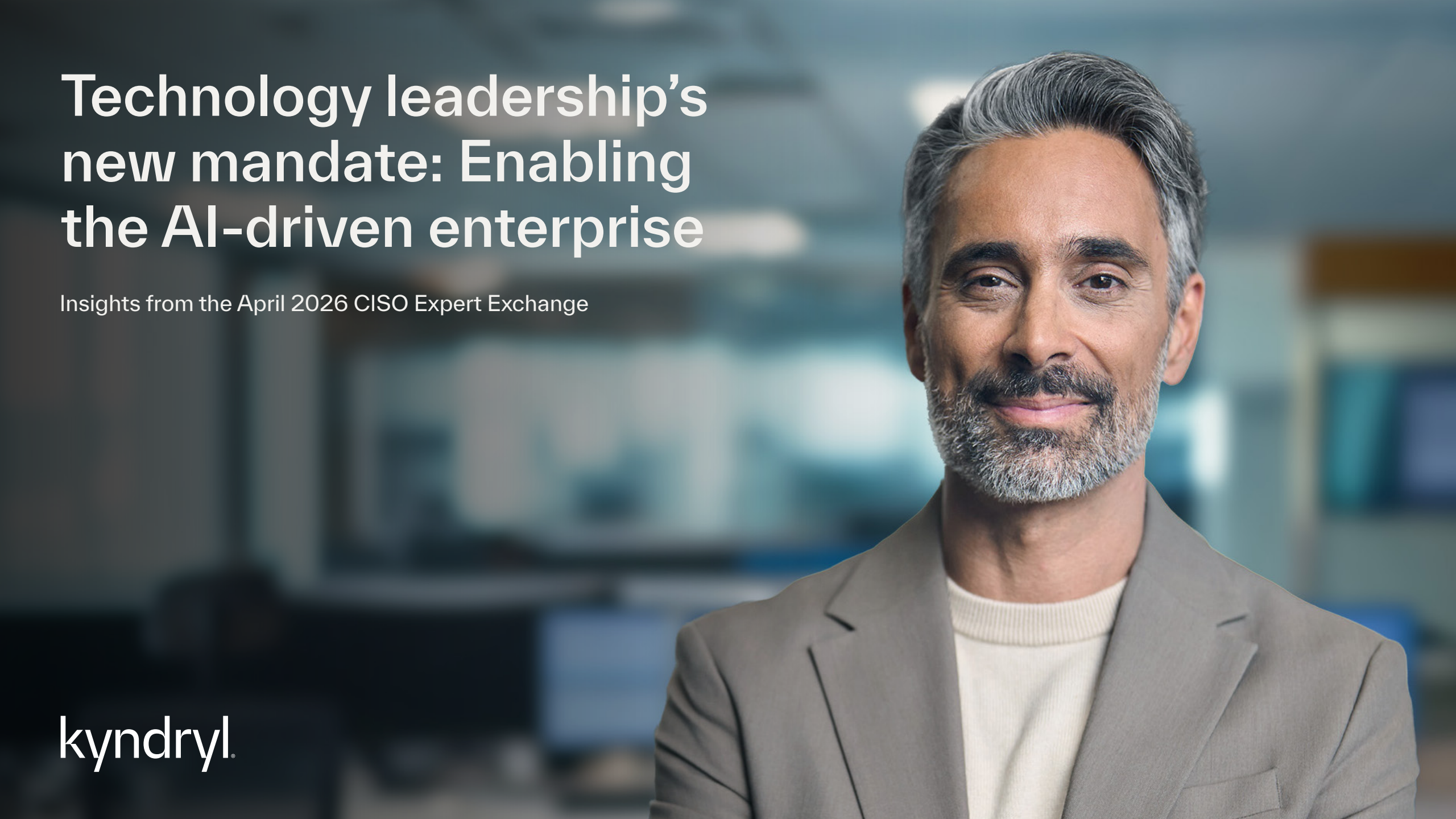
Technology leadership's new mandate: Enabling the AI-driven enterprise

