Is Cloud Security Second-Class Security?

What's keeping your businesses from embracing Cloud?

Not that many years ago, the widespread usage of the Cloud was certainly up for debate. For example, early Cloud upstarts in Customer Relationship Management (CRM) began challenging the enterprise software delivery model (at the time, this was called Software as a Service, or SaaS). Surely a real business wouldn't use an unproven software delivery model. Well… they did, and they did it en masse.

Today, banks are using the Cloud for storage of customer documents. Schools are using the Cloud to convert student records into electronic records. Even healthcare providers are leveraging the Cloud to provide access to medical files and improve quality of care. Cloud computing continues to make its mark on all kinds of businesses. This is because business decision makers feel the Cloud deployment value proposition will cause them to be better off than traditional methods.

But what about security?

What is keeping some businesses from embracing Cloud as a convenient delivery mechanism for computing technology? Utilizing a Cloud service via the public Internet, some private/public Cloud hybrid, or even outsourcing your own private Cloud involves "going outside" for IT. Organizations may worry that Cloud deployment might sacrifice information security. These businesses feel a greater sense of control when they can manage the technology deployment themselves.

We all want control over our data, whether it's personal or business-related. There's satisfaction in handling it ourselves. It brings us peace of mind. As the gatekeeper, you alone control access. However, the downside to managing your data yourself is that you are also its only line of defense. That's a lot of responsibility to keep everything under your control.

Cloud operations are held to very high standards

Think about home construction projects you may have seen on TV or in real life. Many projects can be handled by general contractors, but there's something to be said for specialization as well.

The same should be true for IT. Just because you can do it yourself doesn't mean you will get the best outcome. Today's leading Cloud services are staffed by information security experts whose sole focus is to combat security threats. While your IT staff may possess the necessary expertise, it's possible – and probably likely – that they are pulled in many directions dealing with the day to day IT needs of the company. Unless your office has a dedicated team of security experts, your data could actually be safer in the Cloud. Data center operators are held to extremely high standards, and it's their job to proactively ensure the safety and security of your data.

So what are some of those higher standards? Let's touch on just a few using Ricoh's Integrated Cloud Environment (ICE) as an example. Ricoh's ICE is a Cloud-based scanning and document delivery service.

Ricoh's ICE delivers scanning in the Cloud

Ricoh's Integrated Cloud Environment core components – which include the web application server, OCR server, and the management platform server – are all hosted at a purpose-built Data Center that's SSAE16 compliant. Ricoh Americas Corporation incorporates a formalized set of "Information Security Management System (ISMS)" policies – and is ISO 27001 compliant.

Data center systems are fully redundant to reduce the chance of data loss or corruption. Multiple prevention and detection technologies are integrated into its architecture, including 24-hour security monitoring and control. Multi-tiered system architecture limits access and guards against vulnerabilities to security breaches.

One of the greatest benefits of Cloud computing with Ricoh's ICE is dedicated security personnel. System support is provided by a team of certified system and networking professionals. Help is available 24 hours a day, 7 days a week – and "real-time" systems monitoring is implemented to immediately notify the support staff if a problem is detected.

Protecting your data in transfer

When you scan documents using Ricoh's Integrated Cloud Environment, security measures come into play from the moment you scan at your device. If you're using a Ricoh MFP, whether you scan to email or to the Cloud, security features such as authentication and 128-bit SSL encryption help keep your data safe as it's transferred between the MFP and the ICE server. Since ICE can route your scanned documents into other Cloud services (like Google Drive or DropBox) this leg of the journey between the ICE server and any **external Cloud service** is fully encrypted using 128 bit SSL. The ICE server stores scanning data only temporarily – just long enough to transmit it – and local data on the MFP is purged immediately after the transfer is complete.

Convenience and security – get both!

Are you really throwing caution to the wind by moving your data through the Cloud? Shifting to Cloud services in areas like scanning, document storage, mobile printing, device management and production job submission provides a convenient way to acquire the technology – plus you get built-in security measures as part of the deal. There's no reason to take on the burden when an established service provider can dedicate its resources and best practices to giving you the Cloud computing advantages you want – with the expert-designed security features you require.

Contact your Ricoh Team for additional information

Robert Bava |MedLar |robert.bava@ricoh-usa.com | 630.606.2480
Tim Wise|West-AZ | timothy.wise@ricoh-usa.com |714.689.6781
Constantine Psimaras |CDW-G/SMB |constantine.psimaras@ricoh-usa.com | 312.720.0682
Mike Gonzalez |East Coast | michael.gonzalez@ricoh-usa.com | 973.885.1061
Tara Clarkson | Inside Sales Rep | tara.clarkson@ricoh-usa.com | 636.326.3201

Contact Us