eBook

Axcient

MSPs Must Plan to Backup, Search, Restore, and Audit Productivity Suite Data

FOUR KEY FEATURES FOR UNINTERRUPTED BUSINESS CONTINUITY THROUGH ROCK-SOLID RECOVERY OF MICROSOFT 365 AND GOOGLE WORKSPACE DATA

Your BC Plan

The combination of **rising ransomware attacks,** remote workers, and a heavy reliance on collaboration tools like Microsoft 365 and Google Workspace has created a potential perfect storm for MSPs and a **perfect scenario for hackers.** MSPs are juggling the risks of limited retention, human error, and complete downtime while bad actors find open door after open door. Access to data from anywhere is vital for today's hybrid work environments, but without third-party backups through comprehensive **business continuity** and **disaster recovery** (BCDR) plans, MSPs and their SMB clients' data is in danger.

How confident are you in your ability to recover lost or stolen data in Microsoft 365 and Google Workspace? This eBook highlights four features for uninterrupted business continuity that also provide rapid and reliable recovery.

Consider these questions about your current solution before reading on…

- → **How long does it take** to locate lost data and restore it for client access?
- → **What is the cost** to clients for data storage, including overages and over-provisioning? How do those fees impact your relationship with clients?
- → **Are you able to meet long-term compliance** requirements? If so, what does the management and technical time cost? If not, have you lost clients because of it?
- → How do you recover if a client is **hit by ransomware or accidental data deletion?**

Axcient

Business Continuity Requires Backups; You Can't Have One Without the Other

Microsoft's Services Agreement

While Microsoft 365 does provide business enablement tools for collaboration and data access anywhere – they do not provide data loss protection. Many assume that a brand like Microsoft includes safeguards against today's most pressing cybersecurity issues, but it's just not their thing. This fact is clearly stated in **Section 6b of the Microsoft Services Agreement.**

Microsoft 365 has a limited 14-day retention period for deleted data or 30-days with special configuration, but **56%** of breaches go unnoticed for months. Even with accidental data deletion – a common problem within collaboration tools – businesses commonly go long periods before anyone realizes a critical file or folder is missing. Maybe an old employee's account is deleted, someone decides to "clean up" shared folders or a clever phishing attack gives hackers internal system access. However it happens, human error remains the **number one** cause of data loss and requires proactive protection to ensure **true business continuity.**

"We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."

Table of Contents

Google Workspace Terms of Service

Many MSPs have clients who use Google Workspace, and Google has known vulnerabilities. Google Drive can replicate rogue files already in a filesystem using Google's Backup and Sync tool. In 2019, **Google acknowledged a vulnerability** in its Chrome OS "built-in security key" feature.

And around the same time, hackers launched a phishing attack that used Google Drive and Google Docs to disguise emails and embed malware links, according to **Forbes.** In that case, the malicious actors were able to fool employees and bypass security measures configured to protect email.

In Google's **Terms of Service,** it does not take liability for data loss.

Proactive protection for your clients must include backups of Microsoft 365 and Google Workspace data. Without those, you cannot promise clients that they will be able to keep their business running no matter what – and that's your job as an MSP.

"The only commitments we make about our services (…) are (1) described in the Warranty section, (2) stated in the service-specific additional terms, or (3) provided under applicable laws. We don't make any other commitments about our services."

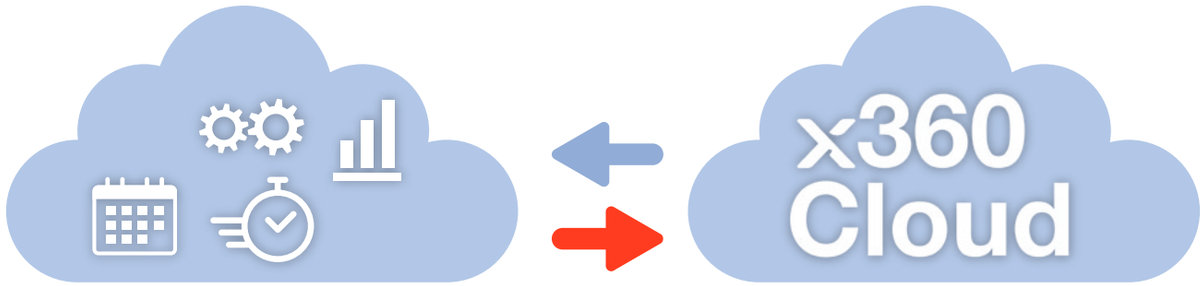
Axcient

If You Think Microsoft and Google Backup Are Sufficient – Think Again.

Sure, Microsoft and Google do provide some of their own backup tools, but the whole reason third-party services are recommended is to avoid complete downtime. When an MSP allows a client to backup business-critical data to the same cloud where their data is stored, the MSP can't deliver business continuity. At that point, it's out of the hands of the MSP, and clients are relying solely on Microsoft or Google.

The problem here is that during infrastructure outages, backups go down too, which means business comes to a screeching halt. And if you think these cloud providers are too big to go down, or it never happens, listen to Microsoft's own words, "all online services suffer occasional disruptions and outages." Microsoft 365 has suffered a worldwide service outage that spanned over **9 hours,** and Google was down for approximately **6 hours** during one of their global outages. Can your clients afford to be without email, contacts, calendars, and work documents for hours at a time?

