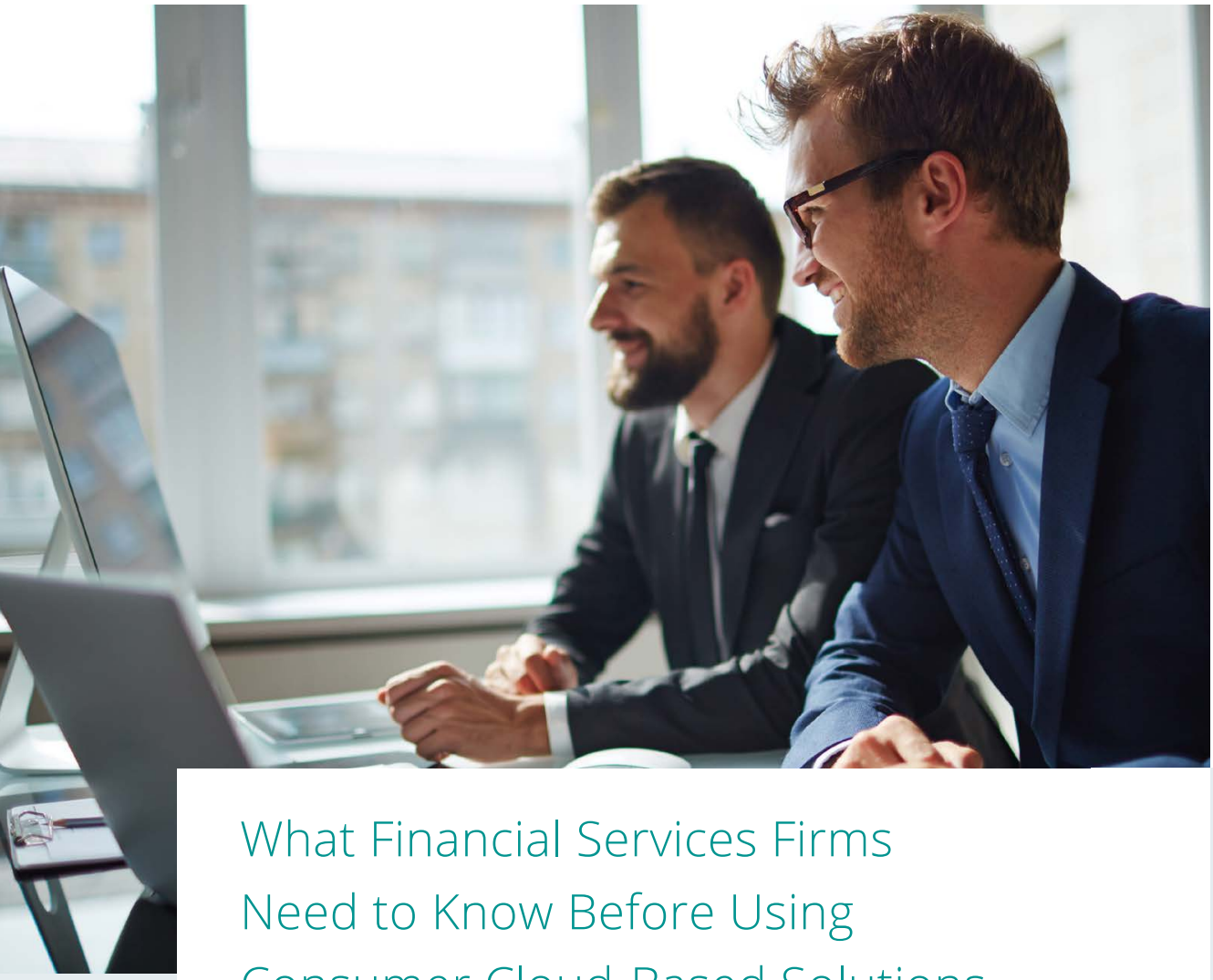
EGNYTE

Top 5 Considerations for Enterprise File Sync & Share Services



What Financial Services Firms Need to Know Before Using Consumer Cloud-Based Solutions

Table of Contents

ABOUT EGNYTE

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.

