the public Ethernet. For external connections, Firewall configurations are enforced by policies in which Egnyte audits, verifies, and analyzes the effects of firewall rules regularly. In addition, a cloud based Cloud IDS is used to provide a managed, cloud-native intrusion detection to protect against malware, spyware, and Command-and-control attacks.

Network Security

Egnyte is responsible for user-to-cloud network security. However, some provider tools are useful in reinforcing network security. First, Cloud Load Balancing is used to provide automatic defense against Layer 3 and 4 DDoS attacks. Meanwhile, Cloud Armor filters incoming web requests by geography or other L7 parameters like request headers.   All communications with Egnyte – continuous data backup, access via the web browser or via desktop - is encrypted using 256-bit AES encryption over TLS 1.2 or later.

DevSecOps

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.

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.

Finally, a Binary Authorization tool is used to verify authenticity & only deploys images and patches when attestations meet organization policy. It also continuously validates conformance to the policy after deployment.

Egnyte Administration Security

Egnyte administration access is provided through a true zero-trust security model to provide Context-aware access. Zero trust requires verification of every session and implements 2 critical philosophies:

- Access based on both user identity and context.
- Shifts controls from network layer to application layer.

Together, these approaches allow the system to make context and behavior-aware decisions to support security. Only a few designated Egnyte Operations Administrators have the clearance level to access Egnyte's infrastructure to perform their jobs including maintenance. These administrators undergo third-party background checks and stringent security training. All operational activity is strictly monitored and audited.

Security Monitoring and Operations

Security Monitoring and operations is continuously monitored through the Security Command Center. Here, Egnyte continuously monitors the cloud environment for misconfigurations, detects threats, malicious activity and helps maintain compliance. In addition, continuous audit logging supports a Security Orchestration, Automation and Response (SOAR) tool to allow Egnyte to respond and mitigate threats quickly.

USER DATA SECURITY AND ISOLATION

In addition to encrypting data in motion, Egnyte also encrypts data at rest. Files uploaded to Egnyte are encrypted by default, using 256-bit AES encryption with a key that is unique to each customer. Egnyte can maintain the key, or the customer can choose to maintain their own key.

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.

The encrypted Egnyte Object Store uses a custom application to store customer data as large, distributed objects. Therefore, even if a key was available, file information can only be decrypted by Egnyte cloud services which are also tightly held. This model also provides for geographically distributed redundancy as well as full file versioning for all files. If a file is damaged or deleted, it can be recovered. Finally, the Object store model makes Egnyte immune from executing code (such as malware) from inside a customer file repository. However, Egnyte scans all uploaded files for known malware signatures as a precaution against spreading malware.

Key Management

Egnyte manages the 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 using Egnyte Key Management (EKM). 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.

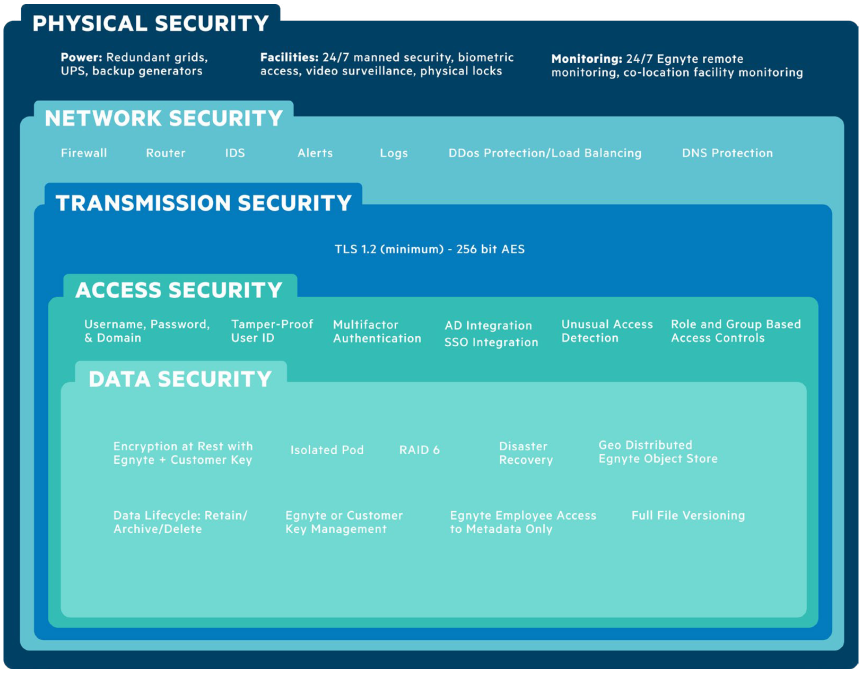
EMPLOYEE SECURITY

Even though system administrators managing your data are long-time Egnyte employees with significant training, unforeseen circumstances such as change of employment or unexplained activities may require Egnyte to take immediate steps to ensure maximum protection of your data. To this end, Egnyte has developed several procedures to manage both employee exit as well as a suspected security breach.

When administrators exit Egnyte through change of employment or termination, all electronic access to corporate resources is immediately terminated. Administrator passwords are changed and access to the data centers is removed. Egnyte also recognizes that even in the most secure systems, breaches of security, confidentiality, or other policies may occur. To this end, Egnyte has formulated a Security Breach Policy that outlines early detection and investigation procedures to mitigate any potential data threats.

SECURITY CONCEPTUAL MODEL

To summarize, Egnyte uses a conceptual model to design and enforce security architecture within the environment. There are 4 general layers including Physical, Network Security, Transmission Security, Access Security, and Data Security. These are shown in the diagram below.



PHYSICAL SECURITY

Power: Redundant grids, UPS, backup generators

Facilities: 24/7 manned security, biometric access, video surveillance, physical locks

Monitoring: 24/7 Egnyte remote monitoring, co-location facility monitoring

NETWORK SECURITY

Firewall

Router

IDS

Alerts

Logs

DDos Protection/Load Balancing

DNS Protection

TRANSMISSION SECURITY

TLS 1.2 (minimum) - 256 bit AES

ACCESS SECURITY

Username, Password, & Domain

Tamper-Proof User ID

Multifactor Authentication

AD Integration
SSO Integration

Unusual Access Detection

Role and Group Based Access Controls

DATA SECURITY

Encryption at Rest with Egnyte + Customer Key

Isolated Pod

RAID 6

Disaster Recovery

Geo Distributed Egnyte Object Store

Data Lifecycle: Retain/ Archive/Delete

Egnyte or Customer Key Management

Egnyte Employee Access to Metadata Only

Full File Versioning

Security Processes

SECURITY PROCESSES

Administration

Egnyte's infrastructure hosts customer data, and any negligence by server administrators while managing the infrastructure can interrupt access. To ensure maintenance activities are performed without incident, Egnyte enforces multiple security protocols. The Operations Management Team provides access on a need-only basis to administrators, restricting permissions so administrators can only work on components related to their current responsibility. Administrator passwords are changed on a regular basis by the Operations Management Team to maintain full control over the infrastructure.

Even though administrators are never given permission to access customer data, Egnyte has taken two additional precautions to ensure that your data is secure. First, your data is encrypted using AES 256-bit encryption, making all files completely unreadable. The encryption key is stored in a secure key vault that is a separate database, with restricted access that is monitored. Second, data is stored in a hashed structure that can only be deciphered through the Egnyte system software, making it impossible for any individual to view file or folder names.
Prior to access, all administrators undergo 3rd -party background checks, receive security training, and sign NDAs to enforce the privacy and confidentiality of their actions. Administrators are also required to maintain updated technical certifications regarding system management.

The Security Team regularly monitors all activity performed by administrators. In addition to validating the purpose of each administrator login, activity is continually monitored through log watch, syslog, auditD and other applications that track all commands and actions performed. These logs are reviewed frequently and are archived for future review. Any abnormal activity in the logs is promptly investigated by the Chief Security Officer.

