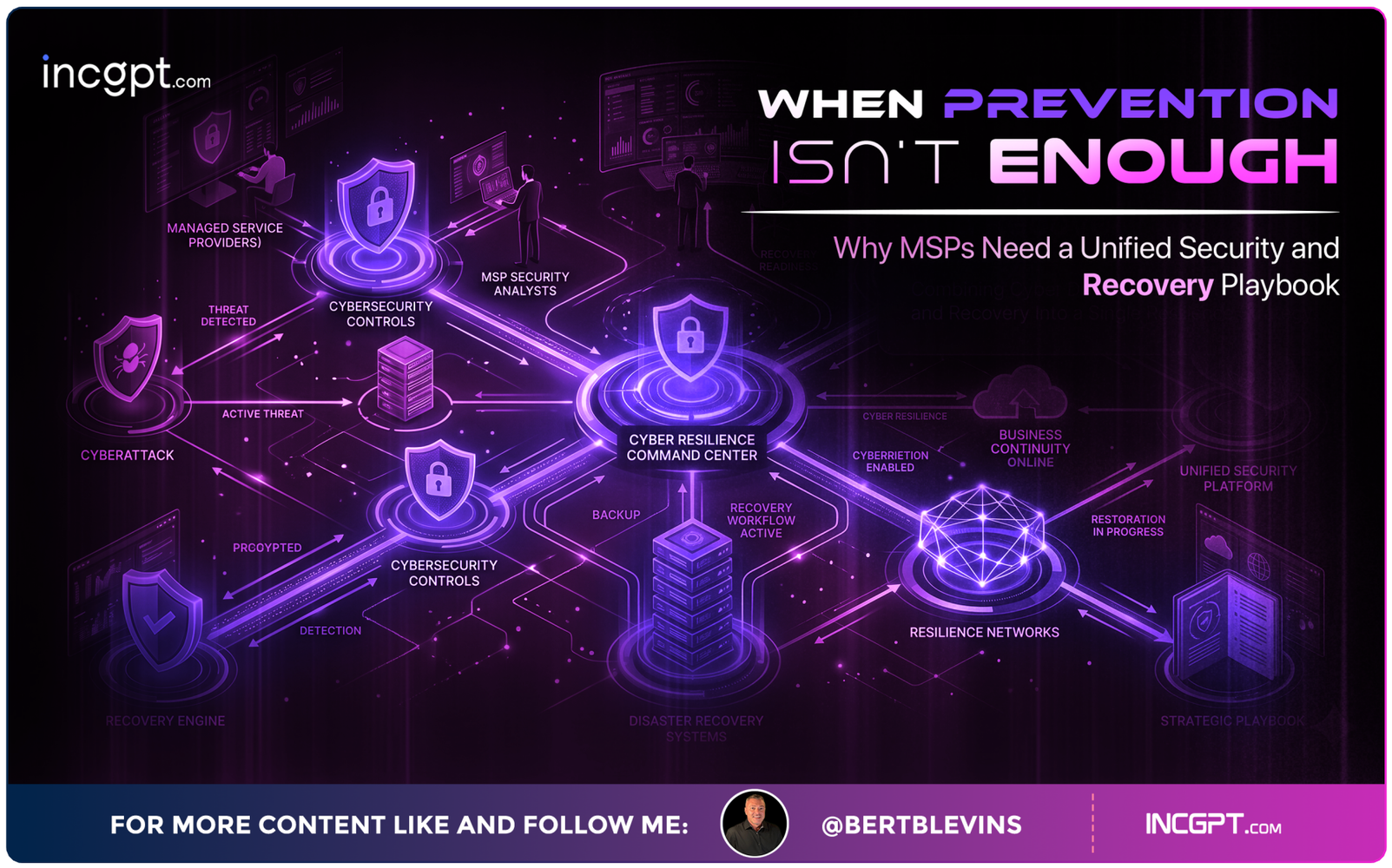
When Prevention Isn't Enough:

Why MSPs Need a Unified Security and Recovery Playbook



A new BleepingComputer and Kaseya webinar makes the case that the line between cybersecurity and backup has effectively disappeared, and that MSPs still treating them as separate disciplines are leaving a gap that attackers are happy to use.

01

On Thursday, May 14, 2026, at 2:00 PM Eastern Daylight Time, BleepingComputer will host a live session with experts from Kaseya focused on a problem that has been quietly redefining the managed service provider business: defenses can hold the line for only so long, and what happens after a breach is now just as decisive as what happens before one.

02

The session is built around a simple but uncomfortable observation. Many MSPs still organize security and data protection as two parallel tracks, run by different vendors, different processes, and sometimes different teams. Modern attackers don't see those lines, and they have spent the past few years building playbooks that exploit the seams between them.

