ACCESS AND SHARE FILES FROM ANYWHERE WITHOUT COMPROMISING DATA SECURITY

Empowering IT to Gain Complete Control

Highlights:

- Most secure enterprise file sharing platform
- Built-in Mobile Device Management (MDM) capabilities
- Deployment - Cloud only, On-prem only, or Hybrid
- 360º audit reports on ALL files, devices and user activity

Individuals and businesses alike are embracing the digital revolution. One of the most prominent drivers for this digital revolution is the increasing adoption of cloud. Cloud is not only transforming IT, but with 'Consumerisation of IT' and bring-your-own-device (BYOD) becoming pervasive, employees are rapidly adopting public cloud services to accomplish their work-related tasks. Cloud undoubtedly provides flexibility, enables collaboration and enhances productivity. As a result, employees are using consumer-grade file sharing applications to gain access to their work files anytime, without IT supervision.

In the absence of an IT-controlled file sharing system, when employees store sensitive work documents in the cloud they jeopardize the security of corporate data, exposing it to unwanted access, threats and data breaches.

Security Concerns around Rogue File Sharing

Security is the number one concern when adopting the cloud. IT departments are mainly concerned with:

According to Verizon, companies have lost an estimated 1.1B records over the past five years. 44M records were lost in 2013 alone.

DATA LOSS

In this BYOD era, companies significantly increase their risk of data leakage when employees store and share confidential business information in the cloud. Although, consumer-grade file-sharing applications have become convenient tools for employees to access data across multiple devices, they are inherently insecure and susceptible to data leakage. Many employees work remotely, telecommute or travel and access files from any convenient device. If these devices are lost or stolen, it can compromise important company data.

LOSS OF CONTROL AND VISIBILITY

Maintaining control over the data is paramount. As security threats increase not only in number, but also in variety and sophistication, IT departments are naturally concerned with losing control over the confidentiality, integrity, and availability of their data stored in shared environments. With the data actually residing in a datacenter managed by the cloud service provider, it becomes challenging for IT to enforce security policies to govern data access. Additionally, the loss of visibility and the lack of ability to monitor user activities puts corporate resources at risk.

According to the Cloud Security Alliance, data breaches were #1 on the list of security concerns affecting companies that employ the cloud for file sharing.

DATA BREACHES

News headlines about the increasing frequency of stolen information have focused heightened awareness on data breaches. Companies where employees use unauthorized file sharing practices, can lose data in a number of forms: government spying, data theft through malware, and malicious users misusing or tampering with sensitive information.

To top that off, recent revelations about NSA surveillance have heightened privacy concerns. Companies are now re-evaluating the way they store and share data and are realizing that not all files are meant to be stored in the cloud.

REGULATORY COMPLIANCE

Companies are required to comply with a growing number of regulations such as HIPAA, FINRA, the EU Data Privacy Directive, etc. They must be able to control, monitor and report on who is accessing what cloud-based resources, and for what purpose. Failure to ensure compliance can result in significant financial penalties and even jail time.

RELIABILITY

. An unreliable cloud storage system can result in unexpected data unavailability or even complete loss. Multiple factors including system crashes, natural disasters, and power outages can leave companies with no way to access their data.

Embrace the Flexibility of the Cloud While Maintaining Security Controls

Since data is a critical component supporting a company's daily business operations, it is essential to ensure privacy and protect data independent of where it resides. Companies need a secure enterprise-grade solution that meets the file sharing needs of their employees, while protecting sensitive business data end to end. According to a recent ESG survey, 97% of early cloud adopters prefer a hybrid model because it allows more flexibility and control. IT should have complete control over where corporate data resides and who is accessing it.

"Egnyte enables my team to do their job efficiently and makes my job easier. I know my files are secure because I have complete visibility and auditing into who is accessing which files and can ensure the right people are viewing the right files. Egnyte was easy to roll out and no training was needed for my staff and contractors to be up and running in a day."

David Kauffman
VP of Business Development
BL systems

Egnyte Provides a Robust Hybrid Cloud File Sharing Platform with Enterprise Grade Security

Egnyte provides comprehensive enterprise file sharing solution that provides secure access to 100% of customer files from any device, irrespective of where those files actually reside. It empowers IT with complete control and visibility while providing employees with secure and seamless access to data. Enterprises can choose to keep their data in the cloud, on-prem (without moving any data or meta-data through the cloud) or a combination of the two depending on the kind of data, size or sensitivity.

Egnyte's solution has been built with multiple levels of security providing comprehensive data protection at every layer.

ACCESS CONTROLS

With the ability to enforce automated access controls, Egnyte protects files from unauthorized access and helps comply with regulations.

DATA SECURITY

Egnyte adopts industry best practices for data encryption both for data at rest and in transit using AES 256-bit encryption.

NETWORK SECURITY

In order to police traffic between public networks and the servers where company data resides, Egnyte employs ICSA-certified firewalls.

PHYSICAL SECURITY

Egnyte provides this first line of defense with strong physical security around its data centers which reside in Tier II, SSAE 16 compliant colocation facilities.

360-DEGREE AUDIT

With centralized administration, 360 degree auditing and reporting capabilities, Egnyte allows IT to gain insights into potential security concerns.

PRIVACY AND COMPLIANCE

Egnyte strives to ensure privacy of data and helps companies comply with industry regulations such as HIPAA, FINRA, EU Safe Harbor framework, etc.

Conclusion

The consumerisation of IT, BYOD, and cloud are here to stay. While the cloud greatly simplifies files storage and anytime access, it also presents its own challenges.

Egnyte provides an enterprise file sharing platform that allows customers to securely access data from anywhere using any device independent of where it lives. In addition to providing deployment choice, it provides end-to-end data protection at every layer for automated security and compliance.

About Egnyte

Egnyte powers enterprise file sharing and access for more than 40,000 customers globally. The award-winning platform optimally balances IT's need for security, control, and compliance with users' demands for simple access to highly sensitive documents stored on-premises and low sensitivity documents stored in the cloud. Founded in 2007, Egnyte is a privately-held company headquartered in Mountain View, CA. It is backed by venture capital firms Polaris Partners, Kleiner Perkins Caufield & Byers, Northgate Capital Group, Google Ventures, Floodgate Fund, and strategic partners Seagate Technology, CenturyLink and an unnamed major storage vendor. Please visit www.egnyte.com or call 1-877-7EGNYTE for more information.

EGNYTE