



FSS Buyer's Guide

Why a File Sync & Sharing Solution is Critical for Your Business

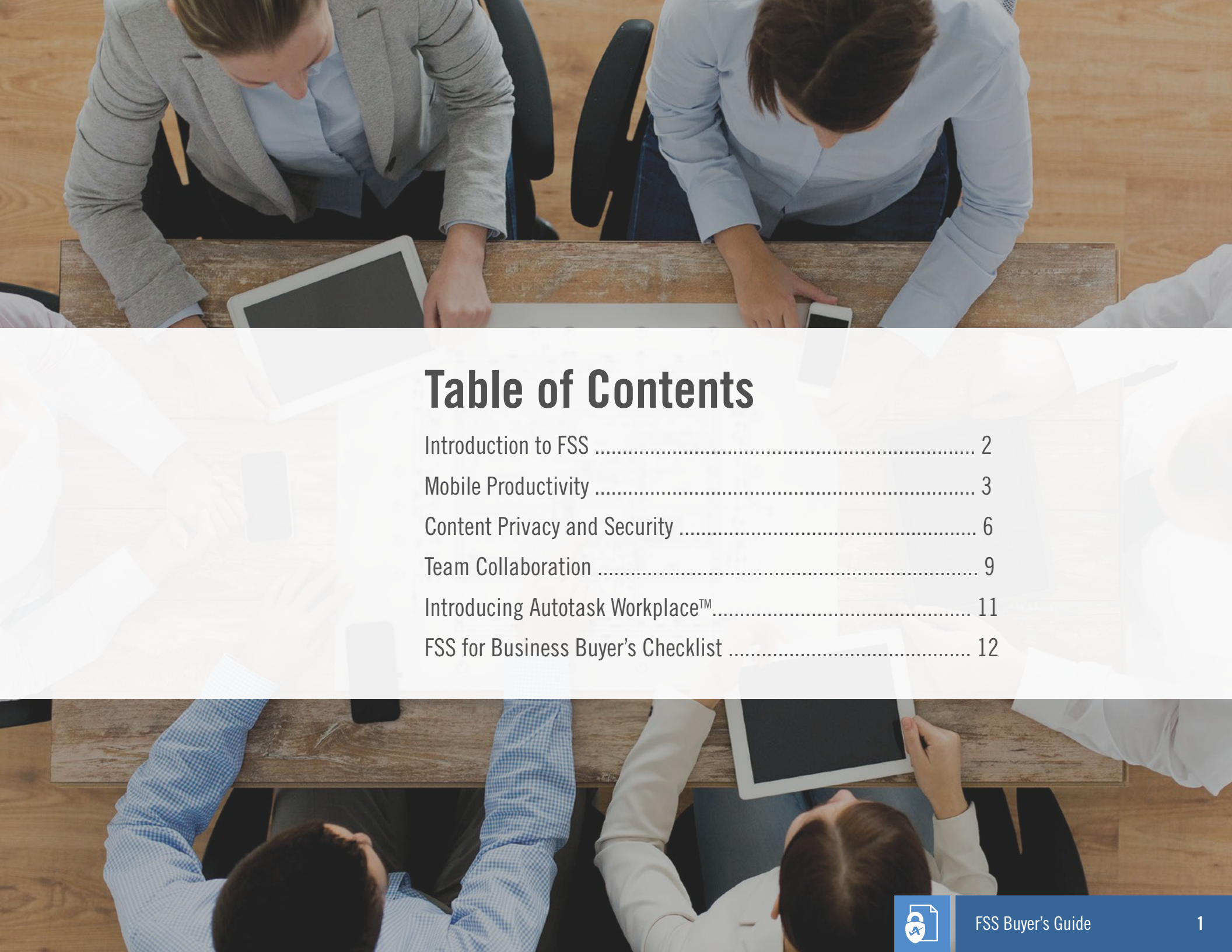
An overhead photograph of four business professionals (two men and two women) sitting around a large wooden table. They are all looking down at their devices, which include tablets and smartphones. The setting appears to be a modern office or meeting room with a light-colored wooden floor.

Table of Contents

Introduction to FSS	2
Mobile Productivity	3
Content Privacy and Security	6
Team Collaboration	9
Introducing Autotask Workplace™.....	11
FSS for Business Buyer's Checklist	12

Introduction to FSS

Mobile sharing of files is increasingly commonplace. In fact, much to the chagrin of those who provide IT support, mobile workers frequently use unmanaged consumer file sharing solutions to meet their business needs. These solutions put business data at significant risk. In a recent GigaOm study, 84% of IT professionals report security problems caused by consumer File Synchronization and Sharing (FSS) services used for company business. Yet without access to a company-approved file sharing solution,

employees will continue to turn to other sources to meet their file sync and share requirements.

