Highlights from a recent webcast on Office 365 security

OFFICE 365 DATA PROTECTION: MIND THE (BACKUP) GAPS

Sarah Beaudoin, product marketing manager for Druva inSync, and Charles Cooper, contributing editor to IT PRO, discuss what IT departments need to do to ensure Office 365 data is backed up and available when the business needs it.

If you've migrated to Microsoft Office 365, most of your business data now resides in the cloud. But how secure and accessible is it?

If there is a human or natural disaster, how easy will it be to restore your data? Is it even backed up? Is there an archive you can turn to? If legal issues arise will you be able to search and audit that data? What if there's a legal hold? Are you in compliance with all government regulations for data storage and management?

Are you going to rely on Microsoft to have answers or technologies for all these questions?

In a webcast discussion, Sarah Beaudoin, product marketing manager for Druva inSync, and Charles Cooper, contributing editor to IT PRO, advocated taking a more proactive approach to data security.

One of the key points they made is that while Microsoft is responsible for the cloud-based infrastructure and applications, you are still responsible for your data.

Blackboard/Shutterstock.com

"Organizations are warming to this idea of using SaaS based apps like Office 365, which offers the advantage of being accessible from the cloud," noted Cooper. "However, in the course of adoption, users often opt to rely on the built-in features for backup and recovery and here's where I think things get interesting and sometimes a bit dangerous from a security and data perspective. When it comes to Office 365, there's often the assumption that Microsoft's software protections automatically cover every requirement that you may need and if you believe that you're in store for a bit of a surprise if not a shock."

What Office 365 provides in terms of backup is not enough to protect your business against data loss from attacks by malicious hackers or natural disaster such as fires and earthquakes, the editor explained. Office 365 is robust in terms of providing Microsoft's end user applications in the Software-as-a-Service (SaaS) model. It was not designed to provide the kinds of backup and archiving capabilities required to meet regulatory and legal standards for governance and data availability, he added.

"At first blush that might seem counterintuitive," Cooper told the webcast audience. "The data is already in the cloud so why even bother with extra protection in the first place? But the fact is that a cloud solution like Office 365 isn't natively designed for data restoration."

Cloud providers may be responsible for functions such as network controls and host infrastructure, but in general, they are not in the business of providing comprehensive data protection, data accountability, and asset management, he explained.

How can IT be sure that business data that is part of a cloud-based SaaS application is actually being archived?

> "We know there is more data outside of the firewall. Your workers are carrying their data all over the place."
>
> *—Sarah Beaudoin, product marketing manager for Druva inSync*

File sharing is not data protection

Cooper said there are a number of misconceptions about what constitutes data protection, including thinking that end user features like file sharing will guard the data.

"File sharing is not data protection," he told the webcast audience. "You shouldn't make the mistake of assuming: Well, we're Office 365 users, the suite comes with cloud based file sync, share solutions, all the data is safe, and secure. When it comes to Office 365, OneDrive is not backed up and file sharing is designed for user collaboration, it's not designed for data recovery. It also doesn't extend to archiving or compliance or any kind of e-discovery challenges."

The bottom line is that the applications that come with Office 365 from venerable Microsoft WORD and Excel to SharePoint and Skype for Business are exactly what many companies need for end user productivity. However, when it comes to protecting data there are gaps and IT may need to look to additional software to make sure data is safe and available.

Filling in the data protection gaps

Druva focuses on helping organizations get control of their enterprise data, explained Sarah Beaudoin, product marketing manager for Druva inSync. This includes data that organizations may have in the cloud with Office 365, as well as data residing on employees' devices ranging from desktops and laptops to tablets and smart phones.

"We're helping organizations regain control of that data," she said. "We know there is more data outside of the firewall. Your workers are carrying their data all over the place. Anybody with a credit card can set up a SaaS account. So you might have some of these different accounts set up where you now have data flowing."

Beaudoin pointed to statistics that should give IT professionals pause:

- 50 percent of data exists outside the firewall
- 70 percent of cloud apps are not protected or backed up
- 600 percent YoY increase in ransomware
- 250 percent increase in regulations

Without data security tools, IT doesn't have visibility into the places where much of that data is stored and thus has no way to oversee its security and protection.

Druva inSync

Druva inSync compliments Office 365 to provide a single point of data protection management across enterprise endpoints and cloud applications. inSync enables organizations to regain control and address end-user data risks by providing a centralized system for the management, governance, and recovery of data.

inSync covers endpoints and cloud applications, and focuses on three key components of Office 365:

- Exchange Online
- OneDrive for Business
- SharePoint

With inSync, IT regains the kinds of data security controls it had when all information resided on servers behind a firewall. Whether it's recovering from human or natural disasters, complying with government and industry regulations or meeting court mandated requests, inSync provides:

- Backup and restore
- Archival
- Search & Audit
- Compliance
- Legal Hold

inSync closes the Office 365 data protection gaps with a unified solution that will:

- Ensure Office 365 data is protected from user error or malware, and is available on-demand
- Unify all end-user data into a single repository for better compliance and eDiscovery enablement
- Meet data retention requirements mandated by regulations or organizations