CONTACT SALES

US: 1.877.734.6983

UK: +44 (0)845.528.0588

www.egnyte.com

Executive summary

In today's connected age, financial services firms find themselves in a constant tug of war – on one side, they need to ensure that customers, employees, and partners have anywhere/anytime access to financial information in order to grow their business; on the other side, they need to ensure that personal customer information and sensitive financial files and data are tightly controlled to protect against costly data loss, fraud and misuse. It's a constant balancing act; one that is made even more complicated by the ever-increasing mix of rules and regulations on how firms must handle insider information, transactional data, client portfolios, etc., and the presence of shadow IT (file sharing methods outside the knowledge of the IT department).

Financial services firms face a constant balancing act complicated by an ever-increasing mix of rules and regulations.

So, how can financial services firms achieve the right balance? While there is no quick, simple answer, a good place to start is with the right file sharing service. Investing in an enterprise-grade file sync and share (EFSS) solution can give financial services firms the agility and freedom to securely share information to meet the varied requirements of their financial advisors and analysts, as well as their IT department, regulators, and customers.

A Ponemon Institute survey of IT practitioners identified securing documents and files containing intellectual property as the most compelling reason to invest in secure file sharing tools (80%), followed by the need to comply with data privacy regulations (77%) and the support of internal and external file collaboration (66%).

But not all file sharing services are the same. In fact, many of the consumer cloud-based services trying to make the transition to the enterprise do little to help financial services firms get the visibility and control they need to protect their customers' personal and financial information and achieve regulatory compliance, e.g. FINRA, PCI DSS. A review of popular cloud apps found 84% of the collaboration apps in use within enterprises today are not enterprise ready.

Typically, consumer cloud-based apps do not meet enterprise standards for security, auditability and business continuity. They were designed to be delivered in the cloud, not integrate with an enterprise's existing infrastructure. As a result, they create information silo's that add complexity and costs. The lack of vital on-premises capabilities means financial services firms cannot maximize their legacy data storage investments or meet data sovereignty requirements defined by the Financial Industry Regulatory Authority (FINRA), Payment Card Industry (PCI), European Union, and other governing bodies. In addition, consumer, cloud-based services often don't provide the granular policies, controls and reporting functionality needed to support secure, compliant file sharing and collaboration

Consumer cloud-based services impact your ability to address security, investment protection and regulatory requirements.

Egnyte Adaptive Enterprise File Services were designed to seamlessly integrate with a financial services firms' existing infrastructure to deliver the enterprise-grade capabilities financial services firms required to balance their information sharing and investment protection, and security goals. Egnyte enables firms to access and share files stored on-premises and in the cloud, providing unparalleled flexibility, unified visibility and centralized control that facilitates collaboration inside and outside the organization in a secure, compliant way.

This white paper covers the top 5 questions to consider while evaluating file sharing offerings to ensure you have the right solution for a financial institution:

