WHITEPAPER

When backup meets security in the MSP stack

Kaseya | DARKREADING RESEARCH

INTRODUCTION

For most of the past two decades, backup and cybersecurity operated in silos within managed service providers (MSPs). Backup teams focused on restore windows and retention tiers, while security teams chased phishing attacks and vulnerabilities. However, ransomware operators now target backup repositories before hitting production systems, making a clean restore dependent on timely intrusion detection.

It's time to treat backup and security as a single cyber resilience discipline, often called BCDR (business continuity and disaster recovery). This whitepaper will guide MSP owners through the audit, consolidation, and customer conversations needed to integrate their fragmented stack into a continuity-first platform. The goal is validated resilience outcomes, not just ticket counts.

Unpacking the MSP value paradox

The irony of the MSP business model is that seamless service goes unnoticed until something breaks. Pricing discussions should focus on protection rather than technical jargon like retention schedules or RPOs (recovery point objectives).

The MSP market divides into three tiers: checkbox-only companies with loose SLAs and poor remediation capabilities; those who have experienced at least one attack and run a local-plus-cloud combination with intermittent testing; and roughly 20% that sit on continuity-first platforms with rigorous testing. The true blind spot for all these tiers is not the backup itself but the validation behind it.

MSPs often don't know if their backups can meet agreed RTOs (recovery time objectives) until a real incident occurs. This issue stems from letting customers dictate tech stacks based on price, leading to parallel platforms and reactive firefighting rather than proactive measures.

The backup baseline most MSP stacks quietly fail

The assumption that hyperscalers back up customer data is incorrect. Microsoft's EULA commits to platform uptime but explicitly disclaims responsibility for customer data inside Microsoft 365 or Azure. Microsoft takes proactive backups for its own SLA purposes only. A customer-side data-loss event can take at least seven days to remediate, for a premium price. The customer will often simply call their MSP instead.

For these reasons, Gartner believes that three in four companies will prioritize SaaS application backups by 2028. That makes SaaS backup a first-order problem for any MSP touching Microsoft 365, Google Workspace or Azure workloads. The shared-responsibility model is a clause in the contract the customer already signed without reading. The MSP that bundles SaaS backup into the standard offering rather than treating it as an upsell eliminates a category of incident that negatively affects its reputation.

Customers are ultimately more concerned about business resilience rather than understanding how it happens. They want outcomes, not technical explanations of the difference between backups and firewalls.

There's currently a massive gap. PwC found that only 2% of companies surveyed have implemented cyber resilience across their entire organization, even though 66% of tech leaders rank cyber as the top risk they are prioritizing for mitigation over the next 12 months.

Prevention and recovery now feed each other as part of this cyber resilience model, and separating them makes resilience weaker. Backups without security increase incident frequency, while security without recovery increases incident severity.

We see this unification of security and storage everywhere. Gartner has highlighted a unified concept that it calls cyberstorage, in which storage architecture becomes a more proactive part of data protection rather than a simple backup mechanism, integrating more closely with traditional cyber security. From a resilience perspective, cybersecurity and backup storage become two faces of the same coin.

From fragmented stack to continuity-first standard

The path from a fragmented stack to a continuity-first one is shorter than most MSPs expect, but it requires three sequenced decisions:

THE AUDIT

Most MSPs run more redundancy than they think, and not the kind that improves resilience. "I can guarantee you that 80% of the solutions have an overlap of their features and functionalities that are identical," says Kaseya's Taher Adamali, Director of BCDR Concierge. "The 20% that are differentiators across those solutions are probably based on an individual customer requirement from some point in time." The differentiators rarely justify the operational drag of four platforms doing the same thing.

THE PLATFORM SHIFT

Define the bare-minimum capability set the MSP needs to offer continuity-first service, then pick the single platform that delivers it.

THE STANDARDIZATION

That platform becomes the only one new customers run on. Existing accounts convert at renewal or refresh. The cumulative effect is one runbook, one training cycle, and a diminishing operational tail every quarter.

How Kaseya helps

Kaseya's technology stack offers MSPs the platform to support business resilience through a unified view of cybersecurity and backups.

The mailbox compromise is the canonical worked example. Let's say Kaseya's Inky AI-powered email security tool flags a phishing-driven compromise. Its SaaS Alerts cloud detection and response product then ingests the telemetry, and freezes the mailbox, preventing it from sending out phishing attacks to the entire address book. It then hands the time-of-compromise signal to the Datto backup product, which uses that timestamp to identify a pre-attack restore point.

Ransomware scanning has folded into backup validation itself, on the logic that a backup carrying a dormant payload is not a backup. A backup is not clean unless it scans clean. Validation has moved further with AI-powered screenshot analysis in the BCDR boot-test pipeline. The old method of confirming that a restored machine was functional carried meaningful false-positive and false-negative rates. The current method runs the recovery against Kaseya-trained AI models inside the service provider's own data center.

Kaseya's forthcoming cyber-resilience portal, currently in beta, aggregates telemetry into a per-customer risk score from zero to five. Five is the worst posture; zero indicates backups are running, validation is running and the contracted RTO is achievable on demand.

Demonstrating value when nothing is going wrong

If unification solves the technical problem, the operator still has to invoice for the absence of incidents. The metric that proves an MSP earns its retainer is the number of incidents prevented, and prevented incidents are by definition invisible without instrumentation. Two patterns in the Kaseya stack address that visibility problem directly.

> **"We have been training our partners, which is our MSPs, to look at it from not only as a technical relationship but as a business relationship as well."**
>
> Taher Adamali, Director of BCDR Concierge

"MSPs should be able to say 'These are how many backups we took. These are how many were successful. These are how many that failed, that we investigated and then remediated.'" Kaseya's CIO tool amalgamates that across tickets, projects, and SLAs to produce a document a non-technical buyer can read without translation.

The second is the automated Hero report. The MSP can configure it to fire weekly, monthly or quarterly, sent directly to the customer. It provides telemetry in the customer's language that demonstrates the MSP's value.

Both mechanisms support a reframed conversation that the better MSPs are already having. The right denominator for the quarterly business review isn't tickets closed, but hours of business not lost. That is the metric SMB owners renew contracts on, because that is the metric they describe to their boards.

Where next?

The technical case for unifying backup and security is sharper than the case for keeping them apart, because threat actors stopped respecting that boundary years ago. Today, the telemetry handshake between detection and recovery is what determines whether the SLA holds.

The commercial case is sharper too. An MSP that reports incidents prevented and hours of business not lost, instead of tickets closed, owns the renewal conversation. The hardest part for an MSP making this jump is the procurement discipline. Refusing to let customers define your stack based on costing might require saying no to revenue. That's a brave decision, but a long-term win. MSPs who retain control of their own stack will always be one step ahead.

Learn more about Kaseya's backup solutions today.