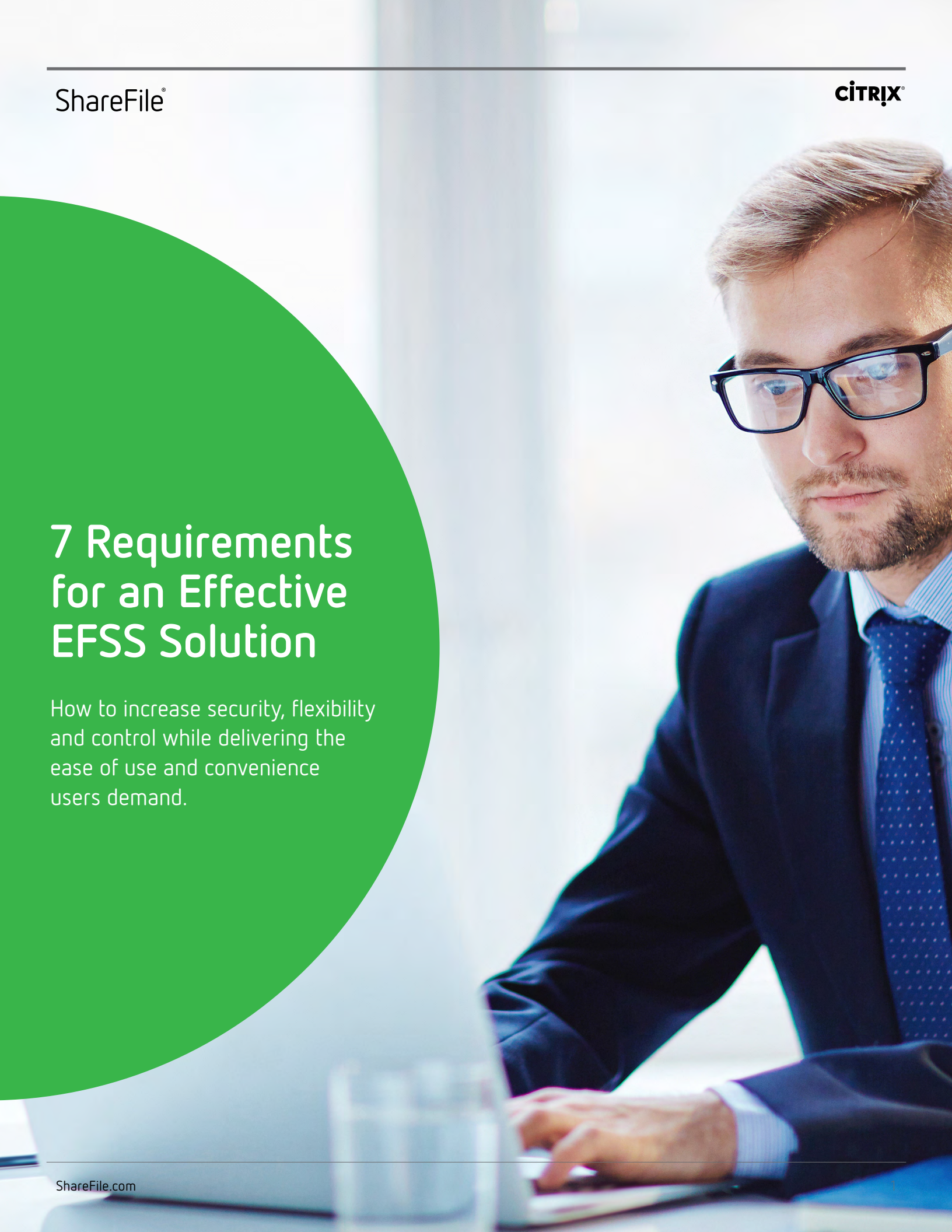

7 Requirements for an Effective EFSS Solution

How to increase security, flexibility and control while delivering the ease of use and convenience users demand.

Some of the biggest challenges IT teams face today stem from data loss and security risks arising from the unauthorized use of personal file-sharing services by employees for business purposes.