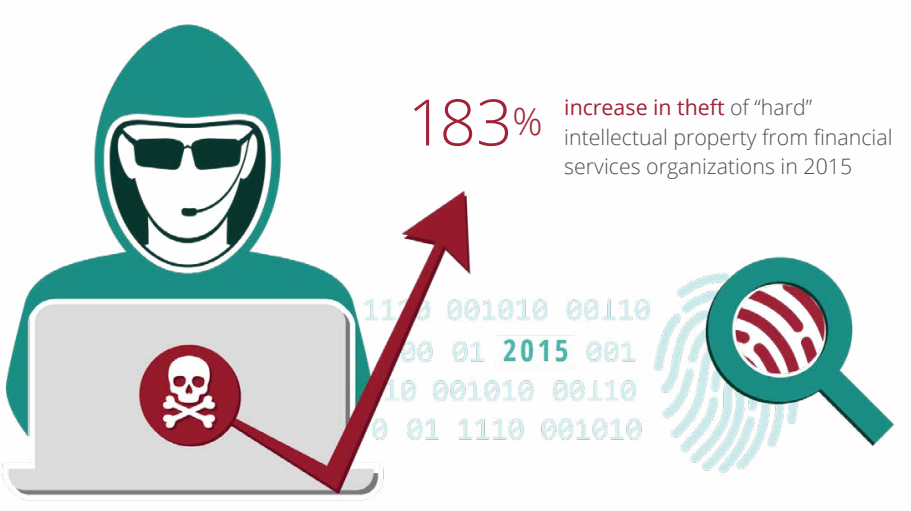
- **How Do I Minizize the Risk to My Content?** - Theft of intelectual property in financial services soared 183% in 2015.
- **How Do I Keep Track of Where My Content Resides?** - Financial services firms need constant visibility into where their information is and how it is being used across their different environments (cloud, on-premises, hybrid).
- **How is My Company Content Being Used?** - Thirty-two percent of organizations say that half of their employees regularly share content outside of the firewall.
- **Do I Have Control Over Regulated Content?** - Simple, effective role-based management can be used to define how files are accessed, used and stored to prevent data leakage and support an organization's compliance requirements.
- **Is My File Sharing Solution Compliant?** - Often, cloud-only file sharing solutions will use language that describes how they can "help you meet legal and regulatory requirements", but they are not actually compliant with the regulations.

Within each question, we will compare consumer cloud-based file sharing products with the Egnyte enterprise-ready file sharing solution, and explore how they each impact your ability to address security, investment protection and regulatory requirements.

Firms have very little control over where the cloud-only service provider stores their data and how it is protected.

How do I minimize the risk to my content?

Theft of "hard" intellectual property in financial services organizations soared 183% in 2015. It is reasonable to assume that financial services firms will continue to be of interest to cyber thieves given the highly valuable personally identifiable information (PII) and financial data (payment card numbers, insurance info linked to health records, etc., transactional info) they deal with on a regular basis.



It is important to ensure the right measures are in place to minimize the risks to that data. According to privacyrights.org data loss associated with portable devices, unintended disclosures and insider abuses make up the majority of compromises within the financial services industry.

Deploying a comprehensive data residency strategy both inside and outside your organization is very important. Any vendor you work with to implement your file sharing strategy should be able to integrate with your existing infrastructure and provide the visibility and control you need to protect your data from unauthorized access/usage and consistently enforce your policies. This requires a comprehensive approach to security.

The risks of using public cloud-only file sharing tools to share corporate data are fairly well documented. For starters, firms have very little control over

where the cloud service provider stores their data and how it is protected. As a result, data breaches involving company data stored in a public cloud environment are likely to go undetected and, very often, unreported, until it is too late. Even if data is encrypted, which is a best practice for protecting the privacy of content in the event it is stolen or intercepted, the cloud provider typically owns the encryption keys. This can jeopardize your ability to comply with regulations that require complete data sovereignty.

With Egnyte, you can be confident you have the comprehensive data protection and privacy you need to protect all your client and financial data. Egnyte gives you granular control over content, client, agent, employee, affiliate and guest access; devices, permissions and more to provide the highest level of security available.

You can apply authentication, authorization and access controls, down to subfolder levels, to ensure only those who are supposed to be accessing and sharing your files can do so. You can retain key management, creating and control your own encryption keys to secure designated files. As a result, you have full control over your data, giving you access to your firm's files anywhere, anytime, whether behind the firewall or in the cloud, while ensuring consistent encryption standards at every point. You also have access to native mobile device management capabilities, such as device pinning and remote wiping, to eliminate the risk associated with data being accessed on devices that are lost or stolen.

In addition, with Egnyte Smart Reporting and Auditing, firms gain actionable information on how their content is being accessed and shared, both internally and externally, across platforms, so you can address potential risks to client and financial data before it's too late. For example, IT admins can spot abnormal behavior (e.g. access of a client's portfolio by someone in engineering), using the solution's dashboards and audit reports, and proactively prevent costly breaches and/or fraud.