Insights from the April 2026 CISO Expert Exchange



kyndryl

Contents

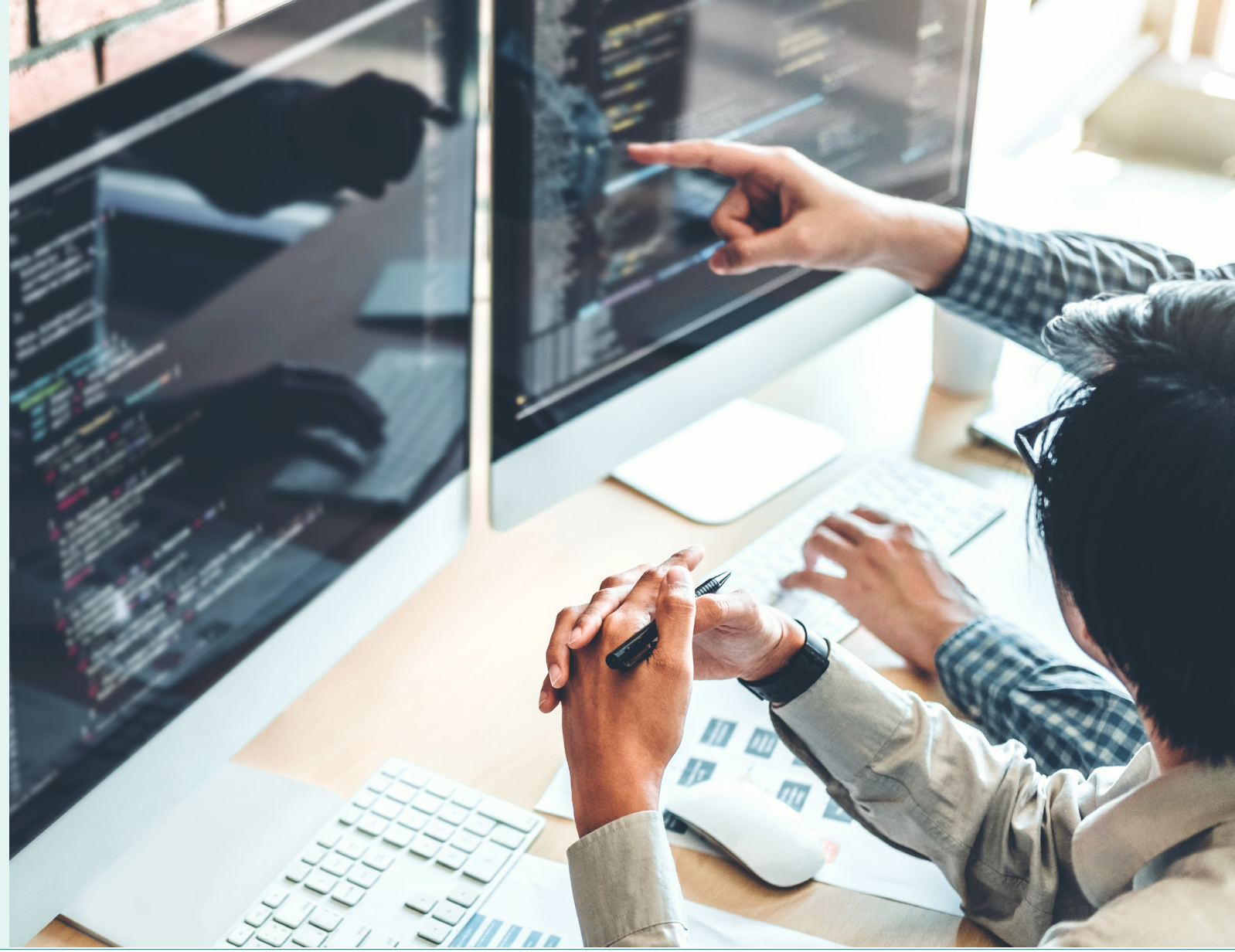
01

CISOs' priority: Scaling AI with manageable risk

Across industries, business leaders are demanding immediate integration of AI-powered tools, automated agents and intelligent workflows. As business units employ AI, which moves faster than traditional governance models can support, they increase the chance of breaches, outages and regulatory failures.

For today's CISO, the question is no longer whether the enterprise should adopt AI, but how it can enable AI-driven enterprise acceleration while reducing risk.

In April 2026, Kyndryl hosted a CISO Expert Exchange to explore questions and ideas related to safely managing AI adoption. Thirteen participants joined the wide-ranging conversation. The following pages present highlights from the session and related notes for consideration.



