

# Market Trends: Secure File Sharing And Collaboration In The Enterprise, Q1 2014

by Heidi Shey, February 4, 2014

## KEY TAKEAWAYS

### **Today's Workforce Needs And Key Business Processes Require Data Security**

Today's anytime, anywhere information workforce is accustomed to working on multiple devices and requires regular communication and collaboration with peers and business partners in order to do their jobs. Unfortunately, easy and common methods for meeting these needs carry the risk of accidental data disclosure.

### **There Is No Shortage Of Solutions For Secure File Sharing And Collaboration Today**

Rising to meet demand, technology and security vendors offer a variety of solutions to enable secure file sharing and collaboration today. There are many flavors when it comes to such solutions, and not all are directly competitive with each other despite sharing similar sets of feature functions and data controls.

### **Support A Holistic Data Protection Strategy With Data Controls Available Today**

Common control features in secure file sharing and collaboration solutions address everything from authentication to watermarking. Combined with data controls, deployment options, data visibility, and reporting capabilities, such solutions help to support a holistic data protection strategy using Forrester's data security and control framework.



## Market Trends: Secure File Sharing And Collaboration In The Enterprise, Q1 2014

What You Need To Know About Workforce Behavior And Available Data Controls

by [Heidi Shey](#)

with [Stephanie Balaouras](#) and Kelley Mak

### WHY READ THIS REPORT

Whether the organization's interest in file sharing and collaboration solutions comes from BYOD initiatives, workforce demands, or peer and partner collaboration requirements, security and risk (S&R) pros are increasingly asked to weigh in or lead efforts to securely enable this critical business process. S&R pros should consider such solutions as tools to help augment and support a holistic data protection strategy. This report (part 1 in a series of three) showcases workforce behaviors and trends that are hastening demand for secure file sharing and collaboration solutions and identifies key data control feature functions that S&R pros have available today.

### Table Of Contents

#### 2 **Workforce Collaboration Behaviors Demand Increased Data Security**

Such Behaviors Contribute To Accidental Data Disclosure, Data Governance Failures

#### 5 **Secure File-Sharing And Collaboration Solutions Flood The Market**

Three Main Pillars Of Activity Spawn A Variety Of Use Cases

Enterprises Encounter A Variety Of Options For Data Control

#### WHAT IT MEANS

#### 9 **Hold On Tight — It's Going To Be A Wild Ride**

#### 10 **Supplemental Material**

### Notes & Resources

Forrester interviewed 40 vendors offering solutions for file sharing and collaboration; drew insight from numerous client inquiries on data security, file sharing, and collaboration; and analyzed data from the Forrester Forrsights Applications And Collaboration Workforce Survey, Q4 2013 and data from CyberFactors for this report.

### Related Research Documents

[Tech Spotlight: Enterprise File Sharing](#)  
December 20, 2013

[What File Sync And Share Customers Have Learned](#)  
July 24, 2013

[Control And Protect Sensitive Information In The Era Of Big Data](#)  
July 12, 2012



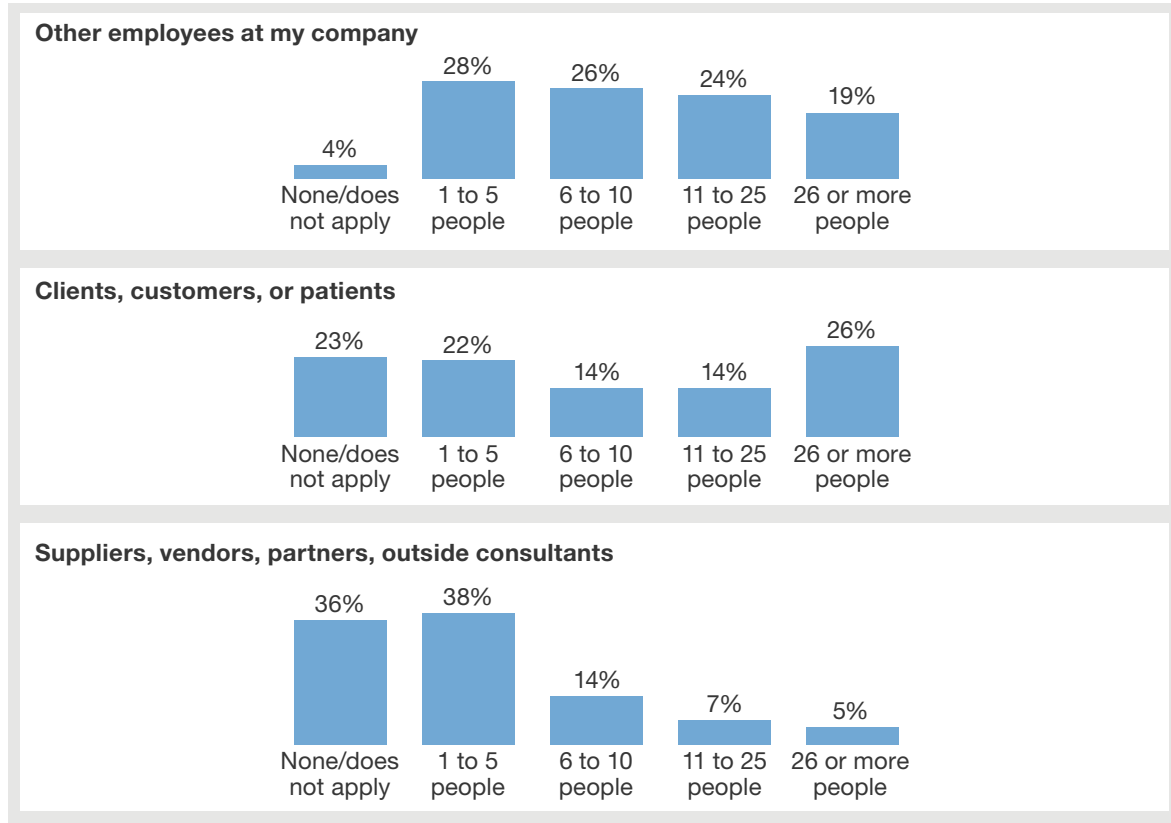
## WORKFORCE COLLABORATION BEHAVIORS DEMAND INCREASED DATA SECURITY

Mobile connectivity and a plethora of free and paid cloud services and tools for productivity have radically changed how peer and business partner collaboration happens today. Consider that today's anytime, anywhere workforce:

- **Requires regular communication and collaboration.** Today, 97% of information workers regularly communicate or collaborate with others in their company as a part of their day-to-day job; 76% say the same when it comes to contact with customers or clients, and 64% do so with suppliers, vendors, and partners (see Figure 1). Such activities are — and always have been — the backbone of doing business. But the security stakes increase as teams, customers, and business partners are more dispersed and more is done online and in digital formats such as signing contracts and submitting/transmitting sensitive information.
- **Uses multiple devices for work.** Roughly 61% of information workers today are using some type of mobile device (laptop, tablet, or smartphone) for work.<sup>1</sup> As we dive in to take a deeper look at how many devices overall (desktops, laptops, tablets, smartphones) information workers use to do their jobs today, we find that 53% are using three or more devices (see Figure 2).
- **Values tool accessibility to ensure that all parties have access to information.** As employees select technologies and tools to help them communicate and collaborate, and specifically, to share information with others, accessibility of the tool by all recipients is the top decision criterion (see Figure 3). Accessibility aside, employees are also selecting technologies to use to share information based on sensitivity of the information, their personal preference of technology, and efficiency. As a result, email, USB flash drives and CD/DVDs, and network are three common methods in use for file sharing today.<sup>2</sup>

**Figure 1** Information Workers Regularly Communicate Or Collaborate As A Part Of Their Job

**“In a typical week, who do you regularly communicate or collaborate with as part of your day-to-day job?”**



Base: 4,106 North American and European information workers at SMBs and enterprises  
(percentages may not total 100 because of rounding)

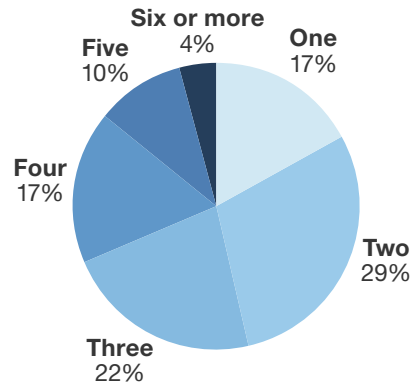
Source: Forrsights Applications And Collaboration Workforce Survey, Q4 2013

109821

Source: Forrester Research, Inc.