Patch Management

Egnyte recognizes that system administrators make up only a portion of the personnel who manage Egnyte's infrastructure, and that the development of new software can also pose a risk to the security of your data. Therefore, Egnyte follows a strict Change Management Program and Patch Deployment Process before implementing any new software. Software updates managed by a single department may result in occasional security details being overlooked. That's why Egnyte requires four separate departments to review each update prior to release. Initially, the Product Management team runs a risk analysis and security review to understand the effects of new features within the system. Once approved, the Engineering Staff implements the features into a new patch. The security team and Operations Staff then run internal tests throughout the deployment process.

Egnyte understands that patches must be fully operational in the field, and that any software issues you experience can interrupt your ability to work with critical data. Therefore, patch deployment is implemented and monitored closely through a four-stage Patch Deployment Process.

First, software is tested by the Quality Assurance Team. The Operations Staff then releases the software update on Egnyte's internal system so that Egnyte employees and the company as a whole work with the newest release. After a designated period, the software update is released to a small percentage of customers (less than 5%), and performance is monitored closely by the Operations Staff. Finally, the update is rolled out to all customers through a rolling release schedule, updating new customers in batches every week.

Egnyte makes time appropriations for standard (pre-approved) updates, expedited (short interval change) updates, and emergency patches. Updates are generally installed on a quarterly basis unless emergency updates are required. Emergency updates are rarely given and have an expedited 24- hour turn-around using a truncated version of the Patch Deployment Process. The Security Council determines priority and must give final approval for all patches, including emergency releases.

How You Secure Your Solution

CUSTOMER SOLUTION SECURITY

Egnyte manages access to information using a multi-layered approach, using either built-in tools or integrated with customer systems. Egnyte provides basic username/password controls with options for setting password strength, password updates, renewals, etc. Multi-factor authentication Is provided as well. However, many customers integrate Egnyte with their own Single Sign on (SSO) and Active Directory services for even more convenience. In addition, Egnyte provides unusual access detection and sends alerts to admins when unusual access events are detected, such as impossible travel. Finally, Egnyte provides both Role and Group based access control management to simplify and scale controls for large organizations.

User Authentication

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.

Multi-Factor Authentication

Egnyte enables multi-factor authentication to allow 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.

Login Credentials

For direct login, 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. 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 geolocations 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.

Role-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. The user's role determines exactly what they can access and do, regardless of whether they are internal or external to the business.

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. 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 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. Access permissions are always uniformly enforced, irrespective of location and access method (web browser, desktop app, secure FTP, mobile app).

REGULATORY COMPLIANCE CERTIFICATIONS

Egnyte is certified for the following certifications.

ISO/IEC 27001:2013 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.

ISO/IEC 27018:2019 is a code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

SOC 2 SSAE 18 Type 2 is a trust services criteria for security, availability, processing integrity, and confidentiality set forth in TSP section 100, 2016 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

NIST 800-171. For customers that need to comply with the minimum cybersecurity standards set by DFARS, Egnyte has the necessary controls in place to meet the NIST 800-171 requirements through the implementation of the ISO27001 controls.

NIST 800-53. For customers that need to comply with the FedRAMP security standard, Egnyte has a dedicated EgnyteGov environment that adheres to all the controls outlined in the NIST 800-53 standard. Egnyte is currently going through the FedRAMP authorization process for this environment.

General Data Protection Regulation (GDPR). Egnyte complies with the requirements of GDPR helping organizations meet data privacy obligations across the globe. We store all European customers' data and metadata in a European datacenter. The data does not leave the EU.

How to Connect with Us

CONNECT WITH OUR SECURITY TEAM

Report a Security Issue
security@egnyte.com

Privacy Inquiries
privacy@egnyte.com

Compliance Standards
egnyte.com/security/compliance-standards

SECURITY DOCUMENTS

Egnyte Cloud Security Alliance Registry Listing
cloudsecurityalliance.org/star/registry/services/egnyte

Egnyte's Privacy Policy
www.egnyte.com/privacy-policy

Real-time uptime and downtime reports: status.egnyte.com