Why Collaborative Tools Do Not Equal Endpoint Backup

CrashPlan

OVERVIEW

Sharing Isn't saving: The Truth About Collaborative Tools

As enterprise productivity and hybrid work models have pushed companies to increasingly rely on cloud-based collaboration products, some have tried replacing their dedicated data backup solution with a cloud collaboration platform (CCP) like Microsoft OneDrive, Google Drive or Box. For accessing files and collaborating with colleagues in the cloud, these tools continue to be a preferred platform for many business users. But when it comes to data backup, relying on a CCP leaves the enterprise blind to much of the picture. Designed to enable real-time sharing of a small subset of files, OneDrive fails to back up all enterprise data. As a result, you lack the data visibility, administrative control, and recovery features necessary to ensure compliant and secure use of organizational data.

Troubling Trend: Cloud Collaboration Platforms as Backup

Cloud-based productivity suites and apps are surging into the enterprise mainstream. **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—leveraging "free" access to OneDrive offered through Office 365. Similar trends can be seen with expanding use cases for Box and Google Drive. The increased visibility of CCP tools tempts some businesses to consider replacing dedicated backup solutions with OneDrive, Box or Google Drive in the name of efficiency.

Why Cloud Collaboration Platforms Are Not Endpoint Backup

CCPs and endpoint backup are two distinct solutions designed to deliver two distinct outcomes. True enterprise endpoint backup is built to cover all endpoint data—securing that data and enabling fast, reliable recovery. In contrast, CCPs are built to cover a specific, user-designated subset of endpoint data—and to enable seamless sharing of that data. The very features and functionality that define OneDrive become its greatest liabilities when used in place of endpoint backup.

DESIGNED WITH THE END IN MIND

Cloud collaboration providers like Microsoft OneDrive, Google Drive, and Box make it easy for people to share and edit files, not recover all their data.

THE LIMITS OF "FREE & UNLIMITED" STORAGE

While OneDrive touts free, unlimited cloud storage, the reality is this storage is not built for a true enterprise endpoint backup use case. Without the data deduplication and compression functionalities of backup, storage adds up quickly. In practice, businesses will quickly hit the hidden limits of "unlimited" storage—typically 1 TB per user—and be forced to pay for added storage capacity. Another problem of data backup without deduplication or compression: in a perfect scenario, users would be transmitting all their files across the network every 15 minutes. Just imagine the bandwidth burden.

Comparing CCPs and Endpoint Backup

ONEDRIVE

Share Some Files	Open Sharing	Full User Control	Moving Files Forward
User-dependent uploads	Convenient, frictionless access	Enable efficient collaboration	Real-time editing of most-current version

ENDPOINT BACKUP

Share All Files	Maximum Data Security	Full IT and Security Control	Going Back
✓ Automatically back up every file, every version	✓ Secure sensitive and valuable data	✓ Visibility into endpoint and cloud services data	✓ Recovering files quickly and reliably

DATA VISIBILITY IN CCPS

While CCPs are not a substitute for endpoint backup, they remain a great tool for collaboration. Nevertheless, it is critical to have visibility into file events on the service, as well as endpoints. If your organization uses OneDrive, Google Drive or Box, consider a digital forensics solution that can detect when and where files are moved to personal cloud storage accounts and external storage devices.

The Disastrous Consequences of Substituting CCPs for Endpoint Backup

Unfortunately, many businesses are making the misguided calculation that OneDrive, Google Drive or Box offer a “good enough” stand-in for endpoint backup. In doing so, a business opens itself to a wide range of risks that can have potentially disastrous consequences.

01 **Your data isn’t fully backed up** - At the most basic level, CCPs fail as an endpoint backup solution because they doesn’t automatically cover all user data. That’s because if OneDrive housed a user’s entire data store, co-collaborators would have to tediously search through folders to find the relevant file. To ensure that only the most relevant files are shared, OneDrive and CCPs like it make file sharing entirely manual and user-dependent. But while users only want to share some files, enterprises expect backup to cover all data—every file, every version.

Patching this gap by requiring users to back up all files to OneDrive is a poor approach. An enterprise data protection strategy can’t hinge on human action—half its purpose is to protect against error prone, unreliable users.

02 **User productivity suffers** - User-dependent backup also impedes productivity. The U.S. Chamber of Commerce recommends backup intervals where the business could recover if data was lost in the interim. For some industries, once every 24 hours might be an acceptable interval, but experts agree that once every 15 minutes is ideal. Imagine the productivity impact of requiring users to stop what they’re doing to manually back up all their data to a CCP four times per hour.

03 **You can't restore data reliably – or efficiently** – CCPs are built for real-time editing and syncing for collaborative productivity. But this relentless push forward is the opposite of data backup's most critical functionality: the ability to revert versions. This increases the risk of data loss from simple user error. For example, if an end user accidentally deletes a file from the shared space, it is deleted for all users. OneDrive has short recall windows—from days to a few weeks—but if the error isn't discovered in time, the data is gone for good. Other CCPs have similar issues. Without comprehensive backup, restores are limited to files manually shared by users—and only the most recent versions, at that. In a total recovery situation—a lost or stolen device, hardware failure or ransomware—this dramatically increases the risk of permanent data loss. Finally, because CCPs aren't built to enable efficient data restores, restoring whatever data was manually backed up is a time-consuming and costly process. There is no bulk or point-in-time system restore capability—only file-by-file restores. This is tedious in even a single-user scenario, but the burden grows exponentially for a large-scale restore—or when you consider a large enterprise's typical annual restore volume.

