Enterprise-Level Concerns

Examine a few of the enterprise-level features that IT departments and administrators will look for in a file-sharing service.

Some file-sharing services make the grade at a consumer level, but don't offer the kinds of features that make a system workable for enterprise. An enterprise-level service should be able to balance its efficiency – a primary user concern – with the needs of a company's IT department.

An enterprise-level service will allow a centralized IT department robust security measures, especially within regulated industries like finance or healthcare. A good service will make allowances for these industries, the compliance issues they may face and their unique workflow needs.

Enterprise-level services should also be flexible and scalable. Enterprise IT is responsible for highly sensitive corporate data, across multiple platforms, sometimes all around the globe. A file-sharing service must work across many systems and devices for hundreds or thousands of users, and it must be able to handle fluctuating user populations and needs.

A workable system will allow IT to delegate administrative functions to other groups or departments. In a company of, say, five thousand people, delegating control of individual files or individual users is crucial. An IT team may need to track the creative department's bandwidth, for instance. But if creative is overusing its allowance, it's up to the department administrators to figure out that John is streaming Netflix in his spare time.

Let's examine a few of the enterprise-level features that IT departments and administrators will look for in a file-sharing service.[1]

Security

This is vital: a good file-sharing service needs to protect your information at all times. Your data should be protected while at rest on a cloud server, during transfer, and while stored on devices (on-device). Check the licensing of your service and make sure it's accredited, preferably by a trusted Data Privacy Management (DPM) company. Your service should use safeguards recognized throughout the industry, employed by government and recommended by trusted organizations like the National Institute of Standards and Technology (NIST).

Here are some specifics guidelines by which to judge a service's security measures:

Security at rest[2]

128-bit and 256-bit AES encryption

Your service should employ no less than 128-bit, and usually 256-bit, Advanced Encryption Standard (AES) encryption to protect data on its servers. 256-bit AES is an encryption algorithm developed by the NIST in 2001. It has been adopted by the U.S. government and is used worldwide. This kind of encryption depends on a key, or code, without which information is not readable to the user. 256-bit refers to the size of this key: someone would have to come up with 256 bits of information, in the right order, to decrypt and read your document. 256-bit AES is considered an advanced form of encryption.

Virus scans, malware scans and firewalls

Just like your own computers and servers, your cloud servers should be checked out by daily virus and malware scans. They should employ regularly updated firewalls to keep your data secure at all times.

Security during transfer

SSL and TLS

NIST standards recommend that your information be transferred via protocols called Secure Socket Layer (SSL) and Transport Layer Security (TLS). These protocols establish an encrypted link between server and client so that vulnerable information is not transmitted in plain text form.

Enterprise-level systems will allow you options about who controls the keys to encrypt your information. Some IT departments may require a managed environment in which the department itself controls the keys, and your service should be able to accommodate this need.

Email

When you email documents through the cloud, you're not emailing attachments. You're sending a secure link to a document via email. You should be able to set your security requirements for this link. You may choose to allow any user with the link to open straight to the document, or you may require users to input a password before accessing it.

Security on-device

Your data is secure while it's on cloud servers, and you can be confident that it's transferred both to and from servers using an encrypted connection. But what happens to your data once it's downloaded to a device like a smartphone or a tablet? After all, these devices are physically vulnerable — they can be lost or stolen, leaving your data available to anyone who happens along. How should a service account for this vulnerability?

Encryption

Data on your mobile device should be encrypted, just like data at rest on servers.

Remote wipe

Check your system for a remote wipe feature. If your device disappears, you should be able to sign in to the cloud and activate a program that deletes all your files from your device's storage, instantly. Voila — secured data!

Other features

Your file-sharing service may offer a number of other on-device security features: you could set files stored on your device to self-destruct after a given period of time, limit access to your files by applications other than your cloud app, or block your files from access without the re-entry of a unique PIN or password. In general, the more of these security features your service offers, the better it will be for enterprise.

Audits

Enterprise-level file-sharing services should be tested and verified by authoritative sources every single year. Anything less than adherence to industry-wide standards does not fully protect your data.

Your clients and vendors have a vested interest in your data security — you want to be approved by organizations they recognize. Also, make sure that your system is accredited via standards approved by the U.S. government.

Your file-sharing service may receive several different kinds of certifications; many organizations out there offer security audits. Look for some of the most well known of them, like SSAE 16 certificates and ISO certificates.

SSAE 16[3]

Statement on Standards for Attestation Engagements (SSAE) audits are conducted by accredited public accounting firms that are certified to do so by the American Institute of Certified Public Accountants (AICPA). They ensure that service organizations like file-sharing services effectively protect information by maintaining good standards for security, clearly communicating those standards to employees, ensuring the physical integrity of their servers and premises, assessing and accounting for potential risks, and performing a variety of other functions that, in combination, protect your data as thoroughly as possible.

Why are these security audits conducted by accounting firms? Because they were originally designed to ensure the security of financial data, some of the most sensitive information out there. Under an SSAE certification, data of any description and from any industry is safeguarded by the same advanced measures to which the protection of financial data must adhere.

There are three kinds of certifications available under SSAE 16 standards: Security Organization Certificates (SOC) 1, 2 and 3. Your service should retain one of these certifications annually.

ISO[4]

The International Organization for Standardization (ISO) is an international body dedicated to providing specifications and guidelines to be sure that materials, products, processes and services work correctly. It has 166 member countries. Millions of people rely on ISO as a standards authority.

ISO offers several types of certifications, including ISO 27001, its standard for information security. An ISO 27001 certification ensures that an organization can manage sensitive information like financial data, intellectual property or private employee details. Find out whether the file-sharing service you're considering maintains an ISO certification, and, if so, which one.

Compliance

Security is particularly important in regulated industries. These industries — the healthcare and finance sectors, for instance — work with highly sensitive data, and they must comply with federal rules about the security, storage and transmission of that data. Companies can be legally liable if they are found to be negligent in their regulatory compliance, and the results can be catastrophic to both the companies and their customers.

Because of this, companies in regulated industries tend to maintain their own internal file-sharing systems as well as a cloud-based system. At the consumer level, the cloud just doesn't offer them enough protection. As cloud-based technologies advance, however, this kind of separation may not be necessary.

Examine your file-sharing service for its specialized security capabilities. Can it provide archiving features? How about dedicated, private storage? Does it advertise support of federal compliance standards? Look for compliance with major regulatory standards, including:

HIPAA10[5]

Under the Health Information Portability and Accountability Act (HIPAA), any company that deals with Protected Health Information (PHI) must comply with stringent data storage and security standards. These companies could include businesses as diverse as:

- Doctors and hospitals
- Lab facilities
- Printing companies
- Medical equipment suppliers
- Insurance agencies

Basically, anyone who could possibly have access to PHI needs to be HIPAA compliant. Your file-sharing service should support this compliance.

HIPAA includes rules about the physical storage of servers, physical building access, emergency procedures, auditing and — here's the important one when it comes to the cloud — data security. Most people know this. What's less well known is that as of 2013, HIPAA has been updated with new regulations: the Omnibus Rule. This update simply makes compliance standards more stringent. Any file-sharing service you choose should have updated its architecture to keep up with the changing law.

SEC[6]

The Security and Exchange Commission (SEC) is a government organization that aims to protect investors and to regulate fair marketplace practices. The financial health of millions of Americans, and of the country itself, rides on the securities industry. That's why the consequences of financial data security breaches have been so catastrophic in recent years.

Anyone in this industry, from credit rating agencies to stockbrokers, has to adhere to SEC standards in the protection of financial data. They also must be able to produce this data for SEC auditing, sometimes years after the fact. Files and folders, email messages, download notifications — all this information may need to be available to the SEC. So a company in the financial industry must be able to archive it.6

To be useful to these companies, a file-sharing service will be able to accommodate their archiving needs. IT departments should be able to specify the amount of time for which data should be archived, and at a minimum, that amount of time should be several years.

FINRA[7]

The Financial Industry Regulatory Authority (FINRA) is an independent regulator for U.S. security firms. It performs a function similar to the SEC, but in the private sector. FINRA oversees brokerage firms and registered security representatives, as well as entities that provide training, testing or other services within the securities industry.

