BeyondID

The Confidence Paradox:
Delusions of Readiness in Identity Security

CONFIDENCE IS HIGH

74% of respondents rate their identity maturity "Established" or "Advanced."

Of organizations say they're confident in detecting an identity-related breach within 24 hours.

85% believe their organization is ready for AI in security.

Security leaders say they're confident. But are they truly prepared?

Our 2025 survey of U.S.-based IT decision-makers reveals a sharp disconnect between how organizations perceive their identity security posture and how they actually operate. This is the Confidence Paradox: high self-reported maturity and breach readiness contrasted with low adoption of best practices, underinvestment in identity, and limited oversight of emerging risks...especially those introduced by AI.

Many organizations claim to be "advanced," yet follow fewer best practices than their peers. Most say they're ready for AI, but few apply fundamental identity governance to non-human agents. And while breaches tied to compromised credentials remain widespread, identity security often remains underfunded and inconsistently managed.

The result is more than a gap, it's a systemic misalignment between perception and reality. A kind of operational overconfidence that leaves organizations exposed. This report explores the root causes of the Confidence Paradox and outlines the steps security teams must take to move from assumed readiness to proven resilience.

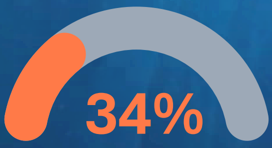
BEHAVIOR TELLS A DIFFERENT STORY

OF ORGANIZATIONS SELF-IDENTIFYING AS "ADVANCED"...

The average follows only 4.7 out of 12 best practices. That's fewer than their "Established" peers, who follow 5.1.

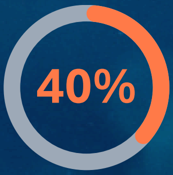
< 3 in 10

Allocate more than 20% of their cybersecurity budget to identity security.

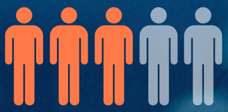


Have failed a compliance audit due to identity-related issues; 14% failed multiple.

Only 27% enforce a least privilege access model, despite it being a fundamental security practice.



Less than half conduct regular user access reviews, leaving them vulnerable to unnecessary or dated permissions.

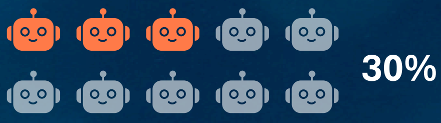


Only 3 in 5 enforce multi-factor authentication - a basic security measure.

These figures show a concerning pattern: organizations may feel secure, but they're not investing or executing at the levels that would support that belief.

Now, AI is Making Matters Worse.

85% of IT leaders believe they're ready for AI in security, and **37%** name AI impersonation of users a top concern.



Only **30%** of organizations regularly map non-human identities like AI agents to critical assets.

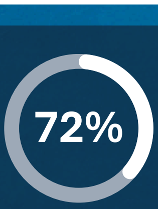
Leaders are eager to adopt AI as a tool, but slower to treat it as a serious threat.

While AI adoption is accelerating, governance is not keeping pace. Most organizations treat AI as an innovation driver, not a security risk to manage.

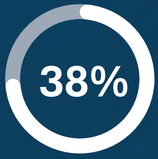
Few apply behavioral oversight or identity governance to AI agents, leaving a growing class of non-human actors outside standard controls.

This isn't just a technical gap, it's a strategic one. As identity programs expand, AI remains a notable blind spot in even the most confident organizations.

THREATS AREN'T SLOWING DOWN



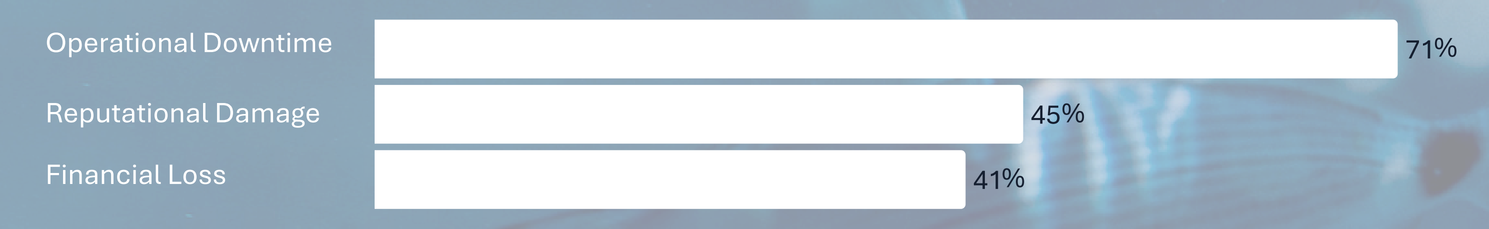
Of organizations experienced at least one attack in the past 24 months. 46% have experienced multiple.



Of those breaches stemmed from compromised employee credentials

These realities undermine the narrative of readiness. If confidence equaled preparedness, these incidents would be far less common.

TOP 3 CONSEQUENCES OF A BREACH



THE BOTTOM LINE

Self-reported maturity means little without demonstrated security rigor. The Confidence Paradox highlights a systemic issue in identity programs: overconfidence without operational discipline.

RECOMMENDATIONS

Benchmark Identity Maturity Against Best Practices

Few apply behavioral oversight or identity governance to AI agents, leaving a growing class of non-human actors outside standard controls.

Invest Where the Risk Begins

Identity is the new perimeter. Budgets should reflect its importance.

Treat AI Like a User

Few apply behavioral oversight or identity governance to AI agents, leaving a growing class of non-human actors outside standard controls.

Close the Confidence Gap

Make continuous improvement and reassessment the cornerstone of your identity strategy.

Want to know where you stand?

Schedule a consultation with BeyondID to benchmark your identity maturity and secure your future with confidence that counts.

info@beyondid.com

www.beyondid.com