Data loss happens, even in the cloud and even to the biggest cloud providers out there, but with proper business continuity in place, businesses don't have to suffer.



Backup, Search, Restore, and Audit with x360Cloud for Microsoft 365 and Google Workspace

Axcient **x360Cloud** gives MSPs and their clients the Microsoft 365 and Google Workspace backups necessary for uninterrupted business continuity – even during cloud outages. It can automatically discover, backup, audit, search, and restore critical data in Microsoft 365 (Exchange, Mail, Calendar, Contacts, OneDrive, and SharePoint) and Google Workspace (Gmail, Calendar, Contacts, Drive, Sites, and Shared Drives). Data is backed up to the encrypted, tamper-proof **Axcient Cloud** with access verified, logged, and protected through multi-factor authentication.

The comprehensive x360Cloud solution includes the following four unique features; built-in, always-on, and created specifically for MSPs and their SMB clients:

View the x360Cloud Data Sheet

Table of Contents

01 SmartSearch

Search more than 100 million objects in less than 5 seconds – including email attachments, files, folders, document libraries, historical snapshots and version history, and throughout communications.

MSPs can perform micro or macro-level restores with full-text search across data sources and multiple users, along with rich filtering capabilities. Single-click, point-in-time, or specific version restores are fast and secure to keep clients moving.

Depending on the data loss scenario, infrastructure, or external requests, data can be exported in two different ways:

- **Export to a folder to satisfy e-discovery requests**
- **Export immutable audit logs and granular backup reports for third-party auditing**

Learn How x360Cloud SmartSearch Works

Axcient

02

Pooled Storage and Secure Retention

At Axcient, we're transparent about our robust storage and long-term retention features. We cover multiple use cases, high volumes of data (C drive, D drive, etc.), and there aren't restrictive data limit tiers or hidden caps.

With Axcient data pooling is allowed, retention times aren't restrictive, and our **flat cost pricing is per-device or per server.** There aren't any surprises, monthly fees, or over-provisioning - something both MSPs and their clients love to hear.

We do it with our proprietary and **patented Chain-Free technology** that frees MSPs from legacy, chain-based backups. Data is stored in a native virtualized state with a pointer array algorithm, so each recovery point is independent. When corruption occurs, bad data blocks are isolated and independently deleted without risking the integrity of the backup dataset. Previous backups can be recovered without disrupting new incremental backups or post-corruption data.

We created our Chain-Free technology specifically for MSPs to simplify backup management and a lower total cost of ownership by removing a lot of unnecessary fluff.

- → **No data loss**
- → **No data bloat**
- → **No wasting time or storage with new chains**
- → **No reseeding**
- → **No surprise cost overages or fees**
- → **No large storage space requirements**
- → **No over-provisioning "just in case"**

Learn How Axcient Delivers Pooled Flat Fee Data Storage

03 Certification and Compliance

Chain-Free technology also helps MSPs ensure long-term compliance for clients in highly regulated industries like healthcare, government, and legal and financial services.

No chains means no time constraints on how long you can backup data. MSPs can easily meet three, five, seven, or even 10-year retention periods. Even if some backups are lost due to corruption, no data is lost because each Chain-Free backup is independent of other backups. Corrupt pieces can be isolated without affecting any other backups.

As additional layers of security, and in order for MSPs to satisfy the compliance needs of clients in specific **verticals,** Axcient is SOC 2 certified, and x360Cloud can help organizations meet requirements for the following regulations:

- → **The Health Insurance Portability and Accountability Act (HIPAA)**
- → **The Federal Information Security Management Act (FISMA)**
- → **The Financial Industry Regulatory Authority (FINRA)**
- → **The General Data Protection Regulation (GDPR)**

Video: Why You Should Care How Your Backup Works

04 AirGap

This anti-data loss technology separates data deletion requests from the actual mechanics of deletion.

So even when data has been deleted – whether by accident or by bad actors in a ransomware attack – there is a saved and protected snapshot of your data that can be restored from a protected archive. When deletion requests are created, verified, and executed, time gaps give MSPs time to detect and stop malicious activity. "Honeypots," or fake signals, give hackers the illusion that they've successfully deleted data – so they stop pursuing corruption – but in reality, the data is stored in an isolated archive.

Additional layers of security include the following:

- **Human factor controls** limit the number of authorized individuals who can create deletion requests within the Axcient organization. This group of individuals is separated from another authorized group of individuals who are responsible for actually fulfilling deletion requests.
- **Human two-factor authorization** is required through audible confirmation to verify deletion requests. So if a hacker attempts to delete data – and phone, email, and support systems are compromised – the deletion request won't be processed without audible approval.
- **Third-party testing** by independent security management companies, FRSecure and Core Security, prove that data backed up in AirGap cannot be deleted.

View the Axcient AirGap Technology Overview

Axcient

Are You Ready to See How x360Cloud Delivers Business Continuity?

See how x360Cloud and Chain-Free technology compares to your current Microsoft 365 and Google Workspace Backup. It might be time for a change.

Schedule Your 1:1 Demo

Get a Free 14-Day Trial

About Axcient

Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 3,000 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202
Tel: 720-204-4500 | axcient.com

Axcient