If your company is SEC compliant, you'll also want to be FINRA compliant. A file-sharing service's archiving feature should help.

Authentication and Compatibility[8]

Your file-sharing service won't be of much use to your company if it isn't compatible with the platforms you employ on a daily basis. In order to be compatible with various platforms in an efficient way, your service must support different authentication procedures.

Authentication is the means by which a system verifies that you are you, and that you have permission to use the system. The authentication field is wide and varied; your file-sharing service should support the most common methods. These include single sign-on (SSO), a process by which your credentials are authenticated for use across different platforms. SSO can be supported by other authentication procedures, such as token-based authentication and multi-factor authentication.

Your file-sharing service should also support standard file access protocols, both traditional protocols like FTP and newer ones like WebDAV.

SSO

Single sign-on (SSO) allows one company to employ the authentication protocol of another company, so a user only has to sign in once.

Single sign-on requires a database in which your authenticating information is stored. Other platforms are able to verify your identity by checking with this database. One common example is corporate directories, databases that centralize employees' files and permissions. When users log in to the corporate network, their authentication and permissions extend from the directory to their file-sharing service.

Why is SSO important? In part because it creates a simpler user experience, and in part because it increases efficiency. People don't like to sign on to multiple accounts when they could do so once. Also, by re-using the corporate directory for additional services, your IT department saves time and avoids costly mistakes by keeping both services in sync.

LDAP[9]

The Lightweight Directory Access Protocol (LDAP) is a generic database structure that employs a hierarchical model. Any given piece of information can have an entire sub-database inside of it. For instance, a list of employees may contain, for each employee, other information: a social security number, department and email address, perhaps.

LDAP and databases like it are commonly used in corporate directories to store user names, groups, permissions, passwords and other identifying information. Because of this, they are a part of authentication protocols. When you sign on to a platform, it checks your credentials against the information in the database.

By integrating with LDAP, your file-sharing service can allow corporate users to access files in the cloud via single sign-on after they are authenticated with the corporate directory. It's also important that your service support LDAP because this protocol is employed by other common products, the most well known of which is Microsoft® Active Directory® (AD).

AD[10]

Microsoft® Active Directory® (AD) is one of the most common corporate directory systems out there, especially for large companies with thousands of employees. An enterprise-level file-sharing service should synchronize with AD to enable single sign-on.

Say you log on to your computer in the morning and, through single sign-on, your username and password are verified with AD. Now your corporate network knows that you're you, and that you're allowed to be there. You can access network files. It would be useful to be able to access your cloud files at the same time, via the single sign-on process. If your service doesn't support AD, however, there's no viable way for your IT department to extend your identifying information and permissions to the cloud.

SAML[11]

Security Assertion Markup Language (SAML) is employed by Microsoft® Active Directory® (AD) and other platforms to enable single sign-on. A markup language is a structured way by which platforms can communicate with each other. Many people recognize one of the most common markup languages: the HyperText Markup Language, or HTML. Instructions about how to place graphics in a browser window might be communicated in HTML.

In the case of SAML, the function of the language is to enforce security policies. It facilitates communication between the two platforms that are authenticating your identity. A file-sharing service should integrate with SAML for the same reason it should integrate with AD: it's a common protocol in SSO procedures.

OAuth[12]

Token-based authentication procedures are also common. One of the most common of these systems is called Open Authorization (OAuth). In OAuth, tokens, or small packets of data, are exchanged between systems in order to prove a user's identity. It's just like handing over a driver's license in order to open a bank account or purchase alcohol.

Here's an example: Mary wants to view photo albums on 500px. Mary isn't a user of 500px, but is a user of Facebook. 500px employs a token-based authentication system, so Mary can authenticate herself via Facebook, get a token verifying her authorization, and sign in to 500px with that token. To Mary, it looks like she's signed in to 500px using her Facebook account.

OAuth is supported by websites you know well — TumblrTM and Google, for instance. It's also used on industry-specific platforms like Salesforce,® a vital service in the sales industry. If your file-sharing service doesn't support OAuth and other token-based authentication systems, you may not be able to integrate easily with third-party applications that are important to you.

