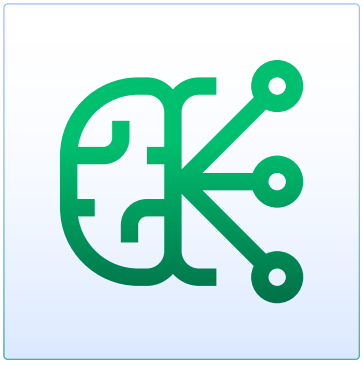
Key takeaways

Is your cybersecurity strategy ready for the challenge ahead?

Evolving cyberthreats, rapidly shifting attacker tactics, and increasingly complex digital environments: Is your security strategy keeping up?



The past year has brought a wave of high-impact incidents — from sophisticated identity-driven attacks to supply chain infiltration and AI-augmented threats — that pushed organizations to rethink their cybersecurity posture. Yet many teams still underestimate how quickly the threat landscape is accelerating. This was the key focus of a recent Keepit webinar, where Kim Larsen, CISO at Keepit, Paul Robichaux, senior director of product management at Keepit and Microsoft MVP, and Trent Widtfeldt, chief of engineering at Technologent, discussed significant cybersecurity trends as well as resilience lessons learned.

From AI-powered attacks and shadow AI to hybrid threats and cloud dependency, one theme was clear: Hope is not a strategy. Read the key takeaways for actionable strategies to make your security posture more resilient in 2026 and beyond.

The key takeaways

AI-powered attacks are accelerating

The complexity and power of cyberattacks is increasing — and so is accessibility. Capabilities once limited to nation-state actors are now within reach of individual attackers. AI is increasingly being used for attack planning, and the barrier to entry is falling. Your defenses must level up for a threat that is more automated than ever.

Shadow AI is today's silent risk

Most shadow IT isn't malicious — it's employees trying to work faster. But AI often stores or transforms sensitive data, operates without governance, and exposes your organization to legal, ethical, and regulatory risk. The real risk is the speed gap: Adoption is happening faster than governance is being applied.

Governance needs to catch up

AI introduces a new governance challenge. Frameworks like TRiSM emphasize transparency, continuous model monitoring, clear ownership and oversight, and embedded compliance controls. You can never eliminate AI risk fully, but you can make it manageable. Build guardrails before scaling adoption.

Hybrid threats are the new normal

Threats no longer live in a single domain. We are seeing pivots from on-prem to cloud and vice versa, infrastructure sabotage, power failures, and regional disruptions, as well as natural disasters intersecting with digital dependency. The question is no longer if disruption happens — but whether your architecture and processes can withstand it.

You need a plan for when the cloud goes dark

In 2025, organizations experienced major SaaS outages, leaving organizations without access to critical systems and considerable downtime. True resilience requires independent backup outside the production ecosystem, clear prioritization of critical systems, and tested disaster recovery plans, including offline scenarios.

People and process matter

Security isn't just about technology, it's about working with your people as well as establishing processes. Effective organizations assume breach, run tabletop exercises and simulations, define recovery priorities, and align leadership on what matters most before incidents occur. Resilience is never a one-person job, but a unified cross-team effort.

Resilience actions for your organization

- Categorize, assess, and reduce risk
- Establish a center of excellence within your organization and be clear on what resources and people you need
- Plan and prioritize recovery of data and systems
- Future-proof your architecture: Demand true immutability from your data protection vendor and physically/logically isolate your backups from your production data
- Test restores regularly and run exercises and simulations with your team

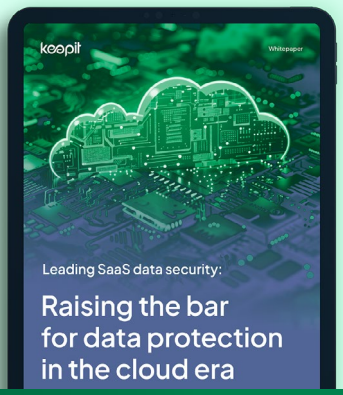
Organizations that will succeed in 2026 are not those that hope to avoid disruption but those that assume disruption, prepare for the worst, and practice recovery regularly. In a world of accelerating automation and converging threats, hope is not a strategy. Mapping relevant risks, preparing for them, and testing your contingency plans is.

Read more about AI of the future in our latest blogpost ⟶

Leading SaaS data security

Read our white paper on how Keepit is raising the bar for data protection in the cloud era to learn more about our unique architecture.

Download now



Keepit provides a next-level SaaS data protection platform purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on Linkedin