**Figure 2** Multidevice Use Is The Norm

**Number of devices used for work**



Base: 4,106 North American and European information workers at SMBs and enterprises

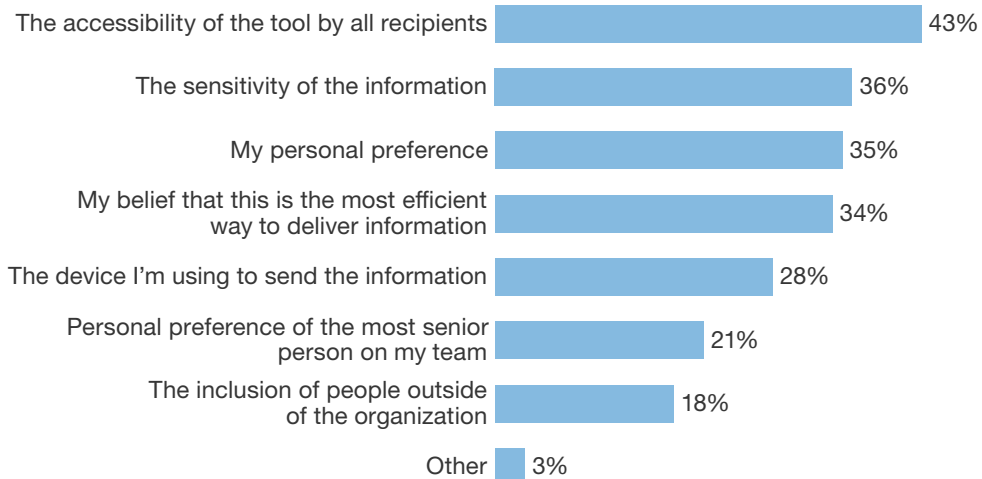
Source: Forrsights Applications And Collaboration Workforce Survey, Q4 2013

109821

Source: Forrester Research, Inc.

**Figure 3** Accessibility Is A Top Criteria For Information-Sharing Tools

**“How do you decide which technology to use when you share information with others as part of your job?”**



Base: 3,665 North American and European information workers at SMBs and enterprises

Source: Forrsights Applications And Collaboration Workforce Survey, Q4 2013

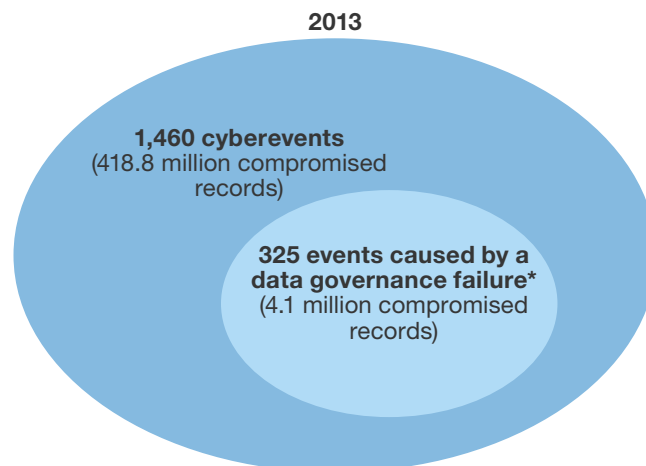
109821

Source: Forrester Research, Inc.

### Such Behaviors Contribute To Accidental Data Disclosure, Data Governance Failures

Human error, in addition to data security policy and data handling process failures, is a common cause of data breach and security incidents. In 2013, out of 1,460 publicly reported cyberevents, 325 were caused by a data governance failure, representing 22% of incidents overall (see Figure 4).<sup>3</sup> As employees engage in collaboration and file sharing, do so from various device types, or seek to sync files across devices for easy access on the go, they also risk losing or exposing information. For example, in September 2013, an employee at the Georgia Department of Labor accidentally emailed an internal file containing names and SSNs of 4,457 career center customers to 1,000 recipients.<sup>4</sup> And in cases where the correct files are shared with the correct recipients, many firms are blind to what happens to their data after that point: Will the recipients forward the file and information to others that should not be privy to it?

**Figure 4** Accidental Data Disclosure And Data Governance Failures Happen



Source: Cyberfactors, LLC

\*These events include data policy or process failure and wrongful data collection, sharing, and distribution. Examples of such events include inadvertent disclosures via email, violation of privacy practices, printed copies of sensitive files found in a dumpster, etc.

109821

Source: Forrester Research, Inc.

### SECURE FILE-SHARING AND COLLABORATION SOLUTIONS FLOOD THE MARKET

In response to enterprise demand, technology vendors of all sizes and stripes are rising up to meet the challenge of secure file sharing and collaboration.<sup>5</sup> There is a multitude of easily accessible (and free!) consumer-oriented file-sharing and collaboration solutions that employees are likely already using. For example, many vendors like Barracuda Networks, Dropbox, Google, and Microsoft that offer an enterprise or business solution for secure file sharing and collaboration also have a free consumer solution. While seemingly pure-play solutions and services like Accellion, Box, Egnyte, SafelyLocked, Soonr, WatchDox, and Workshare — and more! — exist, file-sharing and collaboration capabilities

are also a natural feature or additional extension to the product portfolio of many existing solutions today: file sync, mobile device management, managed file transfer, storage and backup, enterprise content management, virtual data room, and data security and governance.

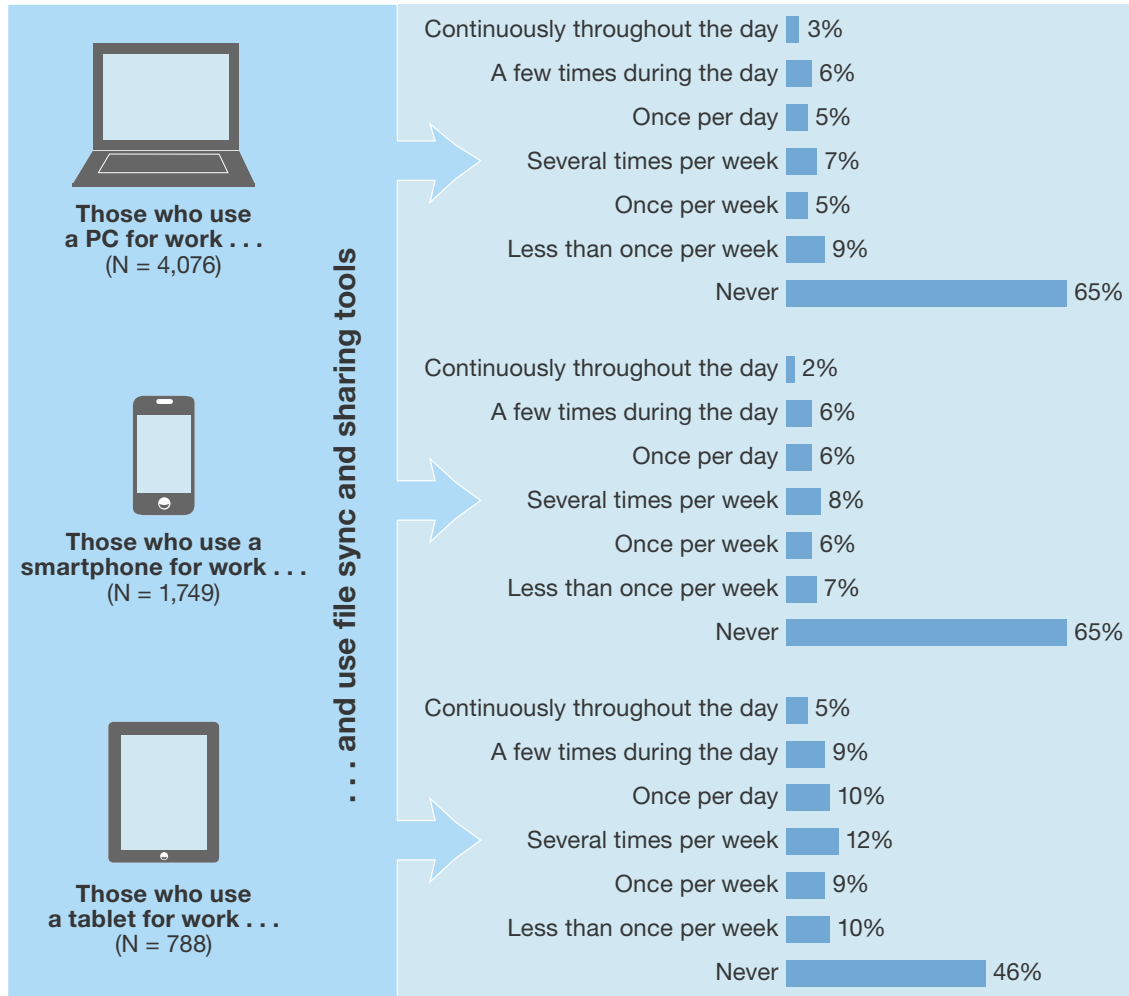
### Three Main Pillars Of Activity Spawn A Variety Of Use Cases

