Axcient

Making Fast Recovery Reliable, Affordable, and Simple with Direct-to-Cloud BCDR

Business Continuity and Disaster Recover in One Platform to Protect Everything™

axcient.com

Introduction

Given widely dispersed data, hybrid infrastructures to protect, and ever-growing numbers of cyberattacks, MSPs are challenged to deliver effective data protection solutions to their clients. The result has been MSPs increasingly burdened with multiple backup and disaster recovery solutions for multiple use cases. At the same time, reducing overhead and simplifying operations are required for MSP profitability and growth. This market needs a unified business continuity and disaster recovery (BCDR) platform that enables MSPs to secure data and ensure rapid recovery while boosting the bottom line.

This whitepaper explores how the Axcient x360Recover business continuity and disaster recovery (BCDR) solution–and its Direct-to-Cloud (D2C) capability in particular—simplifies data protection across all of today's varied use cases. With a single solution, MSPs can elevate their capabilities beyond just backup, and ensure reliable and rapid recovery and protection against cyberthreats like ransomware—all while building a scalable and profitable business.

Rising Security Risks and The Burden on MSPs

Before the pandemic, cyberattacks rose in sophistication and frequency each year. However, dispersed remote endpoints, unsecured network connections, and novice at-home tech users opened the door for new and novel attack strategies during COVID-19 stay-at-home orders. Since then, the spike in ransomware and phishing attacks on small- to medium-sized businesses (SMBs) and MSPs continues to rise.

- **70%** year over year increase in the number of cyberattacks on MSPs and ISPs.
- **50%** of ransomware demands are more than $50,000.
- **40%** of attacks require more than 8 hours to address – typically at a cost of $100 - $250/hour.
- **80%** of businesses that pay the ransom suffer a second ransomware attack, often by the same threat actor group.
- **54%** of MSPs say ransomware attacks are caused by phishing emails, 27% by user practices/gullibility, and 26% by lack of cybersecurity training.

SMBs are increasingly targeted, the hard costs and lost productivity are enormous, and the cause is mainly human error. Today's cybersecurity landscape demands that MSPs must assume data loss is inevitable and provide the technology, support, and proactive protection necessary to keep businesses moving after an attack or data loss incident.

Right-sizing BDR Deployments

Backup and disaster recovery needs vary from client to client. For smaller, cost-conscious clients, an onsite BDR appliance is often overkill. The BDR appliance is expensive, whether purchased or leased, and needs to be amortized over several years and then refreshed at the end of its effective life. Smaller clients may not need or value the ability to do onsite recovery and server virtualization, so the extra costs of the appliance are often wasted. These costs can add up when an MSP has dozens of smaller clients, jeopardizing recovery times in the event of a total failure. Cloud-based recovery is the right-sized and preferred approach for these deployments to defend against hardware failures, ransomware infections, or site-wide disasters.

With the growth in SaaS apps, only a few mission-critical servers may still be on-premises. For these clients, a BDR appliance onsite is often not needed, and a cloud-only approach best supplies data protection and business continuity. In cases where a cloud recovery might take too long, a rapid recovery leveraging an encrypted Local Cache offers speed without a full appliance's management and investment burden.

The traditional BDR deployment model is still ideal for the rest of an MSP's clientele. An on-premises BDR appliance serves as a backup target and resource for onsite recovery and cloud-based recovery as the last line of defense. The reality is that MSPs should tailor their deployments to their various client segments' unique needs and budgets while putting their security and ability to recover first.

New Realities for Endpoint Protection

While server protection requires a tailored approach, nearly every sized client now has a more significant need for endpoint protection. The COVID-19 pandemic fundamentally altered the business landscape, and remote and hybrid work environments are here to stay. Companies of all sizes are reorganizing their real estate footprints, rethinking in-office staffing models, and embracing remote work for the long haul. Moreover, many employees now prefer a remote employment model, and savvy companies adapt to this new reality in the war for talent.

The end result is more business-critical data stored on more remote endpoints. As a result, individual workstations and laptops are more vital than ever and need not just data backup, but Chain-Free, image-based backup protection for rapid recovery. With a vast increase in remote endpoints, the threats from ransomware infections, loss, and theft are the greatest security risks facing MSPs and their SMB clients. Whether a far-flung executive's laptop or a solitary engineer working from a critical workstation, remote endpoints are the new potential Achilles heel in a company's IT infrastructure.

