A File Sharing Buyer's Guide for Corporate IT

Select the Right Solution & Do Business Faster

Introduction

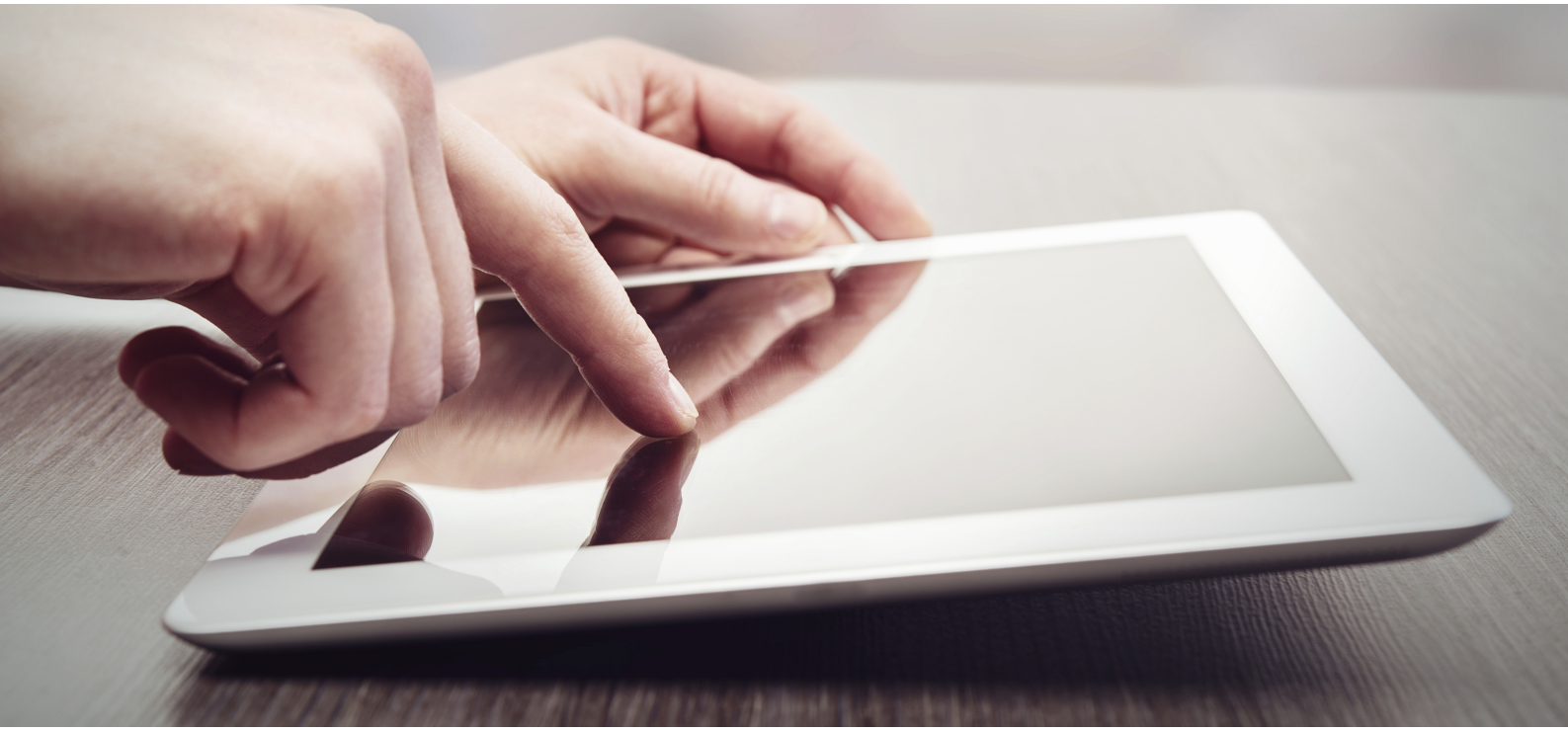
When it comes to file sharing, IT managers all have their nightmares about something going awry. It's a safe bet that the bad dream goes something like this: random end users using unsecured file sharing services to access and share sensitive company documents, especially on unprotected networks while on the road. And the real possibility that these documents get into the wrong hands.

In the business cloud environment – some 1.3 billion mobile workers by 2015 – mobile sharing of sensitive files is increasingly commonplace. In fact, much to the chagrin of IT teams, mobile workers frequently use consumer file sharing solutions to meet their collaboration needs. But these consumer solutions can put corporate data at significant risk. In fact, in a recent GigaOm study, 84% of IT professionals report security problems caused by consumer file sharing and sync services used for company business. Yet without access to an IT-approved file sharing solution, employees will continue to turn to other sources to meet their sync and share requirements.