Secure file-sharing and collaboration solutions address workplace issues that apply across industries. Common expected benefits include reduced risk, reduced paper usage (by reducing the need to print out documents), and increased productivity, speed and efficiency of decision-making, IT visibility, and eDiscovery capabilities. Some cloud-based solutions may also help to reduce storage costs. In general, organizations look to such solutions in order to:

- **Sync.** File sync is a desirable feature for mobile workers, frequent travelers, or those who regularly work on multiple devices to access their content. Today, a whopping 55% of information workers in North America and Europe who use a tablet for work use file sync and share tools; 5% of these workers use these tools continuously throughout the day (see Figure 5).
- **Share.** Content sharing helps support activities like sales enablement for getting collateral and up-to-date information to sales teams and field reps, distribution of operations manuals and documentation to field technicians and workers, and distribution of financial documents such as board packs and regulatory filings. Some firms even use sharing solutions for software delivery to customers, or to distribute training materials. Secure file-sharing solutions can support a host of other industry-specific activities as well. Construction, architecture, and engineering firms use these solutions to share drawings and floor plans. Universities use sharing to distribute information to students or request documentation for financial aid calculations. Financial services firms use sharing to get research into hands of investment analysts and wealth advisors. Manufacturing firms use sharing for supply chain integration with suppliers and customers or for extended R&D uses.
- **Collaborate.** This typically involves editing, commenting, and annotated-markup capabilities to enable multiple parties to work on a single document. Common use cases include marketing content creation and publication, legal documentation collaboration, due diligence, and M&A activities. Research universities or pharmaceuticals can use collaboration solutions to move data and exchange notes relating to research studies or clinical trials.

**Figure 5** Tablet Users Use File Sync And Sharing Tools More Frequently

**“How frequently do you use the following applications or services for work on a computer?”**



Base: North American and European information workers at SMBs and enterprises (percentages may not total 100 due to rounding)

Source: Forrsights Applications And Collaboration Workforce Survey, Q4 2013

109821

Source: Forrester Research, Inc.



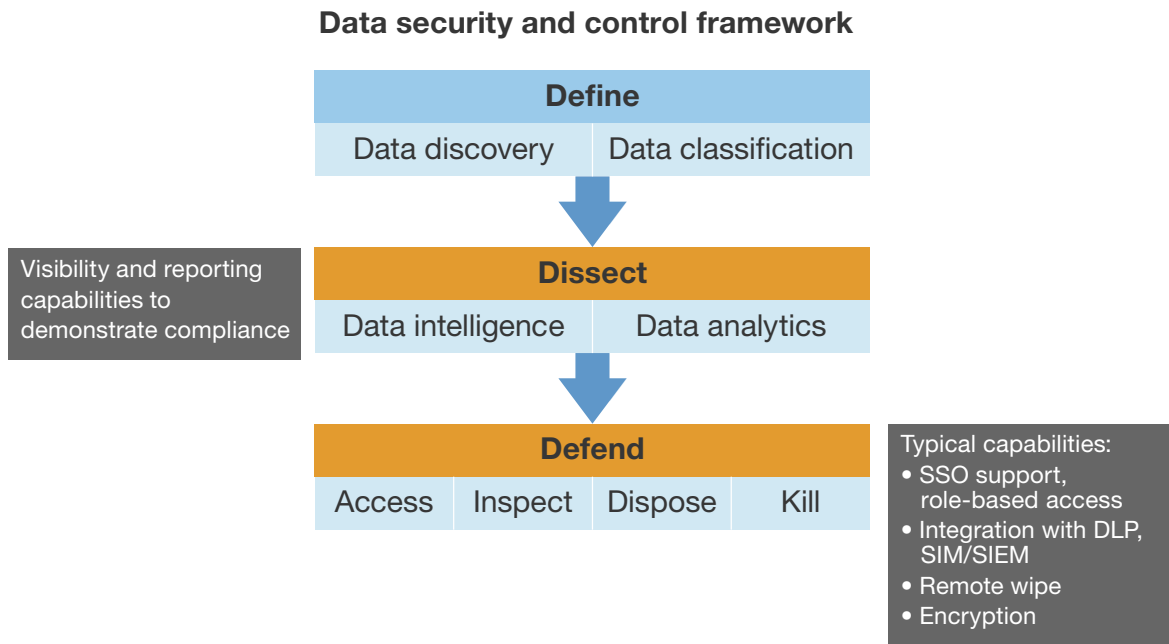
## Enterprises Encounter A Variety Of Options For Data Control

Typically, when organizations think of secure file-sharing and collaboration solutions, file access permissions come to mind, but there are many more additional data control capabilities available: authentication, device pinning, content management and workflow, encryption, file expiration, file retention management, integration with other security tools and technologies, password protection for files, remote wipe, reporting capabilities, and watermarking (see Figure 6). Within Forrester's data security and control framework, the data control, policy enforcement, visibility, and reporting capabilities provided by secure file-sharing and collaboration solutions help to support a holistic data security and control strategy (see Figure 7).<sup>6</sup>

There are also multiple ways to deploy secure file-sharing and collaboration solutions to best fit your firm's requirements and risk tolerance: public cloud, private cloud, on-premises, or hybrid of cloud and on-premises. Security and data control considerations aside, it is critical to understand both business and workforce needs before choosing a solution.<sup>7</sup>

**Figure 6** An Overview Of Common Data Controls Available Today

Control feature	Description
Authentication	Support for Active Directory, LDAP, SSO, SAML
Device pinning	Pin or restrict content access to a specific device.
Content management and workflow	Check-in/checkout, assign tasks, version control, eSignatures, and approvals
Encryption	This varies. It can include encryption at rest or in transit, and encryption keys may be held by the customer or the vendor.
Expiration date	Determine when access to content expires.
File permissions	Read-only, write, edit, disable copying/pasting of content, revoke access; printing, upload/download, or screen capture restrictions; prevent opening of files in third-party apps; ability to work offline; restrict file sync to specific devices (e.g., corporate owned); enable/disable macros
File retention management	Determine file retention and archiving policies.
Other security integrations	Integration with other security technologies/solutions like DLP, MDM, MAM, as well as SIM/SIEM and data classification tools
Password protection	Password protect access to content
Remote wipe	Remotely wipe content on devices
Reporting	This can include a full audit trail of data access and use, with information such as IP address, device type, time stamp, and more. In addition, other types of reporting such as storage use and outcome of authentication requests may be available as well.
Watermarking	Static watermark or dynamic watermarking unique to the user accessing the data

**Figure 7** Secure File-Sharing And Collaboration Solutions Support A Holistic Data Protection Strategy

109821

Source: Forrester Research, Inc.

**WHAT IT MEANS****HOLD ON TIGHT — IT'S GOING TO BE A WILD RIDE**

The sheer breadth and variety of file-sharing and collaboration solutions on the market today makes it a daunting exercise for firms looking to make a shortlist of vendors. Not all vendors that offer file-sharing and collaboration solutions are directly competitive with each other, despite offering similar sets of feature functions. This is a dynamic market that has exploded in the past 18 months. Expect to see more sparks fly in 2014 as:

- **Enterprises clamor for clarity and budget.** Organizations will strive to uncover shadow IT implementations of file-sharing and collaboration solutions, identify how employees prefer to work, and nail down business requirements as they go down the path of short-listing vendors and solutions. Data privacy and deployment option (to cloud or not to cloud?) conversations will dominate as questions about data residency and data access are top of mind for S&R pros. Regulatory compliance is only one aspect of such discussions; many organizations also voice concerns about unknown parties — state-sponsored actors, for example — potentially gaining access to their data without their knowledge. File sharing

and collaboration will gather multiple stakeholders — from business units to the CIO to the CISO — who can then pool budgets to make the purchase, especially if use cases have the ability to change or enable better customer interactions and experiences.

- **Vendors rush to differentiate and gain market share.** File-sharing, synching, and collaboration capabilities are fast on the way to becoming commoditized features. While the market for enterprise and business solutions will continue to grow at a good pace, expect to also see an uptick in growth of consumer solutions. For business teams that are unwilling to wait for corporate IT to implement a solution, many will turn to using either a free solution or a shadow IT implementation out of the departmental budget. As more and more solutions eliminate the need for a recipient to have the solution that the sender uses to share a file, there will be less of a vendor “lock in” effect. Data security (and encryption strategy, specifically!), privacy considerations, integrations, and usability will help separate the market leaders from the laggards initially — and larger vendors will make moves to gobble up smaller ones as revenue or technology purchases. Advances in leveraging user and data context, metadata, analytics, and automation will usher in additional security controls and capabilities for the next stage of this market’s evolution.

---

## SUPPLEMENTAL MATERIAL

### Methodology

Forrsights Applications And Collaboration Workforce Survey, Q4 2013, was fielded to 4,827 information workers located in Canada, France, Germany, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester’s Forrsights for Business Technology and was fielded during October 2013 and November 2013. Toluna fielded this survey online on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates. We have provided exact sample sizes in this report on a question-by-question basis.

Each calendar year, Forrester’s Forrsights for Business Technology fields business-to-business technology studies in more than 17 countries spanning North America, Latin America, Europe, and developed and emerging Asia. For quality control, we carefully screen respondents according to job title and function. Forrester’s Forrsights for Business Technology ensures that the final survey population contains only those who use a PC or smartphone at work for at least 1 hour per day. Additionally, we set quotas for company size (number of employees), gender, and job function as a means of controlling the data distribution. Forrsights uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Forrester collaborated with CyberFactors to obtain the data used in this report. The data may contain publicly available information and/or proprietary data collected by CyberFactors. The analysis of the data is exclusively Forrester’s. More information is available at [www.cyberfactors.com](http://www.cyberfactors.com).

## Companies Interviewed For This Report

Accellion	IBM
AirWatch (now part of VMware)	Infrascale
Alfresco Software	Intralinks
Averail	Microsoft
Barracuda Networks	Mimecast
BoardVantage	nCrypted Cloud
Box	Novell
Brainloop	Safe-T
Citrix ShareFile	SafelyLocked
CloudMe	ShareVault
Content Raven	Soonr
Cubby by LogMeIn	SugarSync
CX.com	Syncplicity by EMC
DigitalQuick by Fasoo	TeamDrive
Dropbox	Thru
Druva	Tibco Software
Egnyte	Varonis Systems
Fiberlink (now part of IBM)	Vaultize
Google	WatchDox
Hightail	Workshare

## ENDNOTES

- <sup>1</sup> Throughout the year, Forrester analysts engage in hundreds of discussions with vendors and end users about data security and privacy. Analysis of B2B survey data from Forrester's Forrsights Security Survey, Q2 2013 and additional data from our data partner CyberFactors provides another layer of insight into the state of data security and privacy today and in the future. This data-driven report outlines budgeting and spending, technology adoption plans, and other key breach, data protection, and privacy trends in North American and European organizations for 2013 to 2014. Understanding these trends and their implications

will help security and risk (S&R) executives examine and adjust as necessary their own resource allocation for data security and privacy. See the October 1, 2013, "[Understand The State Of Data Security And Privacy: 2013 To 2014](#)" report.

- <sup>2</sup> Much of the information used in the course of doing business today exists in a digital format, and there comes a point when it's necessary to share this data with other employees or key business partners. File sharing happens in a variety of ways between multitudes of different groups. While each method has its own risks, a common shared risk is accidental data leakage. For more information, see the December 20, 2013, "[Tech Spotlight: Enterprise File Sharing](#)" report.
- <sup>3</sup> CyberFactors tracks publicly reported cyberevents. Security incidents and breaches that are not publicly reported are not counted here. As a result, the actual number of incidents is likely higher.
- <sup>4</sup> Source: Kristal Dixon, "GDOL Works To Prevent 'Human Error' That Caused Security Breach," Canton-Sixes Patch, September 6, 2013 ([http://canton-ga.patch.com/groups/business-news/p/gdol-works-to-prevent-human-error-that-caused-security-breach\\_cc42914f](http://canton-ga.patch.com/groups/business-news/p/gdol-works-to-prevent-human-error-that-caused-security-breach_cc42914f)).
- <sup>5</sup> In Forrester's 26-criteria evaluation of file sync and share vendors, we identified, researched, analyzed, and scored products from the 16 most significant solution providers in this market: Accellion, Acronis International, AirWatch, Alfresco Software, Box, Citrix Systems, Dropbox, Egnyte, EMC, Google, Hightail (formerly YouSendIt), IBM, Microsoft, Novell, salesforce.com, and WatchDox. We scored factors like mobile support, security, links to systems of record, organizational commitment, market experience, and deployment architecture to give you the decision tools to create the right shortlist for your particular environment and scenarios. This report and accompanying spreadsheet detail our findings about how well each vendor scores based on our criteria and where they stand in relation to each other. For more information, see the July 10, 2013, "[The Forrester Wave™: File Sync And Share Platforms, Q3 2013](#)" report.
- <sup>6</sup> Forrester has created a framework to help security and risk professionals control big data. We break the problem of securing and controlling big data down into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data. For more information, see the July 12, 2012, "[Control And Protect Sensitive Information In The Era Of Big Data](#)" report.

Data defense is the fundamental purpose of information security. To defend your data, there are only four levers you can pull — controlling access, inspecting data usage patterns for abuse, disposing of data when the organization no longer needs it, or killing data to devalue it in the event that it is stolen. Policy addresses when and how much to pull the levers. We designed this report to help S&R leaders develop effective policies using our data security control and control framework as a guideline. For more information, see the January 15, 2013, "[Know Your Data To Create Actionable Policy](#)" report.

- <sup>7</sup> Forrester recently completed a Forrester Wave™ evaluation of file sync and share platforms to help CIOs pick the best solution for their document collaboration scenarios. As part of the process, we interviewed the reference customers of 16 different file sync and share vendors. These early adopters have learned from experience what matters in a solution: ease of use, reliability, vendor partnership, price, and security. These reference customers also identified best practices for choosing a vendor, such as defining the business need and the employee requirements and then running one or more pilots to fine-tune the choice. For more information, see the July 24, 2013, "[What File Sync And Share Customers Have Learned](#)" report.

## About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

### FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at [www.forrester.com](http://www.forrester.com). For a complete list of worldwide locations, visit [www.forrester.com/about](http://www.forrester.com/about).

### CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or [clientsupport@forrester.com](mailto:clientsupport@forrester.com). We offer quantity discounts and special pricing for academic and nonprofit institutions.

---

## Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« SEAN RHODES, client persona representing Security & Risk Professionals