Deployment Options: Appliance Versus Cloud BCDR

The extensive range of data protection use cases puts extraordinary pressure on MSPs. As a result, MSPs must be agile and examine deployment considerations when deciding whether to use traditional appliance-based backup versus hardware-free backup. Axcient's BCDR solutions provide MSPs and their clients choice and flexibility. Our all-in-one x360Recover solution allows MSPs to meet nearly all client needs with just one vendor – endpoint backup, no-appliance BDR, turn-key BDR, and public or private cloud backup.

Appliance-Based BCDR is best…

- **When you need dedicated hardware on-site** for instant local failover of backed-up workloads.
- **When you need to continue local backups** even when the client's internet connection is down.
- **When you need to do local restores** even when the client's internet connection is down.
- **When you need to separate time of backups from time of replicating data to the cloud.**
- **When a client has low bandwidth,** or you need to do a physical seeding of cloud backups.
- **For protecting physical or virtual servers** that need dedicated on-site infrastructure for failover.
- **For protecting desktops in an office** where an appliance is already deployed to protect servers.

Consider these deployment components:

- **Appliance-based BCDR requires an appliance at each client site.** Use a turn-key Axcient appliance (USA only), other compatible x86 hardware, or a Hyper-V/VMware VM that can be deployed via a bootable installer ISO.
- **Existing x86 hardware (servers or desktops and some competitive BDR units) can be replaced to be an x360Recover appliance or vault.** Check the hardware compatibility list for supported hardware configurations and solutions.
- **Local recovery has no dependence on the Internet.** Zero data is downloaded for local recovery.
- **Local recovery is performed via the appliance web-based graphical user interface** (GUI) – which can be accessed via the x360 cloud portal, or locally via a web browser – or can also be performed via the Windows Recovery Center application.
- **Physical seeding of the initial backup is possible, but not required.** Incremental backups are replicated to the cloud even while a physical seed drive is in transit.

Direct-to-Cloud: BCDR Without the Local Appliance

x360Recover Direct-to-Cloud (D2C) hardware-free backup was created to protect remote endpoints without the expense, hassle, maintenance, onsite visits, and limitations of appliances. Chain-Free image-based backups are sent directly to the secure Axcient Cloud for quick recovery of anything from a single file to an entire system in just an instant. Created for today's remote environments, D2C protects employees from the risks associated with less sophisticated at-home infrastructures and public Wi-Fi connections.

Direct-to-Cloud is best...

- **For clients who don't want a dedicated turn-key appliance** because of cost or distributed IT.
- **When protecting virtual machines (VMs) in the cloud,** or in other cases when local backups are not desired, use D2C for Microsoft Azure to separate backups from the production infrastructure to avoid complete downtime.
- **When protected machines roam to different networks –** for example when endpoints are not on the same local area network (LAN).
- **For protecting servers when used with Local Cache –** an optional, fully independent D2C feature that pairs D2C with an inexpensive local USB or network-attached storage (NAS) device to substantially decrease recovery and failback times.
- **If cloud-based recovery is suitable for protecting servers without Local Cache,** or if it is acceptable for restore speeds to be limited by Internet speed.
- **For protecting desktops or laptops, with or without Local Cache.**
- **When you want to leverage existing devices –** including NAS devices, USB disks, and Windows-based BDR devices.

Consider these deployment components:

- **D2C doesn't take local backups separate from cloud backups.** An Internet connection is required for backups, and the backup speed is dependent on the Internet connection speed.
- **The initial backup could take days or weeks, depending on bandwidth.** D2C can run concurrently with the existing backup vendor or Windows backup until the initial backup is complete.
- **Fast local recovery from the Local Cache requires an Internet connection** to download the encryption key and recovery point indexes. More than 99.9% of data will come from Local Cache.
- **Instant local virtualizations require a local Hyper-V desktop or server to access Local Cache.**
- **If the client has no hardware for local virtualization,** we recommend keeping a spare 'recovery BDR' in your MSP office with Hyper-V preloaded that you can transport to a client needing recovery.

