The Fundamentals of Secure Collaboration

Why you can be safe when you work in the cloud

Cloud-based collaboration tools are opening doors for businesses. The cloud provides anywhere, anytime access to key apps, data, files and services.

And from the cloud, you can interact with your clients whether you're at your desk, out in the field or traveling for work. This convenience lets you manage everything from email to file sharing to feedback and approvals on any device whenever you need it.

Many businesses are already experiencing these benefits:

- 80 percent of businesses believe the cloud can improve their flexibility and agility.

- 77 percent think the cloud makes it easier to handle the growing quantities of data they must deal with.

- 76 percent believe the cloud will support their business needs better than traditional technologies.

But even with all these benefits, all clouds are not created equal and these days you need a secure solution. Ultimately, secure collaboration in the cloud boils down to three key issues:

- Knowing what to expect from solutions.

- Understanding what you can do to protect data.

- Ensuring visibility into assets in the cloud.

Cloud services and security

There are plenty of options to consider when it comes to cloud collaboration services, and knowing what to look for can make the difference between getting a secure solution and ending up with a tool that puts your data at risk.

The breadth of technologies and tools at your disposal can make deciding on a service mind boggling – especially when it comes to choosing a solution you're willing to trust with your business data.

And while no solution is perfect, there are fundamental security features you should expect to find in the service you choose.

End-to-end encryption

Data is encoded in storage and when it leaves a device. Then it's decoded when somebody with authorization attempts to view it. Even though codes can be cracked, the reality is that modern encryption codes are so sophisticated that it would take decades - if not centuries - to solve them. Cloud collaboration services that use encryption can play a huge role in keeping data safe, and the Ponemon Institute found that 56 percent of organizations are already encrypting cloud data.

Secure sync and share

Hackers and malware might be out there, but employees can actually introduce more risk when it comes to data security. In fact, one study found that 79 percent of IT pros say that people – not technology – can pose the greatest security gaps. Accidentally sharing or deleting information can lead to data breaches, but secure cloud collaboration services that automatically sync your data ensure that nothing gets lost or stolen.

Compliance support

You need to be able to trust that your cloud service provider will support regulatory laws that apply to your business. Carbonite found that 68 percent of small businesses have at least one regulatory law they need to comply with. Make sure your cloud service provider can support your regulatory demands like HIPAA, HITECH, FINRA, CFPB, and bar association ethics rules. Carbonite found that 68 percent of small businesses have at least one regulatory law they need to comply with.

Passwords and user-authentication

Cloud services have evolved to give you more options than ever when it comes to protecting personal credentials and confidential data. In fact, Capgemini found that 84 percent of businesses are offering multiple login options to go beyond passwords.

With multi-factor authentication you can add layers to how you safeguard data with two-step verification methods, such as form and token-based authentication as well as SMS, voice and backup codes for account entry.

Benefits of the cloud:

80%

of businesses

believe the cloud can improve their flexibility and agility.

77%

think the cloud makes it easier to handle the growing quantities of data they must deal with.

76%

believe the cloud will support their business needs better than traditional technologies.

Activity tracking

Collaboration means putting data in the hands of clients, co-workers and other project stakeholders. Control is critical here and being able to track documents and files is essential. Approximately 36 percent of respondents to a Bitglass survey said that having users share files and data for use on unauthorized devices was a primary concern. What's more, 20 percent said giving access to unauthorized users was a major concern.

When it comes time to collaborate in the cloud, you need clear visibility into where your files are going, who can access them and when they interact with that data. Poor transparency can put you at risk, but high visibility lets you track your data and avoid security gaps.

Collaborating with confidence

With cloud collaboration services constantly enhancing security, the cloud is quickly becoming one of the most secure and simple ways to get work done – from any device, anywhere, and at any time. Choosing providers with secure collaboration apps is a great start, and from there, you're free to focus on issues you can control.

Presented in partnership with Citrix ShareFile.