6 predictions for 2025

WHAT'S NEXT IN DATA SECURITY AND MANAGEMENT

COHESITY

Introduction

The speed with which AI continues to accelerate—and fundamentally reshape both what is possible and what's at risk—is being felt across industries. Organizations that quickly but carefully harness its advantages, while remaining clear-eyed about attackers' use of this same technology, will be well-positioned for the future.

Because we at Cohesity work daily at the intersection of AI, data security, and cloud, our experts are adept at forecasting what to look for (and guard against) in these three fields so critical to our customers, their data, and their resilience. In this eBook, read our six biggest AI, data security, and cloud predictions. We've accompanied each prediction with an actionable takeaway and linked to valuable resources throughout so you can explore each topic further.

PREDICTION #1

Scrutiny of software supply chain vulnerabilities will deepen.

PREDICTION #1

Scrutiny of software supply chain vulnerabilities will deepen.

Software supply chains are a growing threat vector—and their vulnerabilities will worsen over time.

Both the 2020 SolarWinds attack and other more recent, high-profile breaches have brought worldwide attention to this problem, but these are just a few examples among many.

To reduce risk, some companies may claim that the best course of action is for organizations to rely only on their own code, and not to embed open source code or code from partners into their products, especially when that code has access to customer data.

But this is both a naive position and an unworkable solution.

Here's why.

The best and most innovative products all use some third-party code; it's a tried-and-true best practice that is as old as software development itself.

In fact, open source is the biggest contributor to code for most companies—and no company is expected to write all the code in their product.

According to the 2024 Open Source Security and Risk Analysis Report, "open source components and libraries form the backbone of nearly every application in every industry. Ninety-six percent of the total codebases (the code and associated libraries that make up an application or service) contained open source. Seventy-seven percent of all code in the codebases originated from open source. Every industry codebase scanned contained open source—most at percentages from 99% to 100%."

PREDICTION #1

Scrutiny of software supply chain vulnerabilities will deepen.

So focus instead on mitigating risk in your software supply chain:

- Build a walled garden around third-party code (think of the iPhone and Apple app store).
- Monitor CVEs for packages in your software supply chain, and promptly apply patches from trusted vendors across impacted environments.
- Tighten security for vendors, partners, and other third-party services to prevent breaches that can occur through external connections.

The Software Bill of Materials (SBOM) will also continue to be important and will force vendors to disclose and track the third-party libraries they're using.

ACTION ITEM:

Supply chain vulnerabilities will need to be addressed. Recognize that the most effective course is for more companies to come together to solve these problems—not fewer. In today's environment where open source is everywhere, going it alone won't make your company more secure.

Security is a team sport—and so is a secure software supply chain. Read about our Data Security Alliance.

PREDICTION #2

AI will expand the cybersecurity job market.

PREDICTION #2

AI will expand the cybersecurity job market.

Here's how AI will expand the cybersecurity profession in 2025.

There's a global shortage of cyber professionals. The White House Office of National Cyber Director launched a program to fill the gap of approximately 500,000 open cyber jobs in the United States.

And within that shortage is a skills gap. This is where AI can help. AI will make cybersecurity tools easier to use. AI augmentation can make employees more accurate, effective and allow employers to hire employees with broader skill levels.

At the same time, guarding against advanced threats (often powered by AI) will become far more complex. For those gnarly cybersecurity problems, highly skilled AI cybersecurity experts will still be needed.

Employers will prize those who can use defensive AI measures to combat AI-powered cyberattacks. These practitioners, who have the knowledge to implement AI-driven security tools, strengthen AI model security, and develop AI-assisted threat intelligence, will be in high demand.

ACTION ITEM:

Get those cybersecurity jobs filled. Highly skilled AI cybersecurity experts are always in demand. With cybersecurity tools now easier to use, look to hire employees with a broader skillset that can be augmented by AI.

PREDICTION #3

As enterprises continue to accelerate public cloud adoption, certain workloads will remain on-premises for the foreseeable future.

PREDICTION #3

As enterprises continue to accelerate public cloud adoption, certain workloads will remain on-premises for the foreseeable future.

In 2025, public cloud growth will remain strong as organizations continue their modernization efforts. But companies won't go "all in" on the cloud.

Why? Cost is the primary factor: Workloads with predictable resource needs will almost always be cheaper to run in the data center. Keeping some on-prem workloads will help ensure that the costs of securing and managing data remain under control. Similarly, we'll see a slow, but steady, repatriation of workloads from the cloud to on-prem environments to further optimize cost.

Further, the adoption of hybrid architectures will be more important than ever as enterprises seek to balance utilization, cost, control, and convenience.

ACTION ITEM:

Because your enterprise data estate will span data centers and multiple clouds, you'll need security tools that protect your data across environments with minimal operational overhead.