Direct-to-Cloud: Hardware-Free BCDR

With Axcient x360Recover Direct-to-Cloud (D2C), MSPs are discovering how to meet their clients' expectations while also building a profitable business. Axcient x360Recover D2C is built on the industry's only Chain-Free, image-based backup technology. MSPs can back up any server or endpoint without needing a local BDR appliance. x360Recover D2C backs up directly to the Axcient Cloud vault with a 15-minute recovery point objective (RPO) and one-hour recovery time objective (RTO). With D2C, MSPs can protect a wide range of systems and tailor their deployments to the business continuity needs of each client. Axcient partners can ensure rapid recovery with little to no downtime with these customizable options on a simple infrastructure. Additionally, always-on features enable cloud-based virtualization and file-based recovery, anti-ransomware technology that protects against data deletion, and automatic backup protection.

Protecting Every Endpoint

Moreover, D2C lets MSPs address the growing endpoint protection market requirement. Businesses must protect the data and the system configurations for laptops and workstations. Traditionally, most organizations only protected file-level data from corporate endpoints. Axcient D2C does much more by enabling Chain-Free, image-based backup for laptops and desktops. This capability delivers the ability to recover the file-level data from these endpoints and the full system configuration for virtualization or bare-metal restores. Fast and complete recovery is what MSP clients expect. Fortunately, with x360Recover D2C, it is easy for MSPs to add endpoint protection to every client deployment.

Remote Workforce Enablement:

> "Remote workers were the driving force for x360Recover Direct-to-Cloud. People have data literally all over the place in today's environment. We're trying to contain that. Being able to back up a whole laptop or desktop for remote users means that we have the entirety of their data in a worst-case scenario no matter where they are. Users can connect and work pretty much the same way they've been working no matter what."

– Phillip Long, CEO at Business Information Solutions (BIS)

One Platform with Advanced BCDR Technology

While D2C transforms the fundamental infrastructure of server and endpoint protection, the entire Axcient x360Recover platform is designed to deliver faster and more reliable business continuity. Axcient technologies – including Chain-Free backups, Virtual Office, AutoVerify, and AirGap – automate and simplify key BDR functions to ensure a secure and dependable business continuity solution. As a result, MSP technicians can master recovery, support, and service for end-to-end protection and rapid recovery with an all-in-one platform and solution, rather than a sprawl of different vendors. For MSPs looking to gain cybersecurity confidence and infrastructure simplicity, Axcient x360Recover is the solution of choice.

Built-In BCDR Features Make Both Deployment Options Beneficial for MSPs

Chain-Free backup technology eliminates the need for periodic or manual reseeding to dramatically reduce overhead.

Pooled storage for a flat fee provides predictable billing without even a chance of surprise overages or unexpected fees.

Patented AirGap anti-ransomware technology separates data deletion requests from deletion mechanics, so your data is always protected, even after a ransomware attack.

AutoVerify ends manual backup verification by automatically virtualizing and running numerous tests for data corruption, ensuring your data is always ready to recover.

Virtual Office enables self-managed disaster recovery with a minutes-long recovery time objective (RTO) and near-instant virtualization in the cloud.

Simple flat-rate pricing per protected machine per month + 30 free days per year per protected machine of cloud virtualization.

Why You Should Care About How Your Backups Work

Many image-based backup solutions today rely on chain-based technology to perform backups. With these solutions, if there is ever a corruption or deletion of one of the recovery points in the chain, the backup chain is essentially rendered inoperable. Corrupted backups can prevent a successful system recovery during a disaster or result in data loss scenarios. Chain-based backup technologies commonly utilize a rollup or consolidation process to simplify the chain dependencies, but in the process, cause data bloat on the local BDR appliance. MSPs are forced to provision larger appliances for these deployments or alternatively perform annual onsite maintenance visits to control data bloat. A new full backup is performed onsite and then reseeded to the off-site data center in this latter scenario. In all these circumstances, MSPs have to roll trucks and perform expensive onsite visits to maintain or repair backups because of the legacy chain-based backup technology. Chain-based backups also introduce the risk of corrupted backups, while dispatching techs and extra maintenance drive up labor costs and reduce an MSP's profitability.

Axcient x360Recover leverages proprietary Chain-Free backup technology. With Chain-Free backups, data is stored in a native virtualized state with a pointer-based array algorithm, so each and every recovery point is independent. There are no chain dependencies. A particular recovery point can either be deleted or corrupted, and recovery points before or after remain unaffected.

