druva

Five reasons why OneDrive endpoints **need third-party data protection**

Introduction

Many organizations think that Microsoft OneDrive, an electronic file sync and share (EFSS) tool, provides "good enough" backup and restore capabilities for their enterprise data. But it's a risky misconception. OneDrive is purpose-built for EFSS, just as third-party data protection solutions are purpose-built, from the ground up, to reliably protect all the data on a user's endpoint device.

Relying on OneDrive for data protection can expose your organization to substantial risks:

- Jeopardy from employee turnover and insider threats
- Threat of device loss, theft, and corruption
- Uncertainty of accidentally losing intellectual property
- Vulnerability to ransomware — and other malware
- Liability of inadequate legal hold, eDiscovery and, regulation compliance

For data protection in OneDrive environments, a third-party, enterprise-grade solution is essential.

Employee turnover and insider threats

A departing colleague, wanting to be responsible, may “clean their desk” by bulk-deleting what they think of as voluminous old and unnecessary files. Another employee or rogue admin, this one quite angry, may maliciously bulk-delete whatever important files they can access. Due to OneDrive’s inherent collaboration features, both have access to primary (their own files) and secondary (OneDrive-Shared drive) data.

If co-workers discover this loss reasonably quickly, they can search through the Recycle Bin for recent versions of individual files. Bulk recovery by IT isn’t an option. But if it’s discovered outside the Microsoft data retention window or after IT has decommissioned the user’s account, the data is gone.

If the data protection solution includes anomaly detection, it can alert IT to an insider attack and pinpoint when it occurred, speeding the restore process.

This risk doesn’t exist with the right third-party data protection:

- Unlimited data retention periods eliminate recovery limits and extra costs.
- End-users cannot delete or alter backup data, regardless of whether they owned or shared the files.
- In minutes, IT can centrally bulk-recover pristine data regardless of how it was lost.

Device loss, theft, and corruption

Users misplace endpoints regularly, and laptop and smartphone theft is rampant. The cost of the endpoint is one thing. The cost of losing locally stored data, the hours and days of productivity that went into it, is probably much more. But the cost of a data breach can be astronomical. You can't recover the data with OneDrive, and you can't remotely wipe or encrypt the data.

Likewise, if a device is damaged or severely corrupted, IT needs to quickly provide the user with a replacement that's up-and-running with the same systems, applications, and content. Even for any data stored on OneDrive, it doesn't support IT-led bulk-recovery — the end-user has to find and replace content file by file.

Importantly, a dedicated data protection app also collects metadata needed for potential investigations, forensics, and compliance requirements.

With an actual data protection solution (as opposed to a file-sharing productivity app), IT can:

- Protect all endpoint data, in or out of OneDrive folders — enabling fast bulk-restores.
- Remotely delete or encrypt data — protecting against breaches.
- Restore the entire contents of a lost or stolen device to a brand new device — end-users regain productivity right away.

Accidental loss of intellectual property

The upside to OneDrive file sharing is the ease of collaboration. The downside is the ease of overwriting or deleting someone else's work. If changes aren't discovered within the OneDrive retention window, data may be lost forever. Another vulnerability is OneDrive's use of designated folders. Endpoint system files, applications, persona settings, and other data located outside the OneDrive folder simply isn't backed up. OneDrive files are also subject to size and pathname limitations — large presentations and media files may be unprotected.

OneDrive relies on end-users to maintain configuration parameters, and if they intentionally or inadvertently change them, IT won't be alerted to the potential loss of IP. Another risk is from end-users having access to both primary (desktop) and secondary (Shared drive) storage, a significant vulnerability.

Additionally, data reliability and storage consistency checks built into third-party data protection can prevent file conflicts and sync errors that cause data corruption, duplicate versions, and data loss.

Overcoming these limitations requires a solution that offers:

- Unlimited data retention of clean snapshots so data is never lost.
- Automatic protection of endpoints that is centrally managed and configured by IT; end-users cannot alter backup data.
- Flexible data recovery options ranging from single-file to bulk restores, in-place or to another device, performed by end-users or IT.