Egnyte can apply authentication, authorization and access controls, down to subfolder levels, to ensure only those with permission can access and share your files.

How do I keep track of where my content resides?

Is your content on-premises? In a private cloud? In a public cloud? If you are like most organizations, you probably have a mix. It is often born from necessity, as organizations store certain information on-premises, to comply with regulatory requirements, and then turn to the cloud to make other data more readily available to users on the go.

These varied deployments can lead to information silo's, which are exacerbated by the use of different cloud services by different groups, departments and business units. This creates unnecessary complexity:

- **Inhibiting productivity**, as users need to navigate different systems to get at the information they need, which means they have to remember where they put their data and manage version control themselves.
- **Adding costs**, as IT needs to maintain all these different systems to try to deliver a consistent experience and enforce consistent policies.
- **Reducing the ability of the financial services firm** to optimize the efficiency of their access, storage and protection infrastructures.

To regain control, financial services firms first need to gain visibility into where their information is and how it is being used across their different environments (cloud, on-premises, hybrid).

Most consumer cloud-based apps (assuming they are known and sanctioned) can only provide insights into the information stored within their own cloud. They cannot track or apply policies or controls to content stored on-premises or in other clouds. This means firms lose the ability to consistently enforce policies, which often leads to additional complexity and potential for error.

Egnyte has an open architecture that makes it easy to integrate and protect your existing infrastructure investments and eliminate information silos. With Egnyte, you gain full visibility into your content, across your cloud, on-premises and/or hybrid deployments. As a result, you can determine where you want your sensitive client and financial data to be stored (on-premises, in the cloud, or a combination) and how you want to make it accessible, to ensure content is always where it needs to be for those who need it, from a compliance, cost and performance perspective.

Gain full visibility into your content, across your cloud, on-premises and/ or hybrid deployments.

How is my company content being used?

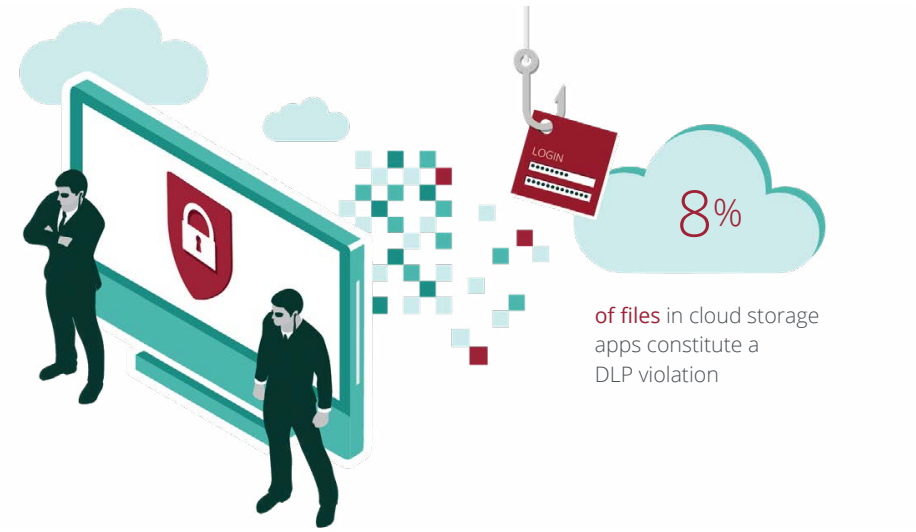
Recent research shows that 54% of employees use personal email to transfer business documents and data; 63% of employees use non-secure, remote storage devices, such as USBs and mobile devices for business file sharing. Many use these methods because it is so challenging to use some corporate-sanctioned file sharing services.

In order to curb these unsafe file sharing methods and cut down on Shadow IT, financial services firms need to ensure the file sharing services they offer actually meet their users' needs. If users won't use the service, it doesn't matter how secure it is. The solution you choose shouldn't disrupt the overall user experience (ideally, it will enhance it and improve productivity).

Financial services firms need to ensure the file sharing services they offer actually meet their users' needs.

