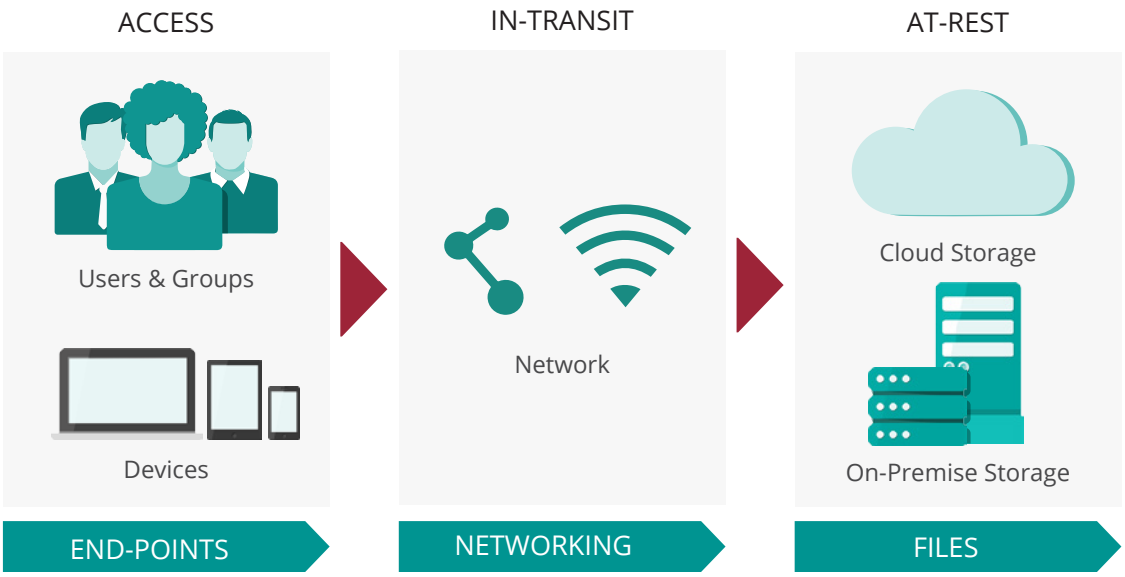
EGNYTE CONNECT℠

Data Sheet

EGNYTE SECURITY ARCHITECTURE

Comprehensive Data Protection and Privacy for Your Business

Security and privacy are top concerns of businesses when adopting new file services platforms. Growing data and users introduces the risk of security breaches, and tighter compliance regulations require greater focus. As an industry leader of enterprise file services, Egnyte provides world-class security with end-to-end, multi-level data protection to give your content the security it needs without impacting the convenience your users are demanding.



For more information, Contact a Product Specialist.

© 2016 by Egnyte Inc. All rights reserved

User Security

There is agreement among IT administrators that the most vulnerable point of any infrastructure is on the login screen. That is why Egnyte gives you strict user and login enforcement, including SAML 2.0 Single Sign-On (SSO), Active Directory, and two-factor authentication. Additional user security comes from subfolder permissions, minimum password length and strength, password rotation, password history, account lockout, and more to ensure that only users with the right credentials can access your company's data.

- Active Directory integration
- SAML 2.0 Single Sign-On
- Two-factor authentication
- Read/Write/Delete/Owner folder permissions
- Subfolder permissions
- Guest access roles
- Password rotation
- Minimum password length and strength

Device Security

The rapid increase in mobile usage has enabled significant productivity gains, but it has also created potential security concerns. To address these concerns, we have developed a comprehensive set of tools specifically for mobile users. With Egnyte, you can choose additional options including mandatory passcodes, idle-timeout settings, and automatic file wipe after a set number of incorrect passcode attempts. You can also control if files can be downloaded for offline access, and if that device is stolen, the employee or administrator can remotely wipe the offline files in the Egnyte application. If you are looking for additional security, local file encryption is also available. Finally, you can use certificate-based device trust, so that only authorized devices are allowed to access your files.

- Passcode use enforcement
- 256-bit AES on-device encryption
- Remote-wipe for mobile & desktop clients
- Trusted devices
- Offline file access controls
- Automatic offline file expiry

Content Security

Protecting your files when they are at-rest sitting on a hard drive is every bit as important as when they are being accessed. We address this by always using 256-bit AES encryption. We even take one step further by storing the encryption key in a secure key vault in a completely separate database that is decoupled from your files. In addition, you can use use multiple domains, each with unique encryption keys to further isolate content within your organization. And for when you need the highest level of security, Egnyte can be confugured so that your files and metadata reside and can be accessed on your premises and never touch the cloud.

- Tier III SSAE 16 compliant data centers
- Data center redundancy
- Crypto-shredding of deleted files
- Physical premises and rack security
- Network redundancy
- Available customer-managed encryption key solutions

For more information, Contact a Product Specialist.

© 2016 by Egnyte Inc. All rights reserved

Network Security

Egnyte takes a multi-layered approach to network security. First, we encode data during transmission using 256-bit AES encryption, which is the same technology used by the most secure institutions in the world. Next, we deploy ICSA-certified firewalls to police the traffic between the public networks and Egnyte's data center servers. After that, we incorporate SSL encryption and a network Intrusion Prevention System (IPS) to monitor and block hackers, worms, phishing, and all other infiltration methods. We also believe in perpetual improvement, so we employ a third-party security firm to perform continual penetration tests to confirm the security of our systems.

- 256-bit AES encryption in transit
- Network Intrusion Prevention System
- ICSA-certified firewalls
- Third-party security audits
- Real-time network monitoring
- Network security experts on staff

Data Center Security

When it comes to physical security of your data in Egnyte's data centers, we have taken steps to eliminate single points of failure to ensure your content is readily available. We have multiple redundancies for our servers, their components, and the associated LAN infrastructure. To protect against cable cuts and network outages, we use Tier-1 network carriers with multiple fiber-optic cables running on both sides of the building. Our data centers are also geographically separated to protect you from catastrophic outages and provide geographic redundancy. Finally, we have highly restricted access to the facility and equipment, including biometric locks, manned security and 24-hr surveillance.

- Granular access controls
- On-premises storage option
- Selective file sync
- Shared-link controls
- 256-bit AES encryption while at rest
- Domain-level data isolation / deduplication

Summary

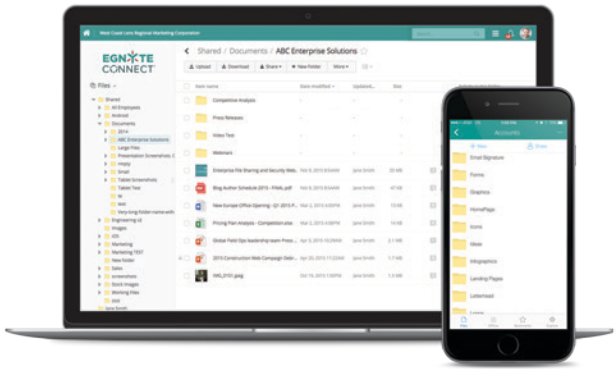
With the proliferation in consumer-grade, rogue file-sharing solutions, we know that it can be a struggle to gain visibility and control over company data, users and devices. At Egnyte, we put you back in control by providing an end-to-end file-sharing solution that supports pure cloud, on-premises, and hybrid deployment options to meet the security and compliance needs of your organization.

READY TO GET STARTED?
Contact a Product Specialist Today

Start Free Trial

For more information, Contact a Product Specialist.

© 2016 by Egnyte Inc. All rights reserved



READY TO GET STARTED?

Contact a Product Specialist Today

Start Free Trial

EGNYTE | Smart Content Collaboration & Governance

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

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