MISPLACED TRUST: INSIDE THE WORKPLACE'S NEW AI SECURITY BLIND SPOT

High trust. Low visibility.

Employees are trusting AI with their logins, often without IT knowing. Here's what we learned from 3,000 employees and 800 IT and security leaders in the U.S., the U.K., and France.

48%

Workers trust AI with credentials faster than new co-workers

48% of employees would lend their login credentials to a new AI tool after a week, vs. 42% for a new human co-worker. Nearly half (46%) regularly say "please" and "thank you" to AI.

21%

Employees are granting AI virtually unrestricted access

21% of employees have shared a password, API key, or login credential with an AI tool or agent, and 52% would comply if AI asked them to confirm their login credentials every day.

61%

Pressure to adopt AI is creating security gaps

61% of IT and security leaders say pressure to move fast is the biggest barrier to securing AI agents. Over half (53%) say AI tools are deployed without a security review, and 71% of organizations have granted AI agents standing access to internal systems or data.

98%

That pressure creates blind spots where shadow AI thrives

98% of organizations have discovered AI agents after deployment, yet 89% of IT and security leaders are at least somewhat confident they know about every agent in use. And 28% of employees say they use AI tools their employer doesn't know about.

72%

Choosing speed over security has real-world consequences

72% of organizations report a security incident involving an AI agent's credentials or access in the past 12 months. And 54% of IT and security leaders aren't fully confident they'd know about every AI-related incident.

Get the full report

Download the report

Source: Dashlane survey of 3,000 employees and 800 IT and security leaders in the U.S., the U.K., and France conducted August to September 2026.