KEEPER

Identity Security at Machine Speed

USA

New research from Keeper Security explores how AI, disconnected tools and unmanaged access are leaving U.S. organizations exposed.

93%

The vast majority of U.S. organizations say managing a growing number of identities is at least somewhat challenging.

- 20% Extremely challenging
- 30% Very challenging
- 29% Moderately challenging
- 14% Slightly challenging

34% of U.S. organizations face attempted cyber attacks at least once a day, compared to just 25% globally.

What the Data Reveals

73% report disconnected or poorly integrated security tools create exploitable gaps – 10 points higher than the global average

67% say their organization has an AI security gap, including lack of visibility into the AI tools employees use and oversight of AI-driven access

53% plan to invest in AI security tools in the next 12 months, the top-ranked security investment category among U.S. respondents

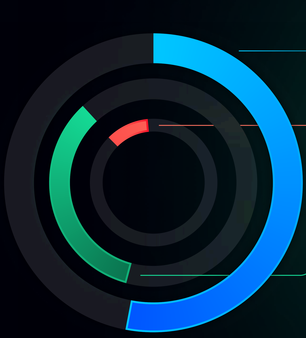
What This Means

U.S. organizations face more frequent attacks than their global peers, and the identity gaps that enable them are growing. Disconnected tools, ungoverned AI and incomplete privileged access controls are leaving identity ecosystems exposed, and most won't know until hours after the fact.

57% lack fully deployed privileged access controls – leaving credentials and access pathways exposed.

Most Organizations Are Already Behind When Misuse Begins

U.S. organizations are losing critical time before credential threats are ever detected.



- 53% Within hours
- 34% Within minutes
- 11% Within days

Methodology

U.S. data based on 500 responses from cybersