Navigating a New Frontier of Risk

How to Safeguard Trust in the Age of Deepfakes, Agentic AI, and Insider Threats

Trust Every Digital Moment



Artificial intelligence (AI) has opened a new frontier for enterprises worldwide, but it's also expanding the threat surface in ways traditional security models aren't equipped to handle. From deepfake-enabled fraud and AI-enhanced insider threats to the rise of autonomous AI agents acting on behalf of users, CIOs and CISOs face new challenges that blend speed, scale, and deception.

To stay ahead, organizations must not only secure AI agents and digital workers that enhance workforce productivity, but also have the ability to verify their legitimacy, ensure they are not overprovisioned, and detect when they've been hijacked by malicious actors. Identity is now the most strategic control point for distinguishing between trusted and compromised entities—human or machine. An adaptive, identity-first security model is critical for detecting, preventing, and responding to these evolving threats, while enabling the business to scale AI safely and securely.

This brief outlines the emerging risks, strategic defenses, and the central role of identity in securing your organization.

Identity is now the most strategic control point for distinguishing between trusted and compromised entities—human or machine.

The Escalating Impact of AI-Driven Threats

AI is a force multiplier for cybercrime:

- Deepfakes and synthetic media are now being used in targeted attacks, from impersonating executives for wire fraud to bypassing voice-based authentication in call centers.
- Insider threats, whether malicious, negligent, or compromised, remain one of the most difficult risks to detect. Fortune 500 companies have unwittingly hired thousands of software engineers who claimed to be U.S. developers but are, in fact, North Korean operatives using a combination of AI and stolen or fake identities. These actors often operate with legitimate access, making their actions hard to distinguish from routine activity
- Generative AI (GenAI) empowers adversaries to scale social engineering, mimic communications across languages and roles, and automate reconnaissance and exploitation. In the financial sector alone, generative AI is expected to drive fraud losses to as much as $40 billion in the United States alone by 2027, up from $12.3 billion in 2023, with a compound annual growth rate of 32%.
- Agentic AI is transforming the way organizations do business, but AI agents – whether they are internally – managed as digital workers or coming from outside parties such as customers or partners, raising new security concerns. With 81% of organizations surveyed in 2025 predicted to adopt AI agents in the next 12-18 months, security frameworks must evolve to ensure these accounts are not overprovisioned or susceptible to hijacking.

Without visibility, real-time risk detection, and secure identity frameworks, organizations face increasing exposure to financial losses, operational disruption, and erosion of trust.

Identity-First Security for the AI-Transformed Enterprise

With the rise of deepfakes, credential theft, and synthetic identities, an identity-first security approach is critical to mitigating AI-driven threats because identity is now the primary attack surface. By anchoring security around who is accessing what, from where, and under what conditions, CIOs and CISOs gain the visibility and control needed to detect anomalies, enforce Zero Trust, and respond to evolving threats in real time.

A modern identity and access management (IAM) platform helps organizations secure their digital ecosystems with an adaptive, identity-first security model that treats identities—of users, devices, and now intelligent agents—as the foundation of Zero Trust. As AI agents become embedded in business workflows, a comprehensive identity platform ensures these non-human identities are onboarded securely, continuously verified, and monitored for behavioral anomalies, helping organizations detect both valid, authorized AI agents and potential agent hijacking.

Key Identity-First Capabilities CIOs & CISOs Can Leverage

A unified identity platform built to defend against AI-era threats enables full lifecycle control and visibility for both human and non-human identities:

- AI-Aware Identity Security: Contextual and risk-based authentication, real-time monitoring, and behavioral analytics detect deepfakes, anomalous access, and impersonation attempts, including malicious or hijacked AI agents acting outside of established behavioral norms.
- Identity for AI Agents: Secure onboarding, authentication, authorization, and governance of AI agents allows organizations to verify agent legitimacy, bring the human into the loop as necessary, and monitor for takeover attempts or misuse, with full policy enforcement and auditability.
- Deepfake and Synthetic Identity Detection: Uses liveness detection, spectral artifact analysis, and biometric validation to prevent fraudulent access attempts at onboarding and login—critical for protecting high-risk workflows and remote channels.
- Insider Threat Protection: Combines real-time behavioral analytics, contextual risk scoring, and fine-grained access control to detect unusual activity across both human users and AI agents. Capabilities like identity orchestration, adaptive authentication, and continuous monitoring can identify when trusted users—whether human or AI agents—begin acting outside expected patterns, enabling automated policy responses to contain threats before damage occurs.
- Unified Identity Architecture: A unified identity platform secures all user types—workforce, customer, partner, and non-human—across every access use case, eliminating silos and reducing complexity.

With the rise of deepfakes, credential theft, and synthetic identities, an identity-first security approach is critical to mitigating AI-driven threats because identity is now the primary attack surface.

Business ROI, Enablement, and Resilience

Leveraging these capabilities, CIOs and CISOs can:

- Reduce breach risk and fraud-related losses by proactively identifying and stopping AI-enhanced threats at the identity layer.
- Enable high-trust, low-friction user experiences, critical for customer retention, partner trust, and employee productivity.
- Streamline compliance by maintaining a defensible posture across evolving data protection and AI regulation landscapes.
- Demonstrate measurable security ROI, linking identity investments to business outcomes such as cost savings, increased speed to market, and reduced risk and fraud.

Protect and Empower Your Business

Defending against AI-driven threats demands more than incremental improvements; it requires a strategic shift. And, as AI agents become part of the workforce, they bring both productivity and risk—IAM systems must evolve to securely onboard, manage, and monitor these digital workers.

This new paradigm calls for adaptive, AI-aware identity strategies with context-driven controls, risk-based authentication, and continuous monitoring. Identity is the modern control plane,
and when enhanced with intelligence and automation, it becomes the enterprise's most effective defense against deepfakes, insider threats, agent hijacking, and whatever AI-driven attack comes next.

By investing in identity-first security, organizations can shift from reactive AI threat mitigation to proactive resilience, protecting not just systems, but brand equity, shareholder value, and long-term growth.

Don't Be Fooled by Deepfakes
Learn how to spot and stop AI-driven deception.
Get the eBook.