Chain-Free backup technology eliminates one of the most significant risks facing an MSP, namely, a corrupted backup job which prevents the rapid and complete recovery of a client's environment. What's more, Chain-Free backup is inherently more flexible and efficient in storage utilization. It is fundamentally a simpler and more efficient architecture, enabling worry-free storage and 30% greater storage efficiency and affordability compared to chain-based backup. With included pooled storage for a flat fee, MSPs can ensure long-term compliance, efficiently and easily manage backups, and provide security for all regardless of budget. There are no unnecessary truck rolls, no onsite maintenance visits, no base image requirements for restore, no consolidation, and no staging space. Chain-Free backup technology simply allows MSPs to deliver near-instant recovery with significantly less complexity and robust data storage.

Rapid Recovery With Simplicity:

> “The Chain-Free technology was one of the things that made me a lot more comfortable with Axcient. Effectively, the chain is just two pieces long: the most recent backup and the base image. That helps me sleep a lot better – knowing that I'm not dependent on 15, 20, or 35 files all working as they should in order to do a recovery. When it's crunch time, you don't want any of that uncertainty.”
>
> – Patrick Salt, Technology Architect at Digital Seattle

AutoVerify for Automatic Backup Integrity

AutoVerify is our patented automation technology that performs nightly BootVM checks, providing validation of the recoverability of backup snapshots. With x360Recover D2C, nightly BootVM checks are enabled for each protected system and will automatically boot the latest backup snapshot and perform AutoVerify operations to ensure that the recovered backup is healthy. AutoVerify extends the BootVM check functionality by automatically performing additional deep volume tests to check bootability, operating system health, data corruption, and file system and application integrity.

MSPs have traditionally relied on manual checks to verify the integrity of backups. The heart of the fundamental MSP value proposition is ensuring that backups are healthy and recoverable. No matter what happens in an IT environment, most MSPs position themselves as the client's first and last line of defense. Even if there is a site-wide natural disaster or massive cybersecurity incident, such as a ransomware infection, every MSP wants to wholly and quickly deliver on their mission of recovering the client's data and operations. Not surprisingly, therefore, MSPs have traditionally prioritized ensuring the integrity of their client backups. Axcient automates this process to eliminate the risks of human error and manual tasks. Proactive alerting prevents critical issue impacts by letting MSPs know about potential backup health issues before they become breaking points to business availability. Axcient AutoVerify automates vital integrity checks on a nightly basis and consolidates backup health reporting in the Axcient x360 Portal, enabling an MSP to manage by exception and proactively intervene only when problems are detected. With less reliance on manual operations, MSPs reduce the risk that something crucial to recovery is missed and threatens business continuity.

Backup and Recovery Confidence:

> “With technology like AutoVerify, we can rest easy knowing that Axcient has built-in protections for our clients' data. We have confidence in Axcient's solutions and appreciate that we have a vendor partner going the extra mile to ensure our clients' businesses are up and running if the worst happens.”
>
> – Paul Charles, CTO at Data Trends

AirGap Anti-Ransomware Technology

One of the greatest threats to businesses today is the plague of ransomware. Cybercriminals are relentless in their attacks on companies' data and operational integrity, especially SMBs. Just a few years ago, ransomware attacks were relatively simple to navigate. If a client had wisely invested in highly reliable backups, MSPs and their clients could avoid the need to pay a ransom by simply restoring from backups.

Unfortunately, today's attackers target backups, exploit long dwell times, and meticulously plan ransomware attacks with a high level of sophistication. Before unleashing the encryption, cybercriminals are upping the ante and deleting their victims' onsite and cloud-based backups in many incidents. In these scenarios, victims and their MSP providers are left powerless and pay the ransom even though payment doesn't guarantee complete data recovery.

Enter Axcient AirGap. This built-in, always-on x360Recover feature makes it nearly impossible for hackers to destroy a client's backups. With AirGap, when protected systems are deleted they are not immediately removed from disk storage, but are instead moved into the AirGap archive system. The protected systems are removed from the UI and any endpoint licenses are returned to the system. Deleted protected systems held within the AirGap are retained for several days before being purged by the cleanup process. This window of time is intended to provide partners with an opportunity to respond to potential attacks against their clients and ensure a successful recovery.

An MSP's reputation is one of its most valuable assets. If a client suffers a ransomware infection and their backups are also compromised, incalculable damage can occur to the brand and reputation. Axcient AirGap is yet another feature that increases the reliability of an MSP's backups and reduces risk, both for the client and the MSP's reputation. However, brands and reputations are not built overnight. Therefore, it only makes sense to prepare with the right technology so an MSP can keep its promises and its clients safe.