Most cloud-only deployments, while user-friendly, typically don't meet enterprise security standards. You have very little control over exactly where your data is stored or how your data is protected. In addition, while cloud-only deployments may provide 'always available' access to users with an Internet connection, they are unable to satisfactorily service users that have low or no bandwidth available. Round-trip latency can make it virtually impossible to sync and share files across remote offices and distributed workers in environments with low bandwidth. This means your agents and clients may not have access to the critical information they need to make sound financial decisions.

Egnyte built its Adaptive Enterprise File Sharing Services to ensure it's easy for users to quickly access and share files to support collaboration, while providing IT the visibility and centralized control they need to enforce appropriate use. Users can use whatever device they want to access files, as if they were in the office. Egnyte supports users' iOS, Android, Windows and other devices and integrates with business apps, such as Outlook, Microsoft Office, Google Apps and many more to make it simple to enable collaborate with anyone, anywhere.



In addition, because of Egnyte's unique open architecture, which supports cloud, on-premises and hybrid deployments, the file services can adapt to factor in constraints within the environment they are operating to ensure users have continuous access to the content they need. For example, Egnyte Storage Sync has the ability to integrate with on-premises storage to offer fast access to large files for those instances when bandwidth is constrained, unavailable, or too costly.

Do I have control over regulated content?

Regulated file are files containing personally identifiable information (PII) or financial data. The storage and handling of this information is governed by a host of policies, rules and regulations.

It is important for financial services firms to identify and appropriately handle this regulated content to protect the privacy and integrity of this data and support compliance efforts.

Cloud-only solutions are generally unable to offer financial services firms the controls you need to maintain compliance. Often, they cannot guarantee data residency (particularly when they don't have a local data center) or provide the oversights IT requires to ensure regulated data is restricted to authorized access and stored appropriately. Eight percent of files in cloud storage apps constitute a DLP violation.

For example, the accidental unauthorized transmission of confidential information outside your network or across network boundaries is a DLP violation. With Egnyte, financial services firms have the visibility and control you need to design effective policies that adhere to your security and compliance requirements and optimize the use of your infrastructure, based on evolving user behaviors and content consumption. Egnyte ensures the integrity of your financial services firm's data by supporting on-premises, cloud and hybrid storage deployment options, with end-to-end file monitoring that gives you full

Consumer based cloud solutions are generally unable to offer financial services firms the controls you need to maintain compliance.

visibility into your content, regardless of where the files are stored or how they are being accessed and shared.

Simple, effective role-based management can be used to define how client information and sensitive financial files are accessed, used and stored to prevent data leakage and support your compliance requirements. With Egnyte, folder and sub-folder access permissions can be uniformly enforced across cloud and local storage systems to ensure policies are always applied consistently. Egnyte also provides robust audit reporting to monitor usage and access permission changes across all users to ensure any issues can be immediately addressed.

Egnyte's hybrid architecture enables firms to maintain complete control over where data resides.

Is my file sharing solution compliant?

There are a host of policies, rules and regulations financial services firms may need to adhere to during the course of their business. Including:

- Payment Card Industry Data Security Standards (PCI DSS)
- Financial Industry Regulatory Authority (FINRA) guidelines
- Criminal Justice Information Services (CJIS) requirements
- Securities and Exchange Commission (SEC) rules and regulations, etc.

These regulations govern how data needs to be stored, managed and maintained, with some imposing strict data residency requirements that limit the physical storage and access of data to certain geographies.

Additionally, global firms, depending on the countries in which they operate, may
be required to maintain data sovereignty and residency within a defined border to adhere to:

- European Union Data Protection Directive
- Germany's Bundestdatenschutzgesetz (BDSG)
- Russia's Data Protection Act
- British Columbia's Freedom of Information and Protection of Privacy Act, etc.

Most EU financial services firms operate globally, which means they need to be cognizant of how and where their regulated data is stored. It is important that you choose solutions that are compliant with the regulations to which you need to adhere.

