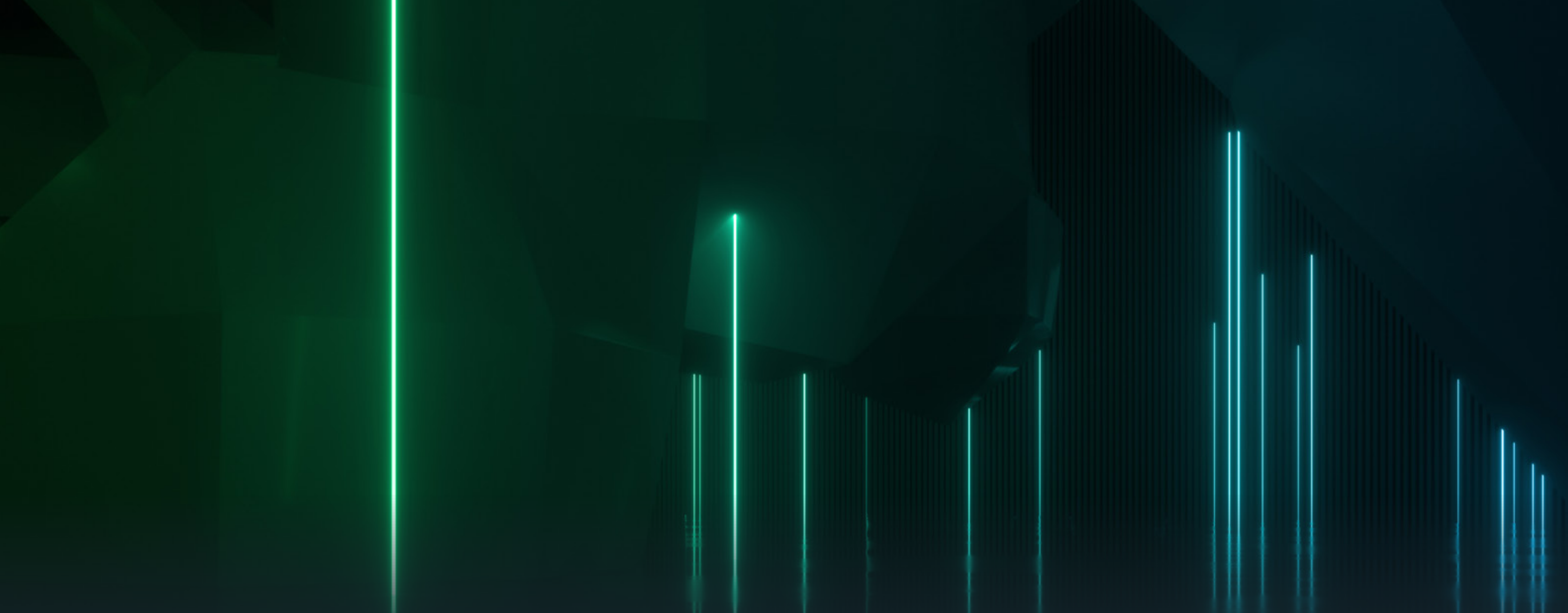


Top 2024 trends in Gen AI, data security, and multicloud

COHESITY

Introduction

AI dominated the tech conversation in 2023. In 2024, leaders and practitioners are doing more than talk—they're building their roadmaps and strategy around AI. At Cohesity, our business is at the convergence of generative AI, data security, and multicloud. So we wanted to share a few perspectives on topics likely to be on the minds of our customers in the coming year. What does AI mean for businesses across a broad spectrum of industries—especially as cyber threats evolve and intensify? How can you strengthen your resilience as you execute your multicloud strategy? And how can you harness the full power of generative AI to search, analyze, and discover trends in your data?

In this eBook, our experts reveal the five biggest trends shaping the future of Gen AI, data security, and multicloud in the coming year.

Trend One

Generative AI and security will come together in the worldwide fight against cybercrime.

As the number of bad actors proliferates and cyber threats get harder to detect, businesses must prepare for this cold fact: Cybercriminals will escalate how they use AI. Look for increased efforts to entice employees—using social engineering—to click, act recklessly, and exploit zero-day vulnerabilities.

But there's good news too. Savvy organizations will use generative AI as a positive security mechanism to fight these bad actors as part of a modern data protection strategy. Expect the end goal to change from thwarting attacks to doubling down on rapid post-attack recovery.

Ultimately, we can expect both adversaries and innovative IT leaders to take full advantage of generative AI and its capabilities, making it a force multiplier in both their efforts.

Trend Two

As businesses expand their multicloud footprint, CIOs and CISOs will double down on data security with clear visibility of their attack surface—or risk additional breaches.

When you move your workloads from on-premises to the cloud, you're extending your attack surface. That means you need to evolve your security posture and even how you track and manage your risk across clouds.

Thankfully, the industry has innovated in recent years to simplify this task. The growing field of **data security posture management** (DSPM) can help businesses manage risk across all your infrastructure, and this category will hit mainstream adoption this year.