Multi-factor authentication[13]

Although multi-factor authentication is not a protocol, it's an authentication procedure that supports SSO, and it's important for the security of your file-sharing system. Multi-factor authentication requires you to provide proof of your identity via two or more types of sources:

- Something you know (like a password)
- Something you have (like a mobile phone)
- Something you are (like a fingerprint)

For instance, you could configure your file-sharing account such that the system texts you after you type in your account password online. It would then require you to enter the information in the SMS before being fully authenticated.

Multi-factor authentication is a more secure method of verifying your identity. In the case above, for instance, someone would have to both know your password and be in physical possession of your phone in order to access your account.

File access protocols

FTP

Are you really wedded to your File Transfer Protocol (FTP) site? Are your clients? FTP is very common in the enterprise, and your file-sharing service needs to accommodate it. Your service should be compatible with FTP and other traditional file access protocols. Make sure you can also use FTP over TLS or SSL for a secure connection.

API[14]

An API lets two pieces of software, like a file-sharing service and a third-party application, communicate with each other. Your file-sharing system's API allows your development team to link your service to another application. In order for this to work, both your file-sharing service and the application must offer APIs.

In other words, even if your file-sharing service itself doesn't interface with a specific third-party application, your team can write an

adaptor that translates between the two. Think of APIs like doorways through which your service and another piece of software can stand and talk to each other.

For instance, say you're a dentist's office that uses Customer Relationship Management (CRM) software to keep track of your patient database. Your file-sharing service's API would allow the service to work with your particular CRM so that when you updated a record on your end, it would also update in the cloud. This feature helps support your unique workflow and helps you tailor file sharing to your industry.

WebDAV

Web Distributed Authoring and Versioning (WebDAV) is an extension of the Hypertext Transfer Protocol (HTTP) that allows you to change, rather than just read, documents and files on the World Wide Web. Integrating with WebDAV lets you use files in the cloud as if they were on your local computer. For instance, WebDAV could allow you to open and edit the latest draft of a white paper saved in your file-sharing service without downloading it first. To you, it will look like you're editing the paper within Microsoft Word (or another word processing program.) To the computer, you're simply changing a file directly on the Internet.

Common applications like Windows® Explorer, Mac Finder and Microsoft Office enable WebDAV. To work with them, a file-sharing service must support WebDAV, as well.

Scalability

When you multiply gigabytes of data by hundreds or thousands of users, perhaps globally, you have scalability issues. IT departments need to meet the high data demands of enterprise-level companies and keep up with increasing strain on their systems as those companies grow. File-sharing services must help them meet this need by providing flexible scalability. Look for these traits in an easily scalable file-sharing service:

- Large file-size, preferably 100 GB or more for a single file
- Multiple devices per user
- High bandwidth
- Unlimited file storage
- Easy licensing and purchasing adjustments as your company grows

Administrative Functions

An IT department can't maintain solid security policies if its file-sharing service doesn't offer thorough administrative control. IT must be able to manage data in the cloud just as well as it does on its own servers.

IT administrators need control over major functions like auditing, user permissions and a host of other administrative tasks.

Audit trails

Data on a file-sharing service needs to be tracked at the highest level. A file-sharing service should allow thorough audit trails to help an IT department maintain its administrative responsibilities over data and users. Think of it like accounting — just like your accountant needs to be able to follow your money, administrators need to be able to follow the actions of a system's users.

A file-sharing service should let you create flexible audit trails that include information like:

- Who accessed what data, and when
- The source (IP address) of the request
- Bandwidth usage by department

- Which folders store which types of data

User and group permissions

Administrators should be able to create user groups based on a wide variety of characteristics, like department or job role, and give them separate permissions. (The creative department doesn't need to see accounting's books; engineers should access different data than copywriters.) They also need to tailor groups to unique security specifications. For instance, administrators might have to create groups based on location because Building A is accredited for better data security than Building B.

Other major functions

Administrators will perform a variety of tasks, and your file-sharing service should allow them to do so with great flexibility. Important actions include:

- Adding users and groups
- Managing the directory structure
- Enforcing password expiration dates
- Specifying bandwidth quotas by group or department
- Creating other departmental administrators

Administrative Delegation

One other major administrative function is the creation of other administrators. Think of administration like a tree. IT administrators have their job — they're the trunk, and they secure and track data at a company-wide level. But they also need to be able to create user administrators (let's go with the metaphor and call them branches), and then delegate functions to them. Robust administrative controls act as a layer of security at the departmental level. Important controls include auditing, monitoring bandwidth and quotas and controlling file and folder permissions.