02

AI governance: From gatekeeping to enablement

CISOs are finding that attempts to restrict or delay AI adoption typically drive its usage underground, preventing effective governance. Unauthorized use of AI tools is now widespread, often driven by productivity demands.

In response, leading organizations are reframing AI governance from gatekeeping to enablement. They are building foundational controls that allow the business to move quickly, but not blindly. Leading teams are investing in continuous, enterprise-wide visibility across browsers, networks, and applications.

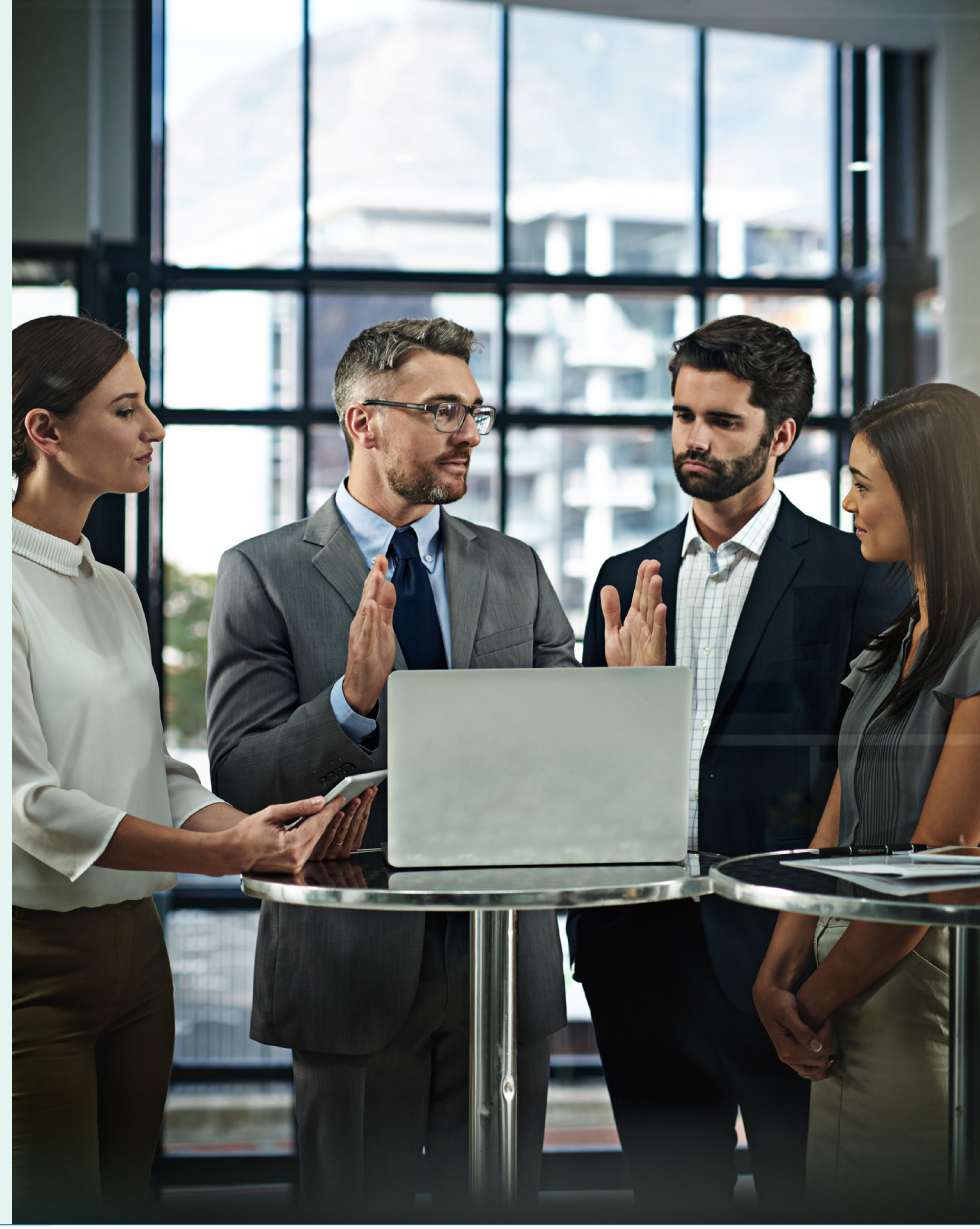
The role of the CISO is evolving from:

Gatekeeper → **Enabler**

Enforcer → **Orchestrator**

Technical authority → **Enterprise risk translator**

Redefining security for the Agentic AI era →



03

A security blind spot: Non-human identity governance

As AI scales, employees are creating and deploying AI agents without formal identity registration, clear ownership, lifecycle management or consistent access controls. This is why **non-human identity governance is a critical gap that demands CISOs' urgent attention.**

Most CISO Expert Exchange participants say that fewer than one-quarter of the digital agents in use at their organizations have auditable identities. And only a small minority of those CISOs report high confidence in their ability to govern agent access at scale.

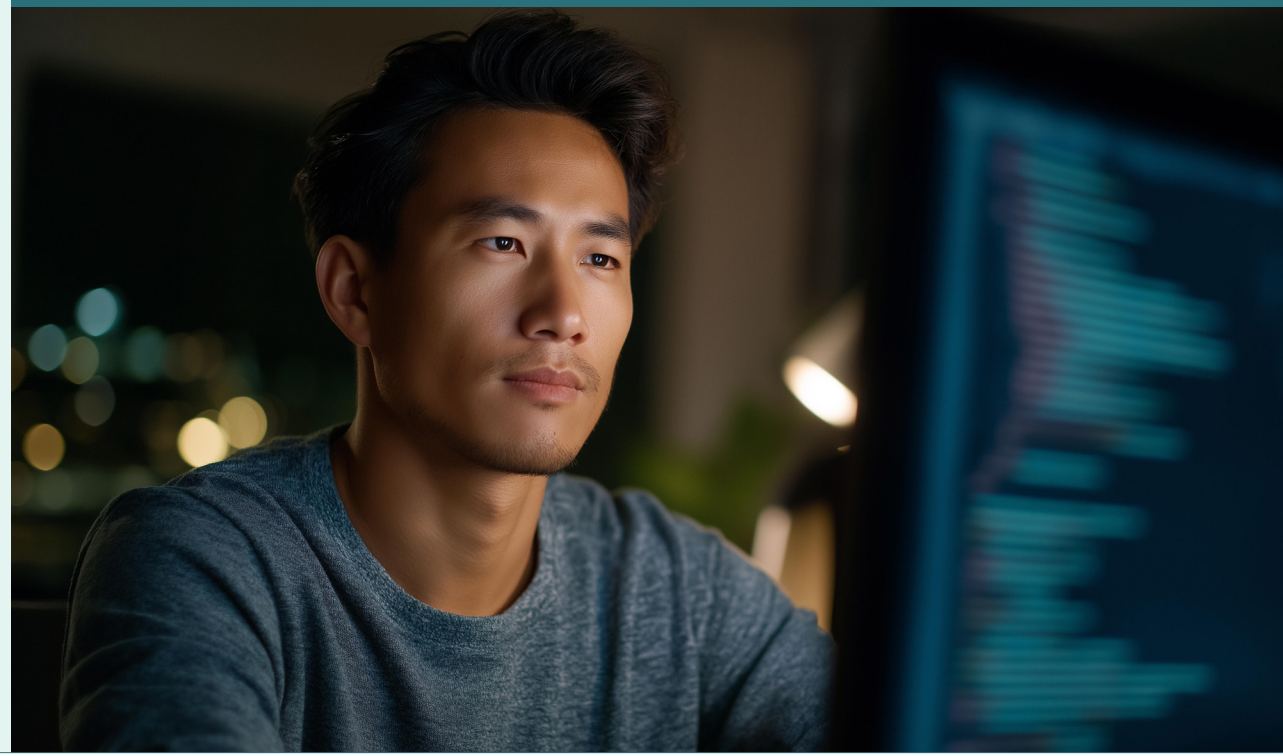
The result is a rapidly expanding layer of untracked, unmanaged identities with privileged access, creating a new and largely invisible attack surface.

<25%

Digital agents at participants' organizations that have auditable identities.