You can assure the security, control and compliance that will protect your vital business information, while achieving the mobile productivity needs of your workforce. **This guide provides a closer look at the top features you need to consider when selecting a secure file sync and sharing solution that is designed specifically for mobile business collaboration.**

84%

of IT professionals report security problems caused by consumer File Sync and Sharing services used for company business

Source: GigaOm Research and Harris Interactive study, June 2014



Mobile Productivity

Introduction

With mobile use increasing and access to viral networks the new norm, the sheer amount of digital information employees want to access and share across multiple mobile devices is growing dramatically.

Workers in all types of organizations, whether mobile or onsite, now expect complete flexibility in which device they choose to use and seamless access and transfer of documents between colleagues and partners, regardless of the device their external contacts may be using.

Your organization needs complete control of those devices and how your users are using them to protect your corporate data from security risks. To ensure you maximize productivity while keeping information secure and accessible, you need a File Sync & Sharing Solution that includes the features listed in the following checklists.

**Sales of FSS products
and services to grow
32% this year, to
\$1.67 billion**

Source: IDC



Mobile Productivity Checklist

1 of 2



☒ Support for Multiple Devices

When you need to share content fast, you don't want to be constrained by the device type you can use. Select a solution that supports all the devices your employees use so that they are never restricted.



☒ Smart Sync Capabilities

Choose a solution that has the ability to replicate desktop file structures on a folder or sub-folder basis. This ensures access to all-important documents while on the road.



☒ Cross-Device Collaboration and Editing

A solution should deliver the ability to edit, annotate and lock content on any device, without the need for third-party mobile applications. Solutions that enable integrated file editing on tablets and mobile phones are ideal.



☒ On and Offline Access

Assure that synced content is fully accessible when the device is out-of-network or offline. This includes being able to manipulate documents (e.g., edit, share, etc.) and not simply view them while offline.

Mobile Productivity Checklist

2 of 2



☒ **Version Control**

A business-grade file sharing service should have built-in file versioning. This eliminates risks of losing important files or changes. With versioning, files can be instantly recovered, viewed, and restored to their original location, either one file at a time or the entire folder. Look for a service with the option to request custom versioning limits that extend beyond 6 months as versions should be stored for at least 6 months.



☒ **Automated Document QR Coding**

For simplified document search and retrieval on the go, select a solution that provides automated quick response (QR) coding for each document. This will save time when searching for content later.



☒ **Secure Sharing without Forced Registration**

For the best flexibility, select a solution that doesn't force recipients to adopt the same file sharing service as the person sending the document.



☒ **Scan to PDF for Instant Field Image and Document Capture**

When working in the field, workers should be able to easily capture document markups and photos into PDF files for direct mobile device sharing.



Content Privacy and Security

Introduction

With the right secure file sharing solution, you can protect employees from risky behaviors without slowing their productivity. **The FSS solution you choose must have certain capabilities to prevent putting your data at risk.** Utilize the checklist on the following pages to determine whether the FSS solution you're considering has crucial privacy and security features like built-in remote wipe capabilities, two-factor authentication and more.

“If I’m going to both use and recommend a file sharing solution, I want it to be completely worry-free with all the security and control that delivers peace of mind.”

Chris Davis
CEO & COO, Polarverse



Content Privacy and Security Checklist

1 of 2



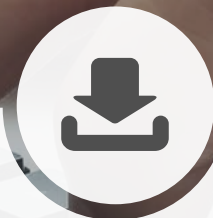
☒ Encryption In-session, In-transit, On-device

To protect your organization's data, select a file sharing solution that delivers 256-bit AES encryption for every point in your content's lifecycle – when it's being accessed in-session, while in-transit and while at rest, regardless of where it's being stored or what device it's on. Also be sure that unique and rotating encryption keys are used for each file.



☒ Policy-based Control of Content, Users & Devices

An enterprise-grade file sharing solution should deliver detailed – yet easy to use – policy controls where you specify settings for content, users and devices at the granularity you prefer.



☒ Download / Copy Prevent; Auto PDF

To protect document tampering, your file sharing service should have user defined download and copy prevention controls and the ability to auto-create view only PDFs when desired.



☒ Built-in Remote Wipe Capabilities

Ideal for environments where remote workers or consultants are given content access, built-in remote wipe capabilities that will delete content from selected devices when desired can safeguard content from getting into the wrong hands. This is also ideal to minimize risk in the event of device theft or loss.