Looking for key strategies to protect, manage, and recover your data in multicloud environments? Learn more about what's most essential in a data protection solution, and discover how to ensure seamless protection for all your workloads—whether on-prem, hybrid, or in the cloud.

Read the white paper

PREDICTION #4

Organizations will see the greatest impact from AI by making individuals more productive.

PREDICTION #4

Organizations will see the greatest impact from AI by making individuals more productive.

Tactical projects that use Gen AI to improve the speed and accuracy of manual business functions, including IT operations, security, compliance, and legal scenarios, will drive this surge in productivity. And enterprises will reap the benefits by increasing their revenue per employee.

To be clear: While AI will help people in their work, it won't take over your company. There's understandable fear that AI will come in and wipe out entire departments or perform higher-order tasks across the board. This won't be the case. There's no "giant brain" coming to run your business.

Instead, AI's influence will be felt across a wider array of small projects. Each project will aim to solve a specific problem, which in the aggregate will help employees do their jobs better (i.e. faster and with improved outcomes). So don't expect IT leaders to invest in "big bang" projects like automating functions completely with AI, building a company-wide AI solution, or developing system-wide AI workflows. But do expect them to take a pragmatic approach and implement AI tools and solutions to increase ease of use, simplicity, and team performance.

ACTION ITEM:

Since AI won't take over executive functions or run big departments, invest in AI projects that will solve point problems, automate routine tasks, or accelerate decision-making at the individual contributor level.

You can use AI-powered search to get trusted answers from your data. Learn how with Cohesity Gaia and watch our webinar on getting started with Gen AI.

PREDICTION #5

With the AI arms race underway in cybersecurity, those not using AI will be left behind.

PREDICTION #5

With the AI arms race underway in cybersecurity, those not using AI will be left behind.

When bad actors use AI in cyberattacks, conventional data security mechanisms will consistently fail.

Take a run-of-the-mill phishing email. A spambot or even a careful eye used to be enough to spot these scams, but no more. With AI, attackers can now craft beautifully-written phishing emails that will fool older systems (and conscientious humans) without the AI tools to identify them.

Quite simply: AI will be required to maintain your current security risk posture and fight back against threats.

PREDICTION #5

With the AI arms race underway in cybersecurity, those not using AI will be left behind.

Expect the following in the year ahead:

- Using AI and machine learning to detect sophisticated threats, automate responses, and identify vulnerabilities will become mainstream.
- AI will become a foundational part of malware research for modeling.
- "Next-gen" SOAR companies will continue to add AI to their playbooks to automate response.
- AI will become common in threat hunting practices, with companies loading a corpus of data into an LLM to search for threats proactively.
- Deception technologies, which create a honeypot and release decoys to mislead the attacker and gather threat intelligence, will become easier for organizations to adopt and implement.

This is a fight between good and evil. Make sure your arsenal of tools is as sophisticated as your attackers'.

ACTION ITEM:

Start using the latest AI-powered security if you haven't already, or your organization will be at higher risk. Conventional security systems are no match for today's sophisticated, AI-based threats.

Read more about how AI and ML are transforming data protection.

Get the ESG report

PREDICTION #6

Global regulations will force companies to be transparent about their cybersecurity posture.

PREDICTION #6

Global regulations will force companies to be transparent about their cybersecurity posture.

Publicly traded firms have spent the last year adjusting to recent SEC rules that require the disclosure of material cybersecurity incidents within four business days.

While the rules have been in place since late 2023, the coming year will see large enterprises taking steps to fully comply with them and avoid penalties.

So expect a surge in reported cyberattacks. Because the disclosure requirements themselves will drive these numbers higher, they'll likely reveal trends that have existed but were previously underreported.

This visibility and transparency has implications for your business and its brand, so learn not just how to disclose but how to do it right.

Interested in pragmatic steps organizations like yours can take to strengthen their resilience to destructive cyberattacks?

Get the white paper

PREDICTION #6

Global regulations will force companies to be transparent about their cybersecurity posture.

In the European Union, the compliance deadline for the Digital Operational Resilience Act (DORA) falls on January 17, 2025—and articles 17-23 refer specifically to Incident Management, Classification, and Reporting. Under DORA, financial entities need to have a clearly-defined Incident Management process. This covers not just the detection and management of ICT-related incidents, but also their classification, recording, and reporting to internal management, competent external authorities, and any relevant European Supervisory Authorities. Noncompliance can lead to severe penalties for both organizations and individuals. Need guidance?

View our DORA resources

ACTION ITEM:

Practice getting comfortable with being transparent because you no longer have a choice about whether or not to disclose cyber incidents. Since you have to disclose, take advantage of resources that prepare your organization to do it right.

Ready to strengthen your cyber resilience?

Get to know our AI-powered data security at
cohesity.com/solutions

COHESITY

6100027-001-EN 1-2025