Vulnerability to ransomware

Given the enormous number of attacks from ransom and other malware, some will eventually succeed. If enterprises can restore pristine backups, no ransom needs to be paid, but the loss of productivity can be significant. Whatever time it takes to find uninfected file versions and restore them — typically a business continuity SLA — costs both IT and the end-user. If there are no pristine versions because of data retention limitations or because files are outside OneDrive folders, data may be lost forever.

OneDrive does not support IT-led bulk-recovery of data from pristine, "point-in-time" snapshots. End-users can hunt for individual, uninfected versions, but simply because it's a file sharing app, a OneDrive environment is more vulnerable to cross-contamination, even within Recycle Bins.

Another important consideration is data protection that integrates automatically with security and incident response tools such as ServiceNow and Splunk. This can substantially speed getting end-users back to work.

A successful defense against ransomware includes:

- AI-based anomaly detection that alerts IT to unusual file activity, helps identify corrupt files, and assists pinpointing exactly when an attack occurred.
- Full backup-data isolation, abiding by the 3-2-1 industry standard: two copies on different storage media and a third on an offsite platform — vs. maintaining all versions within the Office365/Azure environment.
- Fast, bulk-recoveries of entire datasets from snapshots not subject to retention limits.

Legal hold, eDiscovery, and regulatory compliance

The most expensive Office365 editions and Microsoft add-ons offer some legal hold and eDiscovery features. However, OneDrive alone does not and any Office365 solution requires saving files in specific OneDrive folders. For departing employees' data that is often critically important for legal hold and compliance analysis, OneDrive provides no support once an employee's account is deleted.

The lack of fast and easy bulk restores from point-in-time snapshots, inherent to any Office365 solution, has a special impact for legal hold and eDiscovery. Successfully navigating through legal actions demands immediate access to all enterprise data, wherever it was originally located and whenever it was generated. OneDrive and Office365 are productivity apps and were simply not designed for this.

Top third-party data protection apps can preserve data with relevant Department of Justice-recommended metadata to help ensure immutability and include chain-of-custody reporting per Electronic Discovery Reference Model (EDRM) standards.

With data protection designed for legal and regulatory compliance, you can leverage:

- Privacy options for end users that prevent administrators from viewing or accessing data sets in accordance with corporate and regulatory practices.
- Richer forensic and investigatory data such as metadata and artifacts to detect and prevent data leaks and malicious activities.
- The ability to meet specific data residency compliance and retention requirements.

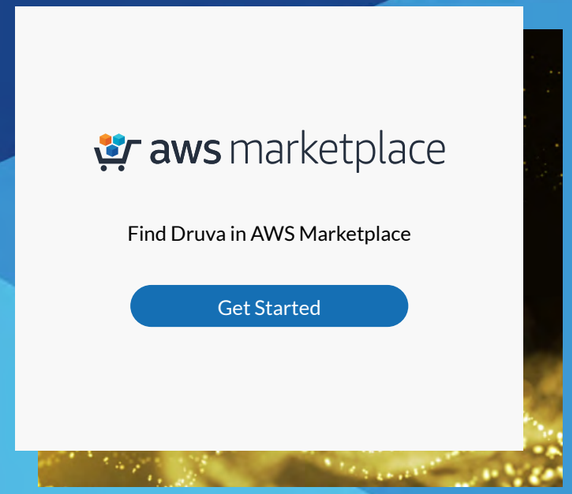
Choose the right data protection solution

Companies deploying OneDrive are getting a great EFSS tool — but they aren't getting enterprise-grade data protection. Microsoft itself is clear: "We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services."

The right third-party data protection solution ensures:

- If employees leave the company, endpoint data is backed up, and that if departing bad actors burn bridges, they can't burn data too.
- All enterprise data on laptops, smartphones, and tablets is safe regardless of device loss, theft, or data corruption.
- Intellectual property isn't lost despite accidental deletions, overwrites, or misconfigured OneDrive folders.
- Ransomware that may penetrate your defenses is no more than a brief nuisance.
- Compliance with all legal hold, eDiscovery, and regulatory requirements is comprehensive and reliable.

To learn more about this topic, visit: druva.com/products/saas-backup/.



druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.

Q420-20093