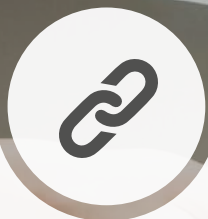
Content Privacy and Security Checklist

2 of 2



☒ Two-factor Authentication

For secure document access, assure that two-factor authentication protection is in place. It's important for you to know who is accessing information and where they're coming from.



☒ Share Content with Links

Eliminate the need to email files, and improve security with link sharing. Look for a solution with an array of customization options for public sharing including password protection, view or download permission, as well as auto-expire after a time period or access count.



☒ Inactivity Session Timers

Protect content from unwanted viewing with inactivity session timers for both mobile devices and computers.



☒ IP Address White Listing

Lock down endpoint access for different components of your cloud service like the browser, mobile app or desktop software. Access shouldn't be granted from anywhere, so look for a solution that restricts access to the cloud from certain IP addresses. This allows admins to accommodate a multitude of company locations while maintaining security.

Team Collaboration

Introduction

With the continued increase of BYOD and remote and mobile workforces, users need to work and collaborate efficiently, and IT support needs to securely manage the flood of user devices and content. In fact, by 2017, Gartner predicts half of employers will require employees to supply their own device for work purposes. When your organization deploys new services, integration with existing systems is critical. And more endpoints mean more contributed content from laptops, phones and tablets. Put to use the checklist on the next page to look for the capabilities that will empower your team to collaborate more efficiently and more securely.

**By 2017,
Gartner predicts half of
employers will require
employees to supply their
own device for work purposes.**

Source: <http://www.gartner.com/newsroom/id/2466615>





Team Collaboration Checklist

Systems Integration

It's important that a solution integrate with your existing systems and deployments like Active Directory for user and group management and authentication; SAML 2.0 for single sign-on; Salesforce and Outlook for simple document upload and attachment; and Office 365 and Google Docs for web editing and collaboration.

Real-time, Multi-Platform Sync

The beauty of the cloud is that your entire team can stay in sync. Arguably one of the most crucial components of a powerful file sharing solution is reliable and functional sync. Look for a solution that supports both Mac and Windows, as well as file servers. Always having access to the right content, whether online or off, improves team productivity and drives the business forward.

No File Size Limit

A file sharing solution shouldn't make you change how you work. Large presentations and graphic files need to be sent and sync seamlessly. Look for a solution with no file size limitations for syncing and backup.

Continuous Real-time Backup

Businesses must be prepared for computer crashes, loss or theft, and scheduled or manual backups are not sufficient. Look for a solution that provides backup of critical files and folders in the cloud for redundancy and restoration in the event of file loss or data corruption. Backup should operate continuously in the background, typically discovering modified files within seconds, and then initiating backup.

Cloud-enable Your File Server

Company employees, virtual teams and authorized parties can securely access the files they need, when and where they need them, and changes are automatically synced across the appropriated user devices and company file servers without intervention. As a result, everyone – including mobile workers and remote offices – has access to the most current versions of files, which are securely protected, retained and archived with greater efficiency and recoverability.





Fully Mobile and Secure File Sharing – Introducing Autotask Workplace™

Autotask Workplace is a complete, secure file sharing and collaboration solution that enables your team members to safely access, manage, organize and share files from any device, anywhere.

It enables productivity by allowing individuals or teams to work on any documents or digital content – from their device – in real time, without fear of security breaches. Autotask Workplace also gives employees built-in security controls that can be set up based on how they need to share information with team members.

- ✓ Mobile Productivity
- ✓ Content Privacy and Security
- ✓ Collaboration Features



150,000 businesses



134 countries



2 billion files managed



FSS for Business Buyer's Checklist

Any secure, built for business File Synchronization and Sharing solution should include the following characteristics. When evaluating file sync and sharing solution providers, utilize this checklist to ensure the solution you select can do the job.

Mobile Productivity

- ☐ Support for Multiple Devices
- ☐ Cross-Device Collaboration and Editing
- ☐ Smart Sync Capabilities
- ☐ On and Offline Access
- ☐ Version Control
- ☐ Secure Sharing without Forced Registration
- ☐ Scan to PDF for Instant Field Image and Document Capture
- ☐ Automated Document QR Coding

Content Privacy and Security

- ☐ Encryption In-session, In-transit, On-device
- ☐ Policy-based Control of Content, Users & Devices
- ☐ Download / Copy Prevent; Auto PDF
- ☐ Built-in Remote Wipe Capabilities
- ☐ Two-factor Authentication
- ☐ Share Content with Links
- ☐ Inactivity Session Timers
- ☐ IP Address White Listing

Team Collaboration

- ☐ Systems Integration
- ☐ Real-time, Multi-Platform Sync
- ☐ No File Size Limit
- ☐ Continuous Real-time Backup
- ☐ Cloud-enable Your File Server