Personal file-sharing services invite data leakage and compliance violations by allowing files being shared to escape beyond the visibility and control of IT. At the same time, these services meet the essential need of today's mobile workforce to be able to access and share data wherever people work. The only way for IT to stop the spread of uncontrolled data sharing, is to address this need through an IT-approved application that meets employees' needs better than any consumer service could.

A true enterprise file sync and sharing (EFSS) service combines the convenience and simplicity of a personal file-sharing service with enterprise-oriented features to increase productivity for users—as well as increase security, flexibility and control for IT. With the risks associated with personal file-sharing usage in the enterprise, it's critical to understand the requirements for a truly effective EFSS solution. Simply blocking network access of personal file-sharing services is no longer a viable option. Businesses must deploy an EFSS solution, as these tools have become an integral part of an employee's daily work efforts.

The risks posed by personal file-sharing services in the enterprise

Employees seek out and use personal file sharing services not out of malice, but to meet legitimate needs to share files for business purposes. These personal services typically provided only limited functionality and lack built-in security, but with free storage, quick installation and a simple user experience, they can seem like a good-enough solution—especially for employees who are unaware of the IT-approved solutions that might be available in the organization. Once the employee signs up for the personal account, the problems begin. As files are shared, business data is stored outside the control of IT, potentially exposing the organization to data leakage and breaches. Consumer-grade services also lack granular file control and many compliance certifications, putting organizations at risk of compliance violations in regulated industries such as healthcare and financial services. Beyond the potential loss of confidential or proprietary information, personal file sharing services can open the network to malware, hacking and other malicious activity. Problems like these are often compounded by embarrassment and damage to the company's brand and reputation.

When an employee stores corporate data in a personal file sharing account and shares files with third parties, IT has no visibility into the types of data stored there and whether any sensitive corporate data is leaving the building. If that employee leaves the company, all the corporate data synced from their corporate desktop or laptop to their personal file sharing account can remain indefinitely accessible from any personally owned devices they may use, creating unacceptable security, legal and business risks for the organization. The personal file sharing problem is both serious and pervasive. According to an Enterprise Strategy Group report, a vast majority (70 percent) of organizations know or suspect their employees are using personal online file sharing accounts without formal IT approval. This is a significant problem for IT organizations

Problems beyond security

In addition to the security issues they raise, personal file sharing services simply fail to meet the full range of enterprise requirements, making them unsuitable for business use even with the full awareness of IT. From a user perspective, these services lack the business-oriented features people need to be fully productive, such as integrations with other enterprise mobile apps to streamline common tasks and workflows. They're also unable to provide access to files in many locations inside the network such as Microsoft SharePoint repositories, ECM systems and network file shares.

Personal file-sharing services also lack the tools IT needs for administration, control and visibility. IT has no way to monitor, manage or report on how data is accessed, stored and shared, and is unable to leverage audit trails for compliance purposes. With no flexible storage options, IT can't control where data resides in order to meet requirements for performance, cost and data sovereignty. With no advanced security and administrative functionality, IT can't address crucial use cases such as employee turnover to ensure that business data does not remain in personal file sharing accounts belonging to departed employees.

As a foundational element of business productivity, file sync and sharing is too important to be left to consumer-grade tools that were never designed with enterprise requirements in mind. IT needs an enterprise file sync and sharing (EFSS) solution built from the ground up explicitly to meet the needs of business professionals, IT organizations, and enterprises.

With these things in mind, consider the following features and functions non-negotiable when selecting the right EFSS solution:

Requirements for a true EFSS solution

1. A great experience for users

In this era of consumerization and shadow IT, user acceptance is the first test for any enterprise service. If a file sync and sharing solution fails to meet peoples' expectations for robust functionality and a great user experience, they simply won't adopt it, and the problems will go unsolved.

To satisfy users, an EFSS solution must provide consumer-like convenience and simplicity to equal or exceed a freemium option. The solution must make it easy to sync and share data from any device securely, and to share data inside or outside the organization regardless of file size or network location. To achieve full mobile productivity, the solution should provide integrated apps like a built-in content editor that lets them accomplish more within the same seamless environment. Similarly, the solution should enable integrated workflows across tools like Microsoft Outlook to streamline common tasks and reduce clicks. Secure offline access and editing are essential to ensure uninterrupted productivity for on-the-go users.