* *As reported by a majority of CISO Expert Exchange participants.*

> "I run identity for the company—and no one has asked me for a single agent ID.
>
> CISO Expert Exchange participant



04

AI shines a light on existing vulnerabilities

AI tools are identifying decades-old weaknesses, insecure dependencies and unresolved technical debt. Participants at the CISO Expert Exchange emphasized this insight: **AI adoption is not so much creating new vulnerabilities as rapidly exposing existing ones.**

This discovery is occurring at a pace most organizations are not equipped to handle. Most participants reported that their organizations have automated only a small fraction of security workflows. Those that lack modern CI/DevOps pipelines, automated patching and scalable remediation workflows risk being overwhelmed by the volume of issues AI can uncover.

In this environment, software delivery is no longer just an engineering function but a core resilience capability. Yet the project of scaling AI faces organizational constraints such as budget limitations and integration complexity.

71%

of CISO Expert Exchange participants report less than 10% of security workflows are automated.

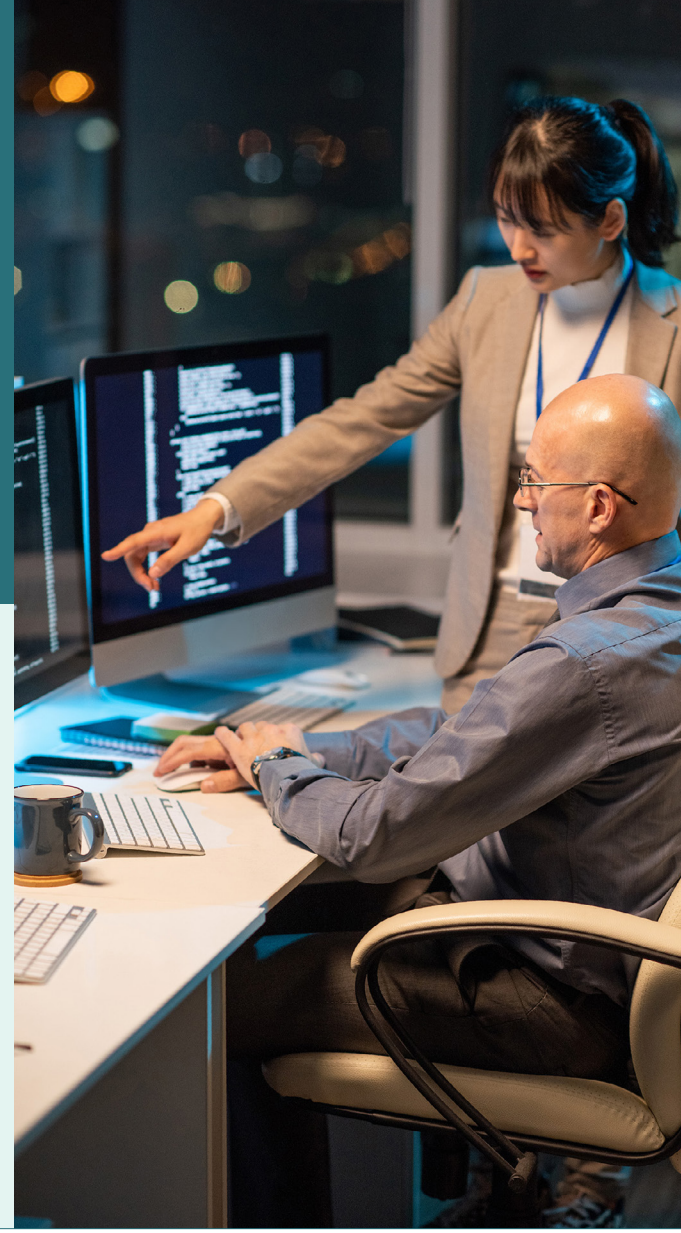
Top barriers to scaling AI, according to CISO Expert Exchange participants:

