Whitepaper

Top 10 Ways to Assess
The Risk of Data Loss

Infrascale™

How Exposed is Your Customer's Data?

10 Ways to Identify the Risk.

Employees across all ranks in your customers' organizations have encountered, and possibly embraced, free file sharing. The risk to their firms could be great, depending on how these tools are used and which departments are using them. This guide will help you evaluate whether or not your customers are addicted to free file sharing applications and if they're leaving their company's data exposed.

1 Does the IT department provide employees with approved file sharing and syncing solutions?

If an organization does not provide an approved file sharing solution, employees will likely find their own applications that also happen to be free. Employees have likely used free file sharing tools, such as YouSendIt and Dropbox at home with friends and family. Naturally, they enjoyed the convenience of such tools and brought them into their organization. While convenience is great, these tools cannot be controlled by IT in this type of situation. This could pose major security risks to IT and the entire organization.

2 On which cloud does the collaboration tool sit?

Knowing and trusting your cloud is very important to most IT departments. Free collaboration tools rarely provide full transparency and detailed information about the quality of their data centers or even basic features of their data centers. Making sure that you have approved the cloud used for your customers' file sharing and collaboration solution will ensure that it meets your standards and will not needlessly expose data to hackers or natural disasters.

3 Do they blacklist or block the usage of free file sharing and collaboration tools?

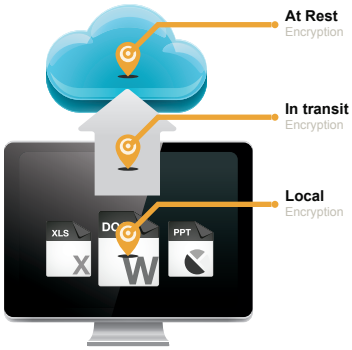
Some organizations have decided to settle the feud between free file sharing and IT by simply blocking usage of Dropbox, YouSendIt, SugarSync, and others. While this serves a short term purpose of preventing data leakage, it prevents their employees from being able to benefit from the productivity enhancing features of collaboration tools. Provide a top-down solution that can be controlled by their IT and meet customers' needs of convenient file sharing.

4 Do they have a written policy stating which free collaboration tools are not approved?

Your customers could be quickly discouraged from using free collaboration tools by simply placing a policy disallowing them in their company handbook. This is an easy way to remove the risk of these solutions and prepare the department for the launch of a top-down, IT controlled file sharing tool.

5 Are you aware of the levels of encryption used in their file sharing tool?

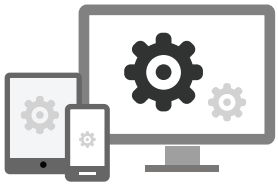
Free file sharing tool websites often fail to present complete information about the encryption levels used in the transmission of their data and of the data at rest. This is generally because their users are consumers or employees and not operating with the expectations of the IT department in mind. Ensuring that you know, and trust, the encryption levels used in the approved file collaboration tool will go a long way to preventing security breaches due to hacks.



6 Does the IT department report on user behavior within the collaboration tool?

Being able to report on collaboration application usage will often detect the symptoms of data leakage problems before they start. If your customers cannot do this with their existing solution, they may miss, or be too late, to detect breaches in data security. Identify a tool that will allow them to monitor user and file activities to identify and eliminate problems, like hot files, before they become too big to handle.

7 Can the IT department control how each user is allowed to use the collaboration tool?



Monitoring user behavior is one thing, but completely controlling it is quite another. If IT does not centrally control the collaboration tool used in the organization, it will not be able to allow and disallow specific behaviors by user. This can cause more problems for some departments (eg. the legal department) than others using less sensitive data-like support.

8 Do they scan employee desktops for viruses or malware separately?

Free file sharing can put your customers at risk for invasion of malware and other viruses. Because these tools are not centrally managed and under your control, there is no guarantee that users may not inadvertently install a virus. Malware and viruses may be included in the synchronization desktop tool or within the web-based application. Use a trusted product that you've evaluated to verify that your customers' collaboration solution does not contain malware or viruses.

9 Do they have a BYOD (bring your own device) policy that is actively enforced?

Tablets, Androids, iPhones, Windows phones and other devices may come with free file sharing tools pre-installed. These devices are frequently used by employees within an organization, but the applications installed on them are managed by the employee. BYOD is a hot-button issue in IT, due to the hardware and software control issues it presents. However, there are collaboration tools that can be approved and used on all of these devices. This will prevent your customers from major headaches in the long term.

10 Are departments such as design, finance, and legal using free file sharing tools?

Design, finance, and legal are the departments most likely to begin using free file sharing tools. After all, they are sending large files that contain your customers' intellectual property. If your customer has employees that perform these functions, they may be very likely to have employees using unauthorized file sharing tools.

Infrascale FileLocker is a secure collaboration tool for your customers.
Visit infrascale.com to learn more.

About Infrascale

Infrascale connects people, devices and their data in ways that are truly secure. Headquartered in El Segundo, California, Infrascale's cloud platform runs from eleven data centers on five continents. Infrascale software spans mobile, desktop and cloud and powers **EndGuard**™, **FileLocker**™, **Infrascale Backup**, **SOS**™ **Online Backup** and over one-thousand independent cloud service companies, VARs and MSPs. Visit http://www.infrascale.com.