CrashPlan

Collaborative tools can't substitute for endpoint backup

Troubling Trend: Cloud collaboration platforms as backup

Cloud-based productivity suites and apps are surging into the enterprise mainstream. [1]Office 365 is used by more than 1 million organizations worldwide as of February 2022. Within this surge, businesses are officially adopting OneDrive to drive collaborative productivity. Similar trends can be seen with expanding use cases for Box and Google Drive. In addition, the increased visibility of Cloud Collaboration Platforms (CCPs) tempts some businesses to consider replacing dedicated backup solutions with OneDrive, Box, or Google Drive in the name of efficiency. But, when it comes to data backup, relying on a CCP leaves the enterprise blind to much of the picture. As a result, you need more data visibility, administrative control, and recovery features to ensure the compliant and secure use of organizational data.

Why cloud collaboration platforms are not Endpoint Backup

CCPs and endpoint backup are two distinct solutions designed to solve two distinct problems. True enterprise endpoint backup is built to cover all endpoint data without user interaction—securing that data and enabling fast, reliable recovery. In contrast, CCPs are built to synchronize a specific, user-designated subset of endpoint data — the same features and functionality that define CCPs become their greatest liabilities when used instead of endpoint backup.

[1] https://www.statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country/#:~:text=Office%20365%20is%20used%20by,using%20the%20office%20suite%20software

The danger of substituting CCPs for endpoint backup

Many businesses are making the understandable-if-misguided calculation that OneDrive, Google Drive, or Box offer a “good enough” stand-in for backup. This decision leaves the business open to a wide range of risks that can be mitigated through backup.

Your data isn’t fully backed up.

CCPs don’t automatically cover all important user data. While users only want to share some files, enterprises expect backup to cover all data—every file, multiple versions, requiring users to save all files to the CCP with a policy-driven approach. However, an enterprise data protection strategy can’t hinge on error-prone human action.

Your data is MORE vulnerable.

A backup is intended to be a secondary copy of existing, working data. By using cloud storage as the “working” copy (even assuming redundancy within the cloud solution) you are reducing the steps between an error and data destruction. This is doubly true when it comes to recovery following a ransomware attack or other breach.

User productivity suffers.

In using cloud as both a sharing system and for backup, users are asked to adopt workflows which feel unnatural, necessarily slow their work, and introduce more opportunity for error. Your team should be able to spend time doing their jobs, not being concerned about roundtripping files.

You can’t meet compliance requirements.

CCPs allow external applications easy access to unencrypted data. This presents a point of entry for a determined threat actor. And, many CCPs give minimal configurability when it comes to data storage location. Expanding data-privacy and sovereignty legislation means that knowing where your users’ data is stored is a core compliance requirement.

You can’t restore data reliably.

CCPs are for real-time editing, syncing, and collaboration, and they have short recall windows from days to a few weeks for near-term version control. But the data is gone for good if an issue isn’t discovered in time—for example, accidental deletion of a file—and restoring en-masse to a given point is effectively impossible with a CCP.

Storage can be expensive.

Cloud storage usage racks up quickly. As CCP vendors move to consumption-based models instead of unlimited, what started as a benefit quickly becomes a liability. A better backup solution can save your organization by leveraging the efficiencies of secondary storage and by utilizing effortless deduplication and compression.

CCPs can't meet enterprise restore needs

CCPs	Endpoint Backup
Ransomware Recovery	**Ransomware Recovery**
⊗ Limited file recovery	✓ Guaranteed file recovery
⊗ No mass point-in-time restore option	✓ Immutable data storage
⊗ Auto-sync spreads contaminated files to other users	✓ Compartmentalized data
	✓ Execute a full point-in-time restore
Data Migration	**Data Migration**
⊗ Manual backup: IT burden, data loss risk	✓ Automatic backup of all files
⊗ Unprotected user profile/device settings	✓ User-driven, full system restore capability
	✓ All user settings saved and migrated
Legal Hold + E-Discovery	**Legal Hold + E-Discovery**
⊗ Limited version and deleted file retention	✓ Customizable version and deleted file retention
⊗ No ability to preserve files not stored in sync directories	✓ Preserve-in-place functionality
	✓ No end-user interaction required

Do more with endpoint backup

Automatic, continuous backup: Protect all enterprise data

Automatic backups eliminate the human risk-factors of manual backups, and do so in the background, without impacting user productivity. Because endpoint backup is continuous and conscious of version retention, endpoint backup allows IT and end users to restore files to nearly any point in time.

Complete IT visibility and control: Reduce time spent on administration

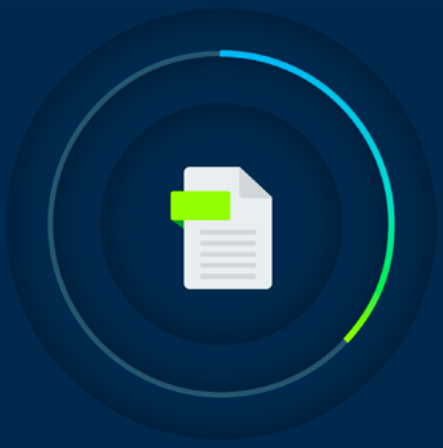
A single administrator can manage all end users from a single console, with complete visibility of all endpoint and cloud services data. This enables IT to spend less time and resources responding to the same preventable issues and focus on larger strategic initiatives.

Comprehensive, effortless data security: Fight cyber threats

End-to-end encryption protects an enterprise's most sensitive and valuable data as it moves from endpoints and is stored securely in the cloud. On-premises key management gives the enterprise full control over its data and enables compliance with strict data security regulations.

Robust restore functionality: Get back to work faster

The ability to execute full-system, point-in-time restores dramatically speeds the data recovery workflow and reduces IT and user burdens. This means users return to work faster—mitigating the productivity impact and cost of a device failure or cyber attack.



Dedicated endpoint backup is essential to business continuity and resiliency

As the business world continues to take full advantage of cloud-based productivity applications, it is easy to be tempted to shoehorn CCPs into the role of endpoint data backup. But the inherent limitations of doing so lead to serious business costs. With a true endpoint backup solution in place, enterprises can work to maximize the potential of cloud-based file sharing and collaboration while ensuring comprehensive data backup, data security, and guaranteed data restores which lay the foundation of a robust business continuity plan.

CrashPlan

crashplan.com

CrashPlan® enables organizational resilience through secure, scalable, and straightforward endpoint data backup. With automatic backup and customizable file version retention, you can bounce back from any data calamity. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds. So you can work fearlessly and grow confidently.

For more information, visit **crashplan.com**.