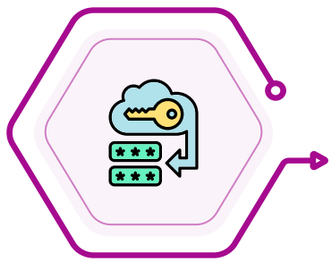
Why the old separation between security and backup no longer holds

For most of the last decade, security tooling and backup tooling lived in different conversations. Security was framed as keeping intruders out. Backup was framed as keeping a copy of the data, mostly in case of hardware failure, accidental deletion, or a natural disaster. Today's attack patterns have collapsed that distinction. Once a threat actor lands inside an environment, their goal is rarely just to look around. They aim for data theft, account takeover, and ransomware deployment, often in the same campaign.

That progression means the moment of compromise is no longer the climax of the incident. It's the opening act. The real damage, and the real test of an MSP's value to its clients, comes from how quickly the affected systems and data can be brought back to a trustworthy state. If the backup strategy was designed in isolation from the security strategy, that recovery often takes far longer than the business can afford.

AI is rewriting the phishing playbook

One of the central themes of the webinar is how dramatically phishing has evolved. AI-generated lures, business email compromise, and brand impersonation campaigns are now well past the era of obvious typos and clumsy grammar. Messages are personalized at scale, branded convincingly, and tailored to specific roles inside an organization. They land in inboxes that have been protected by traditional email security for years, and they slip through anyway.



The result is that phishing has shifted from being one threat among many to being a primary entry point for serious incidents. Credential theft from a single convincing email can hand an attacker the keys to SaaS platforms, cloud admin consoles, and lateral movement paths into client environments. For MSPs managing dozens or hundreds of customers, every one of those inboxes is a potential ignition point.

Trusted infrastructure is being weaponized

Another pattern the session will dig into is the way attackers are leaning on legitimate platforms to disguise their activity. Rather than building exotic infrastructure, threat actors increasingly route their campaigns through services and SaaS tools that defenders are conditioned to trust. A malicious link delivered through a familiar collaboration platform looks very different to an email gateway than one originating from an obviously suspicious domain.

This shift puts pressure on MSPs to refresh assumptions about what counts as safe traffic, what counts as a normal login pattern, and how SaaS data is monitored and protected. It also means that the boundaries between endpoints, identity, and SaaS workloads have to be defended together rather than in isolation.

Detection without recovery is half a strategy

A significant portion of the webinar focuses on what happens after detection fires. Many MSP environments have invested heavily in alerts, dashboards, and threat intelligence, but discover during an actual incident that the response and recovery side of the house was never built to match. Alerts arrive faster than analysts can triage them. Containment runs into stale documentation. Recovery procedures turn out to depend on data sources that the attacker already encrypted or exfiltrated.

The argument is straightforward: if recovery isn't planned, rehearsed, and integrated with the security stack, then a single contained alert can still turn into a full-scale outage. Detection answers the question of whether something bad is happening. Recovery answers the question of whether the business will still be running tomorrow morning. MSPs need confident answers to both.

Why SaaS backups have become non-negotiable

As more client workloads move into Microsoft 365, Google Workspace, and other SaaS environments, MSPs are running into the limits of native data protection. Cloud providers are excellent at keeping their platforms available, but their built-in retention and recovery features were never designed to handle a sustained ransomware event, a malicious insider, or a sophisticated account takeover that quietly destroys data over time.

Independent SaaS backups, controlled by the MSP and isolated from the customer's primary tenant, give service providers a clean recovery point that an attacker cannot reach by compromising a single set of admin credentials. The webinar treats this capability as a core layer of cyber resilience, not an optional add-on, and frames it as one of the most direct ways an MSP can protect both client data and its own service-level commitments.

BCDR as a security control, not just an IT control

Business continuity and disaster recovery has historically been positioned as an operations concern, focused on hardware failure and site outages. The webinar reframes BCDR as an active part of the security architecture. Properly designed, it shortens the window between an incident and a return to normal operations, limits the leverage that ransomware operators have during negotiation, and reduces the financial and reputational fallout that follows a public breach.

For MSPs, that reframing is a commercial opportunity as much as a technical one. Clients are increasingly aware that uptime and security are intertwined, and they are looking to their service providers for a single coherent answer rather than a collection of disjointed contracts. An integrated security and BCDR offering is easier to explain, easier to price, and easier to defend during an incident review than two separate stacks that don't quite talk to each other.

What attendees can expect to take away

Across the session, the BleepingComputer and Kaseya speakers plan to walk through how modern attacks actually unfold from the first phishing email to the final ransomware payload, where MSP defenses tend to break down, and how to close those gaps without ripping out existing tooling. Attendees should expect practical guidance on aligning prevention, detection, response, and recovery into one coordinated motion, plus a clearer view of how SaaS backup and BCDR fit into a contemporary security strategy.

For service providers feeling the pressure of rising attack volumes, more demanding clients, and tighter operating margins, the underlying message is direct. The MSPs that thrive over the next few years will be the ones that stop treating security and backup as separate product lines and start treating cyber resilience as the single thing they actually sell.