2. Granular security and access control

Effective security is central to the value of an EFSS solution for IT, making it possible to reduce the risk of information leakage and provide protection from disasters. The solution should provide capabilities including:

- Granular access control, secure authentication protocols and authorization policies to allow the right level of access for each user, in each scenario.
- Advanced security features and policies including remote wipe, device lock, passcode protection, white/black listings and data expiration policies to ensure that the data people access, including on mobile devices, remains secure and under IT control.
- Robust real-time tracking and auditing of user activity, with the ability to create custom reports to meet corporate data policies and compliance requirements.
- Seamless integration with enterprise directory services to simplify authentication and user provisioning.
- Controls over data sharing inside and outside the organization, including the ability to require a login with defined password complexity for each user account, restrict the number of downloads available to a given user, restrict upload and download permissions for users added to team folders, expire links to files, and restrict access based on network location.

3. Mobility for all enterprise data

Consumer-grade personal file sharing services are typically limited in the network locations they can access, often leaving the most important files beyond the reach of users outside the corporate network. Some organizations try to work around this by migrating data to a more easily accessible location, but the drawbacks of this approach in terms of efficiency and scalability are obvious. An EFSS should provide access to corporate data wherever it resides—including existing network file drives, SharePoint, OneDrive for Business and enterprise content management systems—even from outside the network, allowing a single point of access to all data sources.

4. Flexible data storage options

Different types of business information need to be stored in different places. Some files need to be kept onsite or in a specific geography to meet compliance requirements, while others can be stored in the cloud to simplify management, reduce cost and allow frictionless scalability. For some types of data and apps, the location of data storage can make a significant difference in performance. IT needs the flexibility to choose where data is stored—including both on-premises and cloud options, or a combination of locations—through the same service.

5. Integration with existing infrastructure
To simplify setup and administration, a true EFSS solution should integrate with existing IT infrastructure, such as connecting with Active Directory via SAML tools including ADFS, Ping, CA and Salesforce.com. This makes it easier to implement and manage policies over who can access what in certain scenarios.

6. Integration with enterprise mobility management across all types of devices
People often think of file sync and sharing in terms of mobile devices, but this is only part of the picture. To be productive anywhere, in any scenario people need to be able to access the same EFSS functionality on any device they use—not just tablets and smartphones, but also laptops, desktop computers and thin clients. This any-device access should be managed through an integrated enterprise mobility management (EMM) solution that lets IT implement and enforce access and security policies consistently through a single point of administration no matter how people access the service.

For users on mobile devices, the EFSS solution should be able to leverage essential EMM capabilities such as mobile device management (MDM) to ensure that data remains safe even if a device is lost or stolen, and mobile application management (MAM) to isolate corporate apps and data from any personal apps that may be on the device.

7. Align with corporate goals and initiatives
Finally, a best-in-class solution will provide additional business benefits by helping IT:

- **Support BYOD, CYOD and COPE programs**, making it easy for people to access and share data securely on any device they use, no matter who owns it.
- **Enable corporate mobility initiatives** by mobilizing the full range of corporate data and providing EFSS as part of a complete, integrated solution to manage mobile apps, data and devices.
- **Enhance data sharing** to put corporate data to work more effectively for the business.
- **Improve collaboration** by making it simple for team members to share and create information with colleagues, partners and customers.
- **Increase productivity** by making it possible for people get more done, in more scenarios, with convenient access to all the files their work involves.

Next steps

The unauthorized use of personal file-sharing services poses immediate and serious risks for organizations of all kinds. To prevent leakage and protect corporate data, IT needs to deliver a true EFSS service that combines the security, flexibility and control that IT needs with the convenience and productivity features users demand.

Visit ShareFile.com for additional information about the ways EFSS solutions can exceed employee needs while securing and mobilizing business data.

CITRIX®

ShareFile
North America | 1 800 441 3453
Worldwide | +1 919 745 6111
United Kingdom | +44 800 680 0621
Australia | +1 800 089 572

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States