Feature

Alamy

STORAGE > BACKUP

Here's How Companies Should Back Up Microsoft 365 Data

Organizations shouldn't rely on Microsoft 365 to back up their critical data. Learn about implementing additional backup mechanisms.

Karen D. Schwartz | Nov 27, 2023

365 technologies. Until about five years ago, securing and backing up the data used with those technologies wasn't a concern. Most resources were on-premises, and Veeam backup software did the trick.

However, when the company began to shift toward more SaaS-based technologies, especially with a considerable amount of data now in the cloud-based Microsoft 365, the need for a new backup approach became apparent. Aleh Sadaunichy, Lyreco's network and architect manager, initially explored Veeam, but at that time, it didn't offer backup for Microsoft 365. Fortunately, as Lyreco was making its SaaS shift, Veeam introduced a Microsoft 365 backup module, making Lyreco one of its early users.

Related: Why Microsoft Copilot Technology Will Change How We Work

Since then, Sadaunichy has been a strong advocate for using third-party backups to protect Microsoft 365 data. Lyreco now ensures the backup of its Microsoft 365 data by configuring OneDrive, SharePoint, Teams, and other components. That involves setting up retention policies and versioning when required and choosing where the data will be stored. After that, it's just a matter of pointing Veeam at that data.

What Lyreco discovered echoes a trend observed by other companies – simply having Microsoft 365 doesn't guarantee automatic data backup.

According to a 2022 study by ESG, 33% of respondents felt they didn't need to back up SaaS applications within their organizations, while 35% said that SaaS providers' native backup capabilities and features are adequate. Many organizations incorrectly believe that SaaS applications are immune to data loss, noted Christophe Bertrand, a practice director at ESG.

Considering that Microsoft 365 has become a de facto standard for so many organizations, the absence of a secure backup strategy for Microsoft 365 data is a major concern. Today, more than one million companies worldwide use the productivity suite. That makes Microsoft 365 an attractive target for hackers.

Third-Party Backup Is a Best Practice

All these issues lead experts to one conclusion: Don't rely on Microsoft 365 for data backup. Instead, it's recommended to use an additional backup mechanism to ensure protection.

Sadaunichy agreed. “If you’re using Office 365, you wouldn’t want to store your data [solely] on OneDrive, for example. Even if you have data already uploaded to Azure Blob storage, it should replicated to another region. We keep three copies at a minimum.”

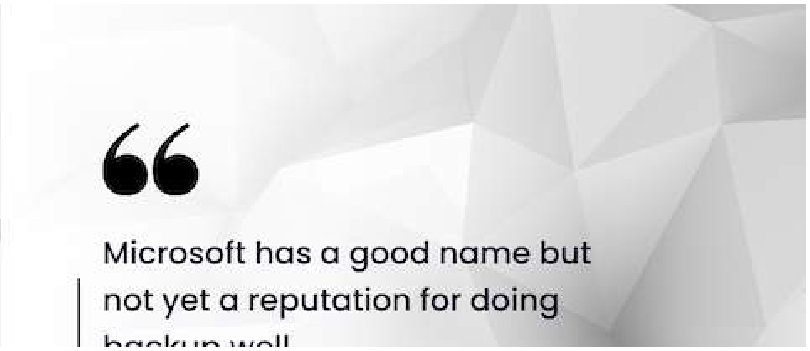
The task of spreading out backups of Microsoft 365 data has become easier in recent years. Most major backup vendors, including Veeam, Commvault, Datto, and Veritas, now offer modules designed to ensure the backup of Microsoft 365 data.

Microsoft itself has introduced one of the latest offerings – an online Microsoft 365 backup and recovery service. According to Microsoft, the service can back up and restore all or select Office-related sites, accounts, and mailboxes. It also provides the functionality to search or filter content using metadata and can connect to non-Microsoft applications via API.

Although this Microsoft service is relatively new, Bertrand said he expects that it will help organizations have a better profile for data protection. However, he added that it’s not best practice to rely on a single vendor for all needs. While Microsoft’s backup and recovery service could be a viable option for smaller organizations, organizations should use multiple vendors in their data backup strategy.

Aaron Turner, a faculty member at IANS Research who worked for Microsoft previously, looks at it a bit differently. “Microsoft is trying to say that they have a redundancy they have built in their own cloud, and they are offering it as a service at a fraction of the cost of something like Veeam,” Turner said. “They are positioning it as a line item that’s available if somebody is sophisticated enough to ask for it.”

As for Sadaunichy, he said Lyreco Group plans to stick with Veeam for now. “Microsoft has a good name but not yet a reputation for doing backup well,” Sadaunichy noted. “Veeam, Rubrik, Commvault, and others have been doing this for some time and have a proven record.”



“

Microsoft has a good name but not yet a reputation for doing backup well

Aleh Sadaunichy
network and architect manager, Lyreco Group

At the same time, Sadaunichy noted that it could be an interesting opportunity for some companies in the future to switch to Microsoft backup directly. The decision might ultimately come down to factors such as pricing and brand reputation, he suggested.

Harden the Platform

If an organization can't invest in a third-party backup product, it's especially important to harden and optimize the security of Microsoft 365 as much as possible, while also monitoring the platform's integrity over time. Establishing clear conditional access policies is key, Turner said.

Turner recommended using the Cyber & Infrastructure Security Agency's Secure Cloud Business Applications (SCuBA) reference architecture to ensure maximum security. Other resources include free downloadable toolkits (like this one) that offer penetration tests to pressure-test and establish the right level of telemetry.

"If you have tuned and hardened your 365 environments correctly and taken the right hygiene steps, the number of times you'll actually have an outage or ransomware situation should be very low," Turner said. "There are very good controls inside the Microsoft ecosystem to reduce the likelihood of massive outages."

Also, be smart about managing your user content, Bertrand warned. Even when employees leave the organization, there may be emails and backups that require retention due to potential legal rediscovery later on.

About the author

Karen D. Schwartz is a technology and business writer with more than 20 years of experience. She has written on a broad range of technology topics for publications including CIO, InformationWeek, GCN, FCW, FedTech, BizTech, eWeek and Government Executive.

0 COMMENTS

RECOMMENDED READING

How a University Evolved Its Disaster Recovery Strategy Over the Years
AUG 28, 2023

Achieving Data Immutability in a Backup and Recovery Strategy
AUG 21, 2023

A Look at Park 'N Fly's Cloud Backup and Recovery Journey
APR 07, 2023

A Switch from Datto to Redstor Backup and Disaster Recovery
MAR 01, 2023