43%

Budget constraints

29%

Integration complexity



05

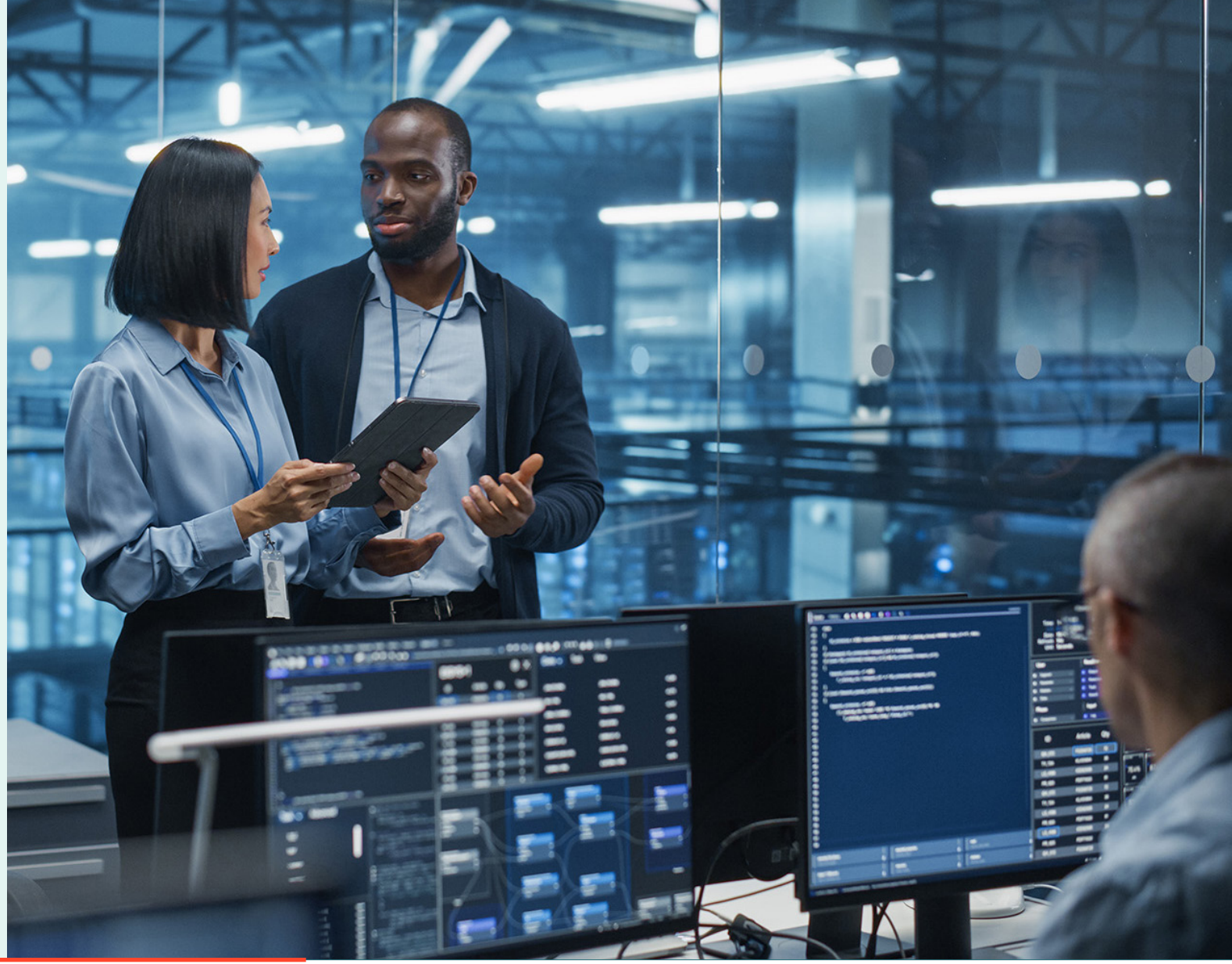
Data exposure is now inevitable and demands action

Executives at the CISO Expert Exchange shared real examples of sensitive data and intellectual property appearing in public repositories and cloud environments. These breaches were usually the result of speed, experimentation and outdated policy frameworks.

CISOs now know that preventing every instance of data exposure is unrealistic.

Instead, leading organizations are focusing on continuous monitoring, rapid detection and coordinated response across legal, security and operations. This approach shifts focus toward minimizing impact rather than attempting a perfect level of prevention.