Often, consumer cloud-only file sharing solutions will use language that describes how they can "help you meet legal and regulatory requirements", but they are not actually compliant with the regulations. This is an important distinction - to be compliant the solution must have been reviewed and audited by the regulatory body, which takes significant time and effort to accomplish.

Egnyte's hybrid architecture enables firms to maintain complete control over where data resides. In addition, Egnyte maintains compliance with the strictest standards to ensure financial services firms can enforce the privacy and data protection they require. For example, Egnyte is compliant with:

The EU Data Protection Directive

Which provides a consistent data protection framework with EU-level enforcement, and a baseline of security around information storage, transmittal, and processing.

FINRA

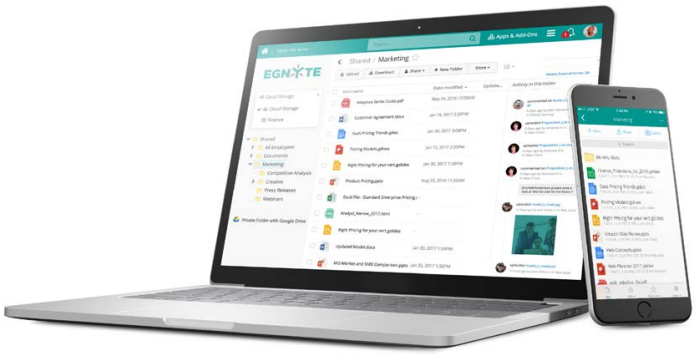
Where Egnyte is fully compliant with SEC 17a, 31a, 204 and recordkeeping regulations for confidential data storage, retention, digitalization and accessibility.

	Egnyte	Cloud-Only Providers	Egnyte Difference
Regulated and compliant Datacenter located in Europe to comply with European data sovereignty and regulations	✓	?	Ability to keep content on-premises without moving or copying to the cloud. Egnyte maintains a data center in Europe (Netherlands) for those European customers that are concerned about data sovereignty.
Hybrid deployment option	✓	?	Fast access to large files. Access to latest version of the file irrespective of the location (on-premises or on-the-go). Cross-site replication in the event a new site is added to improve productivity and user experience by enabling VPN-less access for users.
Open architecture	✓	?	Ability to integrate with any existing architecture. Ability to use any cloud storage. Ability to integrate with any CIFS compatible on-premises storage. Ability to enable any productivity applications with Egnyte's tight integration with Google Apps, SFDC, DocuSign Microsoft Office 365
Role-based administration	✓	?	Egnyte supports role delegation with Role-Based Administration that enables IT Admins to delegate certain functions to Business Leaders.
Advanced security and compliance	✓	?	Granular permissions at subfolder level and advanced admin controls. Role-based administration and option for European data center for data sovereignty.
Business continuity	✓	?	Egnyte's architecture enables business continuity with a copy in the cloud and copy on-premises for all the content.
Any Cloud storage, any On-premises storage	✓	?	Egnyte supports any cloud storage (Azure, AWS, Google etc.) Egnyte enables customers to preserve past infrastructure investments by plugging in right onto their existing storage infrastructure. Egnyte supports any CIFS compatible on-premises storage.
Power, Standard, External Users	✓	?	Each Egnyte user type has true enterprise experience.
"Standard User" License for enabling External Collaborators	✓	?	Full control on content, users, permissions and devices both for internal and external users. Security controls including link expiration.
Upload links	✓	?	Securely and anonymously enable external users to upload files without deploying the solution for them. Example: Finance (Loan Processing)

For more information, take a look at how Egnyte addressed Semperian's file services requirements.
Check out the Semperian case study

Leading Finance Firms Love Egnyte

Nasdaq · SEMPERIAN · NFP · Lincoln Financial Group · TRIUMPH



READY TO GET STARTED?

Start a free trial online, or contact our sales team today.

15-DAY FREE TRIAL

1-877-734-6983

EGNYTE | Smart Content Collaboration & Governance

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.

CONTACT US

+1-650-968-4018

1350 W. Middlefield Rd,
Mountain View, CA 94043,
USA

www.egnyte.com