Bottom line, file sharing solutions are here to stay. Today's workers will use them – in whatever form they can – to achieve their mobile productivity needs. Your best bet: give them what they need while also assuring the security, control and compliance that will protect your vital business information. In this buyer's guide we outline the top features you need to consider when selecting the secure, business-grade file sharing solution your business, and its users, requires.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr



Mobile Productivity

Incidents such as the one depicted above have greater probability as mobile use increases and viral networks are so accessible. Also, at the same time your company's workers, clients and partners are all using multiple mobile devices, the sheer amount of digital information they want to access and share is growing dramatically – estimated to grow by a factor of 300 between 2005 and 2020. Clearly, the complexity of maintaining this amount of data and file sharing securely is at an all-time level of demand, and stress!

Enterprise workers, whether mobile or onsite, now expect complete flexibility in which device they choose to use and a seamless transfer of documents between colleagues and partners, regardless of the device their external contacts may be using. IT needs complete control of those devices and how your users are using them to protect your corporate data from the risk of leakage.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr

Mobile Productivity

To help, select a file sharing solution that offers the following:

Support for Ubiquitous Devices
It may sound obvious, but 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.

Integrated Document Control on Devices
Solutions that deliver the ability to edit, annotate and lock content on any device will deliver the most mobile productivity. Be sure that this can be accomplished without the need for third-party mobile applications that may involve additional complexities or create a potential for data leakage. Ideal are those solutions that enable integrated file editing on tablets and mobile phones.

Smart Sync Capabilities
For full mobility, choose solutions that have 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. Furthermore, given different devices have varying on-device storage capacities, choose a solution that enables device aware sync in order to adapt to these limitations.

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 viewing them while offline.

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. Content should still be secure and available, regardless of whether recipients are "members" of the file sharing service used.

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.

Automated QR Coding for Document Accuracy and Access
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.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr

Content Privacy and Security

Most employees, partners and vendors don't properly consider the risks of file sharing security. And can you blame them? They're focused on closing deals, getting contracts signed, trading insights on data, planning the next product. But as you know, all of these aforementioned tasks are rife for security breaches. With a secure file sharing solution you can protect employees from risky behaviors without slowing their productivity.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr

Content Privacy and Security

Consider these privacy and security features. Without just one of them, you may be putting your data at risk.

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.

Dual-factor Authentication
For secure document access, assure that dual-factor authentication protection is in place. It's important who you know and where they're coming from.

Download / Copy Prevent; Auto PDF
To protect document tampering, your file sharing service should have user definable 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 the risk of leakage due to device theft or loss.

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.

Password and Time-to-Live Protection
Public links to all shared content – including projects, folders and files – should be controllable with password protection and time-to-live controls which can enable and disable content access at defined times.

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

Non-persistent Use of Credentials
Protect unwanted access with non-persistent credential use.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr


“84% of IT professionals report security problems caused by consumer file sharing and sync services used for company business.”
GigaOm Research and Harris Interactive study, June 2014

Enterprise-Ready

As an IT manager responsible for the smooth flow of data, you never want to hear networking glitches have resulted in costly downtime for your organization. The same holds true for file sharing: your solution of choice should ensure you that the employees and their external partners will not suffer the inefficiencies and inconvenience of downtime caused by service interruption, performance degradation or malware infections.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr

Enterprise-Ready

To assure that your secure file sharing solution is enterprise-ready, use one that offers the following credentials:

No-breach History
Look into the history of your file sharing provider. Ideally, it should have a history free of security breaches and downtime, or at a minimum has the proper safeguards to prevent them.