Organizations are at wildly different stages in their multicloud maturity. "You won't see a 100 percent transition from on-prem to cloud," says Brian Spanswick, CIO and CISO, Cohesity. "You're going to see a hybrid infrastructure model practiced by most companies. But they're going to have to rethink their security posture and the controls they use to protect their cloud environments."

Here's the bottom line: How you back up and recover your data and how you minimize the impact of breaches requires a modern set of controls and procedures. And companies need to fully understand the security implications of shifting to a cloud-native model.

Trend Three

Organizations will use generative AI to search, analyze, and discover trends and patterns on both primary and secondary data.

Historically, organizations have used AI on their primary data. In 2024, we'll see secondary data become a valuable source of new insights. Business leaders now recognize the incredible potential of generative AI in secondary data to:

- Analyze large volumes of backup and archive data
- Identify patterns and generate insights and reports from complex datasets
- Create new innovations in search and discovery

Consider the example of a large global bank seeking to review loan performance over a 10-year period, or a law firm digging into historical compliance issues.

Layering generative AI atop an enterprise's own datasets (both primary and archived data) can generate more knowledgeable, diverse, and relevant insights, leading to faster decision-making and breakthrough innovations with untold potential.

> Harnessing the power of data security and management solutions enhanced by AI unleashes greater efficiency, innovation, and growth potential than ever before.

Trend Four

Organizations will increasingly look to engage with tightly integrated ecosystems that include a broad range of security, data management, and AI services to combat continuing cyber threats.

To date, cybersecurity has been a separate, largely compliance-driven discipline within the organization. This made sense, as traditional security solutions were implemented to protect the perimeter of a company's data center. Moving forward, though, advanced capabilities will be more tightly integrated and plugged into existing SOC workflows.

API-driven tooling has influenced organizational change too. Security and IT teams are working more closely together, often in a DevSecOps capacity. This is part of the larger "shift left" trend, where security becomes built in early in IT processes rather than bolted on at the end. Vendors are also adjusting how they serve their respective markets. Many leading providers now realize they must collaborate more closely to solve increasingly complex problems, remain agile, and improve cyber resilience for their customers.

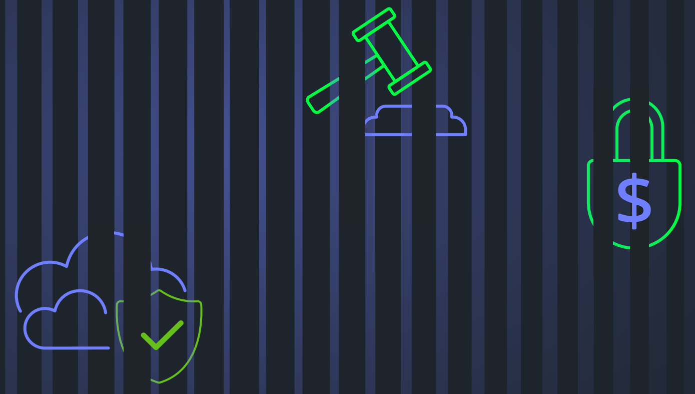
Look for IT leaders to abandon spot solutions in favor of platforms that already include security capabilities, plus greater sharing of threat information across public and private partnerships.

Trend Five

Governments will strongly recommend not paying for ransomware. But this won't deter attackers.

A group of nearly 50 countries recently pledged to no longer pay ransoms demanded by attackers. This represents a diplomatic accomplishment, but it won't blunt the frequency or sophistication of attacks. So what does this declaration mean for companies and other nongovernmental entities?

Expect organizations of all kinds to intensify their focus on cyber resilience, putting less emphasis on preventing ransomware or preventing a breach and more emphasis on reducing its impact if and when a breach occurs. They'll invest in recovery rather than over-rotating on prevention.



Trend Five

If you can ensure that:

- Your secondary data is encrypted and immutable
- You've got detections in place to know if a bad actor has abused the integrity of your data
- You can recover, and bring core business processes back online from a backup of production with aggressive recovery time objectives

...then even...

... if attackers can get through your firewall, break your identity, access management controls, crack your password, and move laterally through your network—even if they can get to that asset, you can minimize your operational risk.

You'll have effectively blunted the attack's impact, and removed the motivation for future attacks.

Trend Five

What does this mean for the cyber insurance industry? Cyber insurance will remain a popular hedge against risk. According to insurer Munich Re. as cited in Moody's September 2023 Special Report, the cyber insurance market is projected to grow to $33 billion in premiums by 2027, up from roughly $12 billion today. For a complete discussion of its benefits, costs, coverage, and eligibility, read our eBook, Cyber insurance for the enterprise.

In 2024, expect to see a stronger commitment to cyber resilience, more investments in ways to minimize the impact of attacks, and less focus on deterring the attacks themselves. But don't expect cyber insurance to go away anytime soon.

Ready to strengthen your cyber resilience?

Get to know our AI-powered data security and management at cohesity.com

COHESITY

www.cohesity.com