Kaseya®

Is your organization cyber resilient?

IT readiness checklist

Most organizations believe they're protected because they have backup in place. However, relying solely on backups could prove catastrophic, since modern cybercriminals target them first. Over 90% of ransomware attacks attempt to delete or tamper with backups before deploying ransomware to prevent recovery.[1]

Today's attacks are identity-led and cloud-targeted, specifically designed to bypass MFA, evade email security, hijack sessions and destroy backups first. Microsoft 365, Google Workspace and other SaaS apps no longer simply support business operations — they run them. Email, files, access, devices, third-party apps and internal collaboration all rely on SaaS identity. When that identity is compromised, the entire business is at risk.

Cybercriminals don't "break in" the old way anymore. And if your recovery plan still starts with "restore from backup," you're already behind. True resilience requires more than just backup. You must secure your business-critical SaaS at the identity level with continuous monitoring, hardened authentication and rapid recovery controls.

Use this cyber resilience checklist to assess whether your organization is truly resilient and recovery-ready or simply backed up.

1 Identity visibility

Identity is now the primary attack path. Do you have visibility into:

- ☐ Suspicious inbox rules?
- ☐ Impossible travel logins?
- ☐ SaaS app abuse?
- ☐ Session hijacking activity?

Without clear visibility, breaches can go unnoticed until it's too late.

Deploy advanced cloud detection and response with real-time alerts and automated containment to detect and stop account compromise early. Invest in reliable Microsoft Entra ID backup and recovery to ensure identity data remains protected and quickly recoverable in the event of a disaster.

2 MFA bypass readiness

Are your end users protected against:

- ☐ Adversary-in-the-middle (AiTM) attacks (Evilginx-style)?
- ☐ Stolen session tokens?
- ☐ AI-driven phishing attacks that slip past email security?

Traditional defenses alone aren't enough to tackle today's sophisticated cyberthreats. Modern cyberattack techniques are specifically designed to bypass MFA and evade standard security controls.

Strengthen protection with phishing-resistant authentication, continuous session monitoring and advanced SaaS threat detection and response to stop identity-based attacks before they spread.

3 Maturity of backup protection

In 2025, over 60% of businesses worldwide experienced a ransomware attack.[2] If ransomware hits:

- ☐ Can attackers delete or encrypt backups?
- ☐ Are backups immutable and isolated?
- ☐ Is recovery tested for identity compromise scenarios?

Cybercriminals know that organizations rely on backup as their recovery safety net, so they target it first. In fact, nearly 60% of attacks targeting backups succeed.[1] If they alter, delete or access your backups, your recovery points are erased with no way to restore.

Implement immutable, isolated backups and regularly test full recovery scenarios to ensure you can restore data and maintain business continuity in the event of a disaster.

4 Fast investigation and response

When an incident occurs:

- ☐ How long does a log review take?
- ☐ How many systems need to be manually checked?
- ☐ How long have service(s) been down?

The longer it takes to investigate and respond to a cyber incident, the greater the damage. Alert overload and manual investigations not only slow response times and extend downtime, but also increase admin stress, frustrate users and damage both revenue and trust.

Implement automated detection, centralized visibility and guided-response workflows to reduce investigation time and restore service(s) quickly.

5 Unified visibility across tools

IT teams use a variety of tools to meet different IT and security needs. But ask yourself:

- [ ] Does your email security integrate with the rest of your stack?
- [ ] Does your EDR solution send alerts to your other security tools?
- [ ] Is your backup solution connected to identity and threat signals?
- [ ] Are your SaaS logs actively monitored and correlated?

When these systems operate in silos, critical signals are scattered across platforms. Early warning signs get buried in separate dashboards, forcing your IT team to manually connect the dots.

Consolidate visibility across your security stack with integrated monitoring and cross-platform correlation, so you can detect the full attack chain before the damage is done.

6 Double extortion preparedness

If data is exfiltrated before encryption:

- [ ] Do you know what was taken?
- [ ] Can you prove the extent of the damage?
- [ ] Are you ready to talk to stakeholders if attackers steal your data and threaten to expose it?

In double-extortion attacks, encryption is only half the threat, since threat actors also exfiltrate data alongside encrypting files. Therefore, even if you manage to restore every file from backups, stolen data can still be leaked, sold or used to put pressure on your organization.

Implement data monitoring, exfiltration detection, access controls, encryption and clear incident response playbooks so you can detect threats early and prevent hackers from stealing or leaking your sensitive information.

7 Scalable protection

User expectations are rising. Can your current team:

- [ ] Deliver fast responses on time?
- [ ] Maintain zero-downtime performance?
- [ ] Manage growing SaaS complexity?

As cyberthreats evolve and SaaS environments grow more complex, your team faces increasing pressure. Without the right tools and systems in place, rapid threat response, business continuity and high-quality delivery become difficult.

Invest in automation, integrated security controls and streamlined backup and recovery processes that scale with your business, without increasing headcount.

8 Recovery preparedness

If an identity-led SaaS attack hits your organization tomorrow, can you confidently answer the following:

- [ ] Do you have a clear, documented recovery playbook for identity compromise?
- [ ] Can you restore access, secure accounts and resume operations quickly?
- [ ] Is your team trained to execute recovery without improvising in real time?

Without a predefined recovery plan, such events can result in data loss, halt business operations or potentially put you out of business for good.

Develop and test a structured, identity-focused recovery plan that enables your team to respond quickly and ensure rapid recovery with minimal or no disruption.

Beyond backup: The shift to cyber resilience

Cyber resilience goes beyond backup. It's the strategy that ensures business continuity when identity, SaaS platforms and even backups are compromised.

Traditional tools, such as email gateways, MFA, endpoint protection and backup, are now table stakes. On their own, they aren't enough. Without integrated monitoring, shared visibility across tools and a coordinated recovery plan, gaps emerge — and attackers exploit them. Cyber resilience closes those gaps by connecting protection, detection and recovery into a single, continuous strategy focused on maintaining operations, minimizing downtime and protecting your brand reputation.

Your organization depends on IT not just to keep systems running, but also to help manage business risk and ensure operational resilience. When stakeholders assume backups equal protection, critical gaps in security, identity protection and recovery readiness can go unaddressed until an incident occurs.

By helping stakeholders understand identity-based threats, evolving attack methods and the business impact of data loss and downtime, IT teams can shift the conversation from basic backup to true cyber resilience.

Don't wait for a cyber incident to reveal your vulnerabilities.
Start building a cyber-resilient organization today.

Start now

Sources:
1 https://prolion.com/blog/ransomware-is-growing-exponentially/
2 https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/?srsltid=AfmBOoo6d4R8jqJD_IaEgJMSiPHyDFipjSSjRLqogw8upcT4TattZf0X

Kaseya®