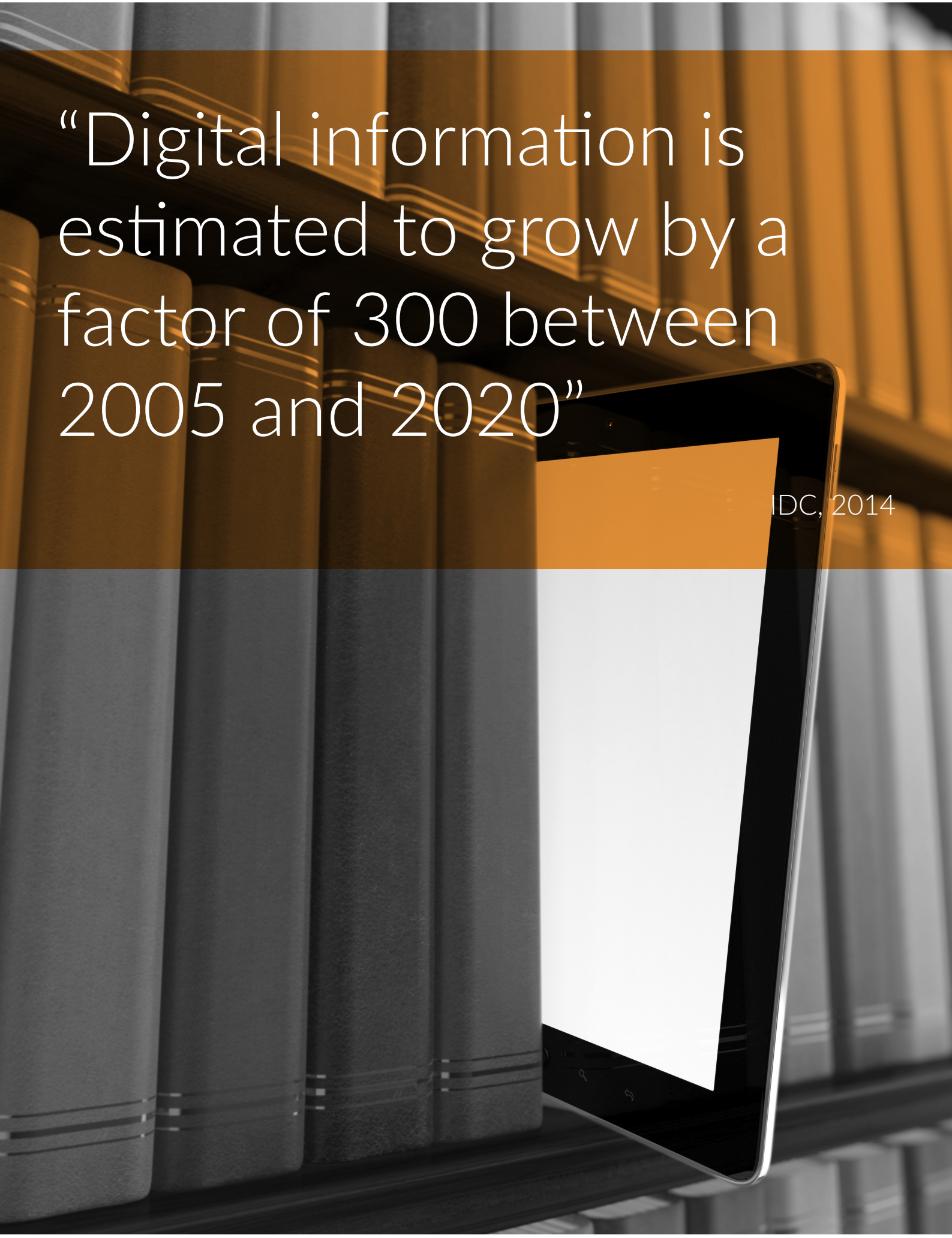
Geo-redundant, Regionally Segmented Data Centers
To reduce any possibility of experiencing service interruption, performance degradation or malware infections, select an online file sharing service that owns and operates geo-redundant data centers. For increased data privacy and control, it's also important that data centers are geographically located to ensure that your data remains within certain countries and regions while in storage and in transit.

Compliant and SSAE 16-audited
Look into your file sharing service's validation audits. The best have been validated by independent certified public accountants for SSAE 16 SOC2 Type 2 audit completion. This will assure that it offers exceptional operations in the areas of data protection, access controls, authentication mechanisms, audit trails, physical and logical security, software development, change control and other critical operational areas.

Administrator-controlled Access and Reporting
Ensure that the file sharing solution you choose also has granular policy controls and reporting so that you can generate and export audit records on all account activity, including projects, groups and mobile access. You should also have the enterprise policy management that allows for the administration of passwords, sessions, IP address whitelisting, public links, remote access and mobile devices for your entire team.