Claim control in the age of AI →



06

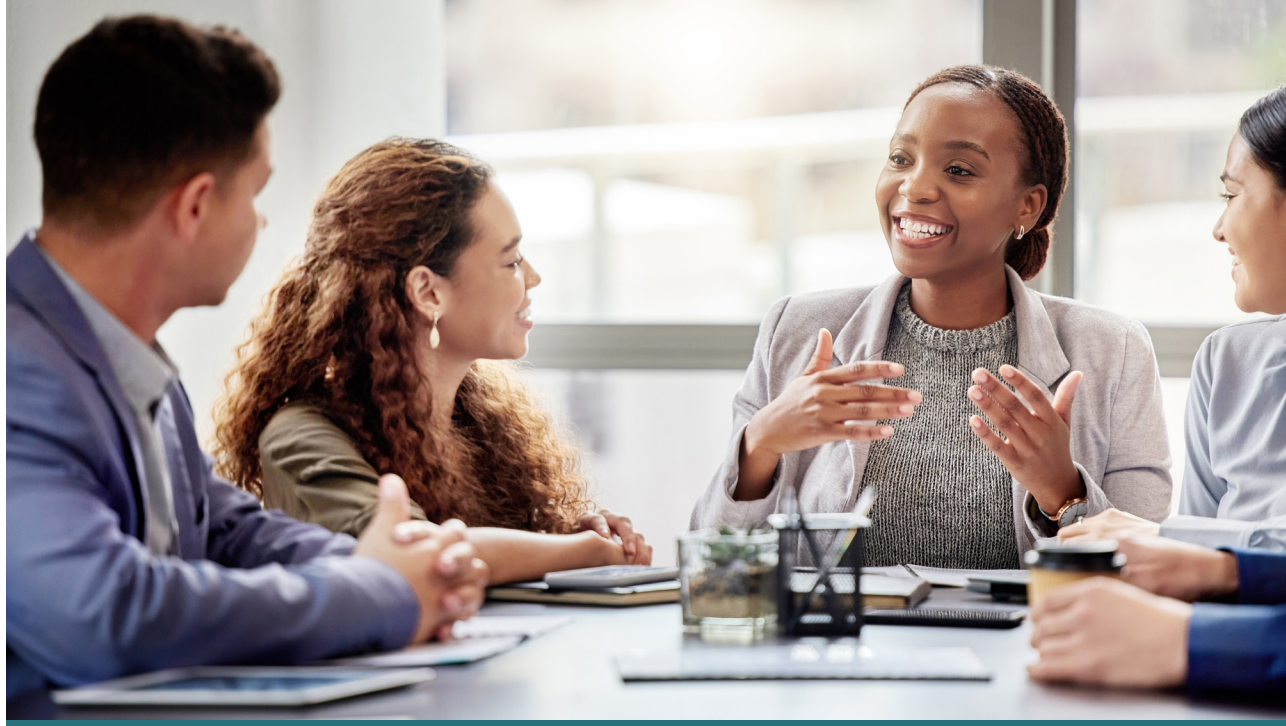
The new mandate for technology leadership

Taken together, these insights point to a defining reality: The biggest near-term challenge of AI adoption is not gaining more sophistication, but managing the volume of its impacts.

AI adoption means more vulnerabilities, agents, alerts, data flows and decisions, all accelerating simultaneously. CISOs, CIOs and CTOs are now governing risk in real time under constant pressure to enable speed without losing control.

The organizations—and CISOs—that succeed will be those that invest in visibility, prioritization, automation and resilience to rise to the AI management challenge.

Changing role of the CISO →



Benchmarks for AI-era technology leaders:

- → **Resilience**
- → **Transparency**
- → **Recovery at speed**

07

What is the Kyndryl CISO Expert Exchange?

The Kyndryl CISO Expert Exchange is a curated, peer-driven program that brings together CISOs and senior IT leaders for meaningful collaboration and shared learning. There are CISO Expert Exchange communities in the U.S., Canada and Europe.

The April 2026 conversation was moderated by Paul Savil, Global Practice Leader Cyber Resilience & Connectivity at Kyndryl.

Paul Savill
Global Practice Leader Cyber Resilience & Connectivity

Visit Kyndryl CISO Expert Exchange →

08

Kyndryl cyber resilience services

Kyndryl helps organizations transition from their current infrastructure to a high-performance, AI-native future. Our security and resiliency services are designed to accelerate growth and innovation, offering scalable solutions that protect data and AI assets, ensure compliance, and stay ahead of emerging threats. We secure mission-critical infrastructures and develop AI-native capabilities by combining strategic advice with hands-on execution, empowering leaders to confidently pursue growth and innovation. Learn more at Kyndryl.com.

kyndryl