04 **Your data is highly vulnerable to attack** - Yet another elemental data security feature lacking from CCPs: comprehensive encryption. While OneDrive touts advanced encryption of the data stored in the shared cloud, it does not protect or encrypt this data as it moves to and from the cloud. This leaves enterprise data vulnerable to attack from outsiders, who no longer need to hack into the secure cloud—they can simply attack less-secure network channels and intercept the unencrypted data. Another problem with OneDrive encryption: it does not enable the enterprise to manage its encryption keys. This limits enterprise data control, opens the possibility of blind subpoena and may conflict with data security compliance requirements. Box and Google Drive offer encryption at rest and in motion, but may still fall short of business requirements.

05 **You can't meet compliance requirements** - The managed encryption key issue is just one of the compliance challenges of the OneDrive as backup approach. OneDrive also allows external applications and third-party support services, such as content indexing, to access unencrypted data—violating the data security regulations governing many businesses.

Additionally, OneDrive doesn't allow their enterprise customers to choose where their data is stored, making it extremely difficult to comply with growing data residency regulations. Complicating this issue, OneDrive offers local storage, but ultimately leverages a central data repository in a separate location. This means that data that is initially stored locally may, at some point, be transmitted outside the region or country, violating data residency regulations.

Mapping Shared Drives is a Nightmare Scenario

Attempting to replicate a traditional, on-premises shared-drive environment, some businesses have tried mapping their shared drives to CCPs. This approach has proven extremely difficult to implement. Migrating what can be years of data is complex, both from the perspective of making sure only relevant files are migrated, and that applications that currently source data from a shared drive continue to work. This not only creates a nightmare of IT time and costs—it leaves a high likelihood of holes or gaps in the mapping process. Moreover, this approach still depends entirely on users to manually save all files and all versions—the most fundamental flaw in effective data backup.

The Critical Differences of True Endpoint Backup

Enterprise technology experts and industry analysts like Gartner agree that CCPs should never be used in place of a dedicated endpoint backup solution. Unlike OneDrive, Google Drive, or Box, true endpoint backup solutions are built to provide IT with complete data visibility and—above all else—guarantee data recovery in a wide range of scenarios. The essential features and functionality of true endpoint backup solve critical business challenges.

CCPs Can't Handle Enterprise Restore Needs

RANSOMWARE RECOVERY

CCPs	Endpoint Backup
✕ Limited file recovery	✓ Guaranteed file recovery
✕ No point-in-time restore option	✓ Quarantine the system
✕ Auto-sync spreads contaminated files to other users	✓ Execute a full point-in-time restore
✕ Tedious, file-by-file manual restore	✓ Never pay the ransom

DATA MIGRATION

CCPs	Endpoint Backup
✕ Manual backup: IT burden, data loss risk	✓ Automatic backup of all files
✕ File-by-file manual restore	✓ User-driven, full system restore capability
✕ Unprotected user profiles/device settings	✓ All user settings saved and migrated

LEGAL HOLD + E-DISCOVERY

CCPs	Endpoint Backup
✕ Limited endpoint visibility to data stored in specified location	✓ Complete endpoint visibility
✕ No ability to lock down files not stored in specified location	✓ Preserve-in-place functionality

Automatic, continuous backup: Protect all enterprise data
Automatic backups eliminate the human-factor risks of manual backups, and do so in the background, without impacting user productivity. Because endpoint backup is continuous, endpoint backup allows IT and end users to restore files to nearly any point in time.

Complete IT visibility and control: Mitigate insider threats
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 monitor high-risk user activity and mitigate the risk of insider threats, whether accidental or malicious.

Comprehensive, enterprise-grade 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 of 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 both IT and user burdens. Whether recovering from ransomware or hardware failure, or managing data migration for tech refresh, this means users get back to work faster—mitigating the productivity impact and cost.

Dedicated endpoint backup is essential to business continuity

As the business world rushes to take full advantage of the potential of cloud-based productivity applications, some are tempted to shoehorn CCPs into the role of endpoint data backup. But the inherent limitations of doing so can lead to serious business costs. Experts, business leaders and even OneDrive agrees that it cannot—and should not—be used as a substitute for dedicated endpoint data backup. With a true endpoint backup solution in place, the enterprise can work to maximize the potential of cloud-based file sharing and collaboration, while ensuring the comprehensive data backup, data security and guaranteed data restores that lay the foundation for business continuity.

CrashPlan

Corporate Headquarters
400 S 4th St Suite 410
PMB 31083
Minneapolis, MN 55415-1419
612.464.2112

crashplan.com

CrashPlan® provides peace of mind through secure, scalable, and straightforward endpoint data backup. We help organizations recover from any worst-case scenario, whether it is a disaster, simple human error, a stolen laptop, ransomware or an as-of-yet undiscovered calamity. We continue to innovate as the landscape of work evolves, which makes CrashPlan foundational to organizations' data security. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds.

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