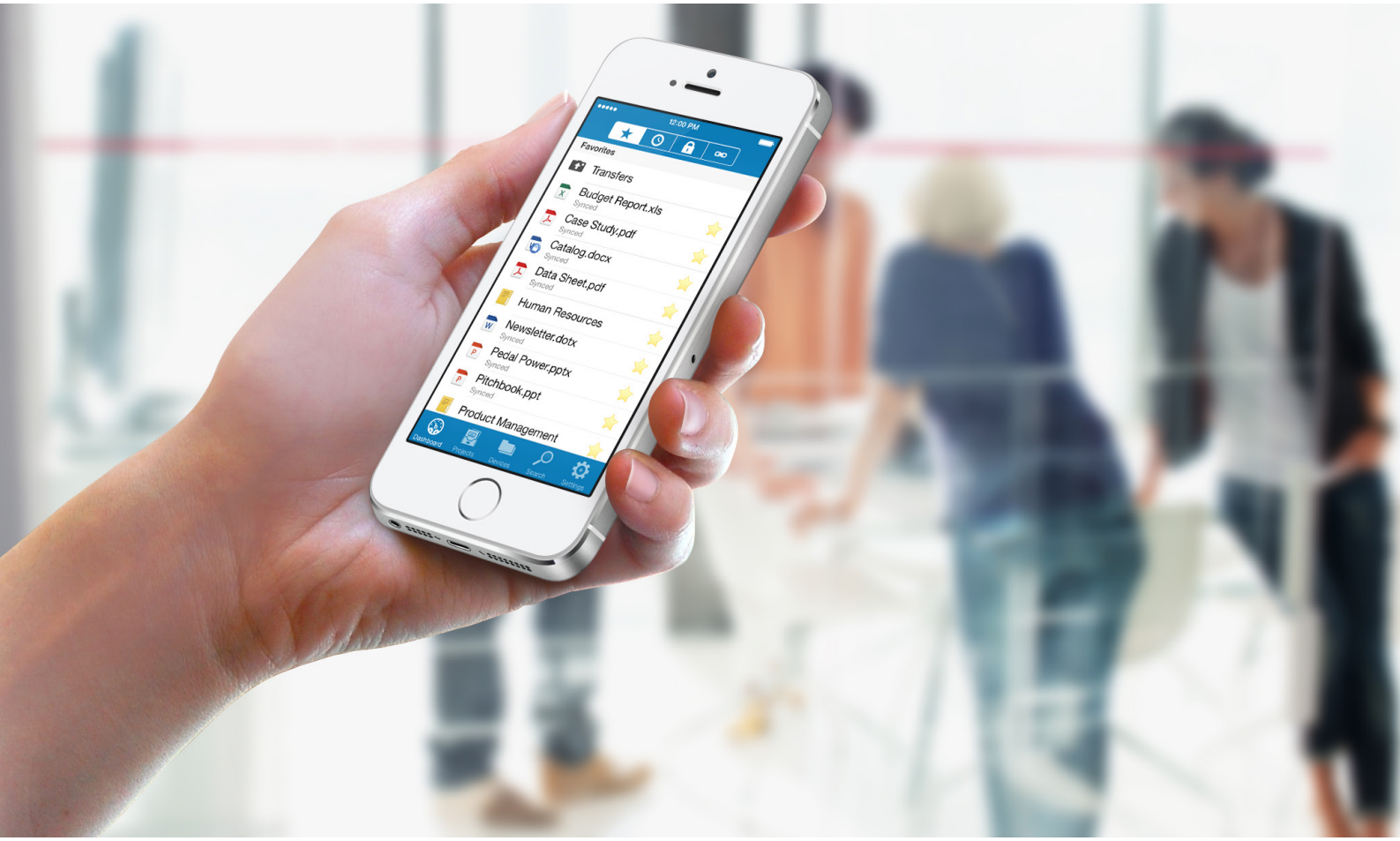
150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr



“Digital information is estimated to grow by a factor of 300 between 2005 and 2020”

IDC, 2014



File Sharing that's Fully Mobile Ready and Secure – Soonr Workplace

How do you prepare your organization for a future in which data devices will continue to proliferate at the same time employees and external partners reject any boundaries on access, sharing and time limitations? One of the first must-have solutions to accommodate this new world order of data flow is putting in place the best secure file sharing features available – Soonr Workplace.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr

Soonr Workplace is a complete, secure file sharing and collaboration solution that enables your team members to safely manage, organize and share files from any device, anywhere. It enables productivity by allowing teams to work on any type of business document or digital content – from their device – in real time, without fear of security breaches. Soonr Workplace also gives workers built-in security controls that can be set up based on need-to-share so your teams can focus on tasks and strategy that enhance business value.

Get the flexibility your teams need with the business productivity executives demand, at the same time providing a wide range of security controls to prevent data breaches and costly downtime. Find out more about Soonr Workplace today at www.soonr.com.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr

About Soonr

Founded in 2005, Soonr is headquartered in Silicon Valley, California with offices in the UK and Denmark. Our mission is to make organizations more productive and competitive by securely connecting office and mobile workers and their critical information. Our secure file sharing and collaboration services have been in commercial production since early 2007 without a single security breach or a data loss incident.

Embraced by users and endorsed by IT, Soonr delivers its service to over 150,000 paying businesses worldwide in 134 countries, through a network of cloud service providers, VARs, MSPs and systems integrators.

Built on a highly scalable and secure infrastructure that is Type 2 SOC (Service Organization Controls) audited against SSAE 16 standards as well as HIPAA and PCI DSS compliant, Soonr operates geo-redundant data centers in four jurisdictions including the US, Canada, EU and Australia. Customer data always resides and is redundantly mirrored in alternate sites within the same jurisdiction to comply with regional privacy and security concerns and regulations.

150 South Almaden Blvd, Suite 1050 San Jose, CA 95113
www.soonr.com | 408.377.8500

soonr


soonr