Virtual Office

As part of x360Recover, the Virtual Office feature lets MSPs self-manage cloud recovery for both single servers and an entire office. When a cyberattack, natural disaster, or other data loss incident occurs at a local office, Virtual Office can spin up multiple servers quickly and automatically using runbooks. Runbooks allow for proactive, disaster recovery pre-planning for up to 100 servers based on the desired configuration. Additionally, Virtual Office enables anytime disaster recovery testing to prove the value of BCDR to clients ahead of the real thing. Quarterly testing shows clients how their entire office – including every server, workstation, desktop, and laptop – can be virtualized in order of necessity to maintain business availability no matter what.

Local Cache

x360Recover D2C features optional and fully independent Local Cache as a recovery acceleration layer, designed to reduce the time needed for recovering data or entire protected systems from a cloud vault. In addition to backups directly in the cloud, the Local Cache contains only block data in an efficient deduplicated storage database on an affordable, local storage device for fast local file recoveries or bare-metal restores. In the case of hardware failure or isolated outage, using Local Cache in tandem with D2C gives MSPs the ease of cloud BDR and the speed of local backup without needing a local BDR appliance onsite.

Flexibility With Less Complexity

Designing a reliable business continuity solution requires flexibility and a tailored approach to the needs of the client and the MSP. This whitepaper has already explored how Axcient x360Recover Direct-to-Cloud enables MSPs to customize their deployments to client needs, eliminate unnecessary and risky manual tasks, and address a broad range of client data protection, security, and business continuity requirements.

When an MSP standardizes x360Recover, it can serve almost all of their clients' data protection and business continuity needs with a single vendor. With consolidation comes less complexity and a more focused tech team that can master the solution for better client service. In addition, an agile and unified platform empowers technicians to become more efficient at configuration, deployment, and problem resolution. And when vendor support is required, Axcient is there with its industry-renowned and MSP-focused support organization.

Streamlined Support:

> “It's nice to have everything under one umbrella. One, the pricing is good. Two, I have direct data that our ticketing for failed backups and issues has dropped. So I'm spending a quarter of the time now that I was before on trouble tickets and stuff like that regarding backups.”

– Ryan Keele, CIO at Midwest Computech

Switching is Easy for MSPs and Clients

Many MSPs are challenged with a smattering of different BDR vendors deployed in the field. Traditionally, switching out legacy BDR solutions was costly and time-consuming. In most cases, forklift upgrades required an onsite visit to deploy a new BDR appliance and perform new full backups of the client environment. For many labor-constrained MSPs, it's easier to kick the can down the road simply. Unfortunately, the result is often a mish-mash of different vendor solutions deployed across a client base. As MSPs mature and get more laser-focused on the bottom line, one of the best ways to improve recovery times is to standardize and consolidate technology vendors.

Thankfully, Axcient x360Recover D2C makes it easy for MSPs to migrate off legacy solutions and standardize on x360Recover. For clients that no longer need an on-premise BDR appliance, Axcient designed D2C to simplify the process of standardizing deployments and upgrading to Axcient. D2C enables MSPs to silently deploy the Axcient agent through an RMM tool, configure the backup schedule, and then let it run. With Chain-Free backup, Axcient quickly starts backing up data without server reboots or deactivating your existing backup products. Once D2C is up and running, the MSP can easily remove other backup agents and enjoy automatic, reboot-free upgrades from Axcient. With fewer truck rolls, fewer vendors to support, and right-sized deployments, Axcient helps partners supply their clients with world-class business continuity services, including rapid recovery.

Standardized BDR:

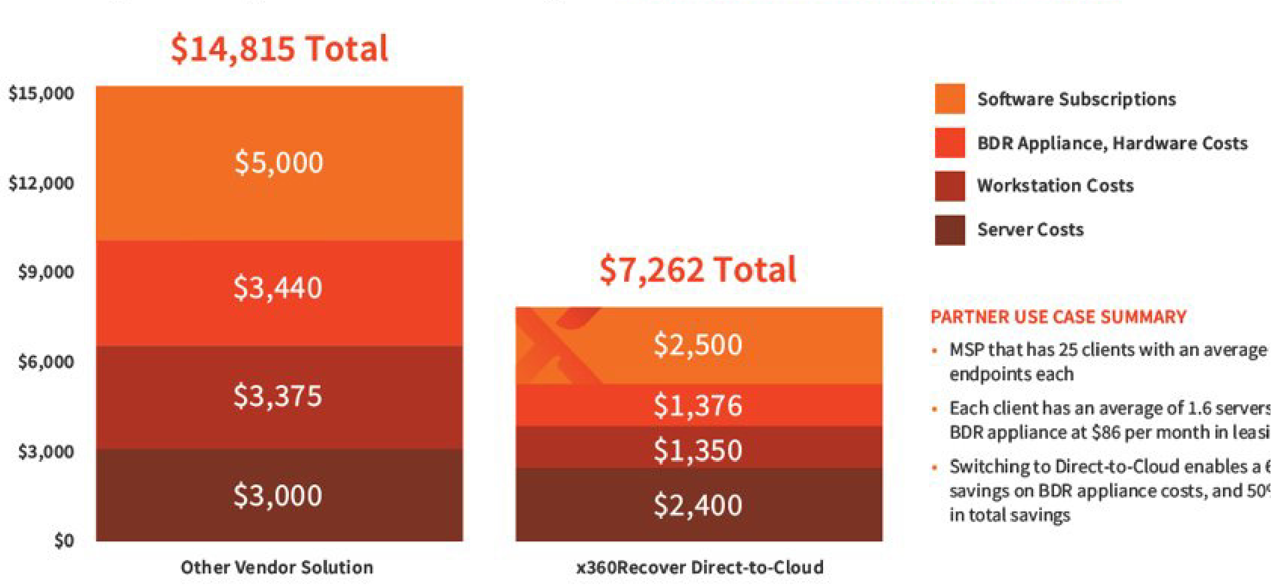
> “We had about 25 different backup vendors, and we were spread too thin. You can't focus on any one vendor or product. There's different training plans, different product support, compression is different, retention is different, and they all do different things. …With Axcient, we have a complete backup solution. Everything from cloud backup to on-prem servers and servers in the cloud. It gives us the flexibility to say, ‘we use one tool to protect everything.”
>
> – Neil Hawkins, COO at LANAIR Technology Group

Reduce your BCDR total cost of managed services by up to 50%

The Axcient Team has curated real-world cost savings seen by our partners who adopted x360Recover Direct-to-Cloud. You can get more details and see that the numbers for this scenario reflect real partner experiences documented in case studies such as Lanair Group, Cinch I.T., Absolute Technology Solutions, and Business Information Solutions.

D2C with Local Cache provides the speed you get with a local BDR appliance but at up to half the cost. Typical BDR appliances burden MSPs and their clients with prices ranging from $1k to $10k. Local Cache devices set MSPs back anywhere from $50 to $500. MSPs who adopt D2C also know that fewer appliances mean less maintenance and fewer onsite visits, and their techs can focus on other activities. Redirect those costs and resources into your business to improve client value and expand your business while delivering comprehensive business continuity. Plus, Axcient's simple flat-rate pricing and pooled data storage and retention without complicated pricing tiers add to software savings compared to channel competitors.

Monthly Savings from Switching to x360Recover Direct-to-Cloud



PARTNER USE CASE SUMMARY

- MSP that has 25 clients with an average endpoints each
- Each client has an average of 1.6 servers BDR appliance at $86 per month in leasi
- Switching to Direct-to-Cloud enables a savings on BDR appliance costs, and 50 in total savings

Conclusion

Business continuity, backup, and disaster recovery shouldn't be complex. MSPs can utilize automation and innovation to efficiently provide proactive data protection for business survival after a data loss incident. This whitepaper has explored how x360Recover D2C enables MSPs to deliver comprehensive BCDR services to their clients. MSPs switching to Axcient benefit from a highly reliable, rapid recovery solution that is flexible to different business needs. After making the switch, most partners can meet more stringent SLAs and can grow their MSP based on the unique security features, confidence, better cost margins, and peace of mind provided to clients. The promise to keep businesses running and the critical capabilities included in x360Recover make Axcient the right choice for secure backup and business continuity services.

Don't take our word for it.

See Axcient's proprietary Chain-Free backup technology, unique security features, and DR capabilities in action in your own MSP environment. **Activate a 14-day Free Trial to experience the benefits of rapid recovery through simplicity.**

Start a no-cost, no credit card trial today

Axcient

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.

CONTACT:

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202 | Phone: 720-204-4500

FOLLOW US:

axcient.com