Audits

Just as IT departments track information at the company-wide level, other administrators should be able to do so at a departmental level. A service should allow internal audits of a document's history. Need to assess who made the last changes to your latest new-client pitch? You should be able to do so. Want to determine whether your employees are working at capacity? Ditto.

Quotas

Administrators need to be able to assign bandwidth quotas and allowances to users, and they need the authority to enforce these limits. A creative department manager is in the best position to decide whether the videographer or the graphic designer gets more bandwidth, or which team is allowed to change draft copy. These are user-level concerns that should be under departmental administrators' purview.

File Permissions

Administrators also need to be able to create relationships between files and users — who has permission to do what to any given file. These permissions fall into three categories: reading, writing (creating or modifying) and deleting.

What if you're a TA, and you need your students to be able to read, but not modify, a syllabus? You need to be able to set file permissions accordingly. What if you're an attorney, and you want your administrative assistant to delete folders after a certain date without reading their contents? Same goes.

When you're evaluating the administrative functions of a file-sharing service, ask yourself

whether the administrator can specify who has the ability to:

- Create files
- Move files
- Rename files
- Delete files
- Modify files
- Append files

Individual file and folder properties

Department administrators are also responsible for individual file and folders. A file-sharing service should offer features that give them granular control. It should enable them to assign a range of properties to individual files.

These properties could include:

- Expiration dates
- Version control
- Change notifications

Features like these will determine whether a file-sharing service can be of use to your company. Look for a system that gives you as much flexibility, security, and control as possible.

Works Referenced

[1]Gould, S. A Win-Win for IT Professionals. (White paper) Citrix ShareFile: https://sharefilemarketing.sharefile.com/download.aspx?id=sb3b77fc5abe4cca9#, accessed 01/09/2015.

[2]Rouse, Margaret. "Advanced Encryption Standard (AES)." TechTarget: November, 2014. http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard, accessed 01/09/15.

[3]http://ssae16.com, accessed 01/09/15.

[4]http://www.iso.org/iso/home.html, accessed 01/09/15.

[5]Kepes, Ben. "Citrix ShareFile for Healthcare, Delivering To-the-edge Cases." Forbes.com: November 12th, 2013. http://www.forbes.com/sites/benkepes/2013/11/12/citrix-sharefile-for-healthcare-delivering-to-the-edge-cases/, accessed 01/09/15.

[6]http://www.sec.gov, accessed 01/09/15.

[7] http://www.finra.org, accessed 01/09/15.

[8]"Single Sign-On." AuthenticationWorld.com. Huntington Ventures, Ltd.: 2006. http://www.authenticationworld.com/Single-Sign-On-Authentication/index.html, accessed 01/09/15.

[9]"SSO and LDAP Authentication." AuthenticationWorld.com. Huntington Ventures, Ltd.: 2006. http://www.authenticationworld.com/Single-Sign-On-Authentication/index.html, accessed 01/09/15.

[10]"So What Is Active Directory?" Microsoft: MSDN Library, 2015. http://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx, accessed 01/09/15.

[11]"Markup Language Definition." The Linux Information Project, 2006. http://www.linfo.org/markup_language.html, accessed 01/09/15.

[12]Gordon, Whitson. "Understand OAuth: What Happens When You Log Into a Site with Google, Twitter or Facebook." Lifehacker: June 13th, 2012. http://lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook, accessed 01/09/15.

[13]Rouse, Margaret. "MultiFactor Authentication (MFA)." TechTarget: June, 2014. http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA, accessed 01/09/15.

[14]Citrix ShareFile. "API Reference." http://api.sharefile.com/rest/. 01/09/15.

[15]Whitehead, Jim. "DAV Frequently Asked Questions." April 21st, 2010. http://www.webdav.org/other/faq.html. Accessed 01/09/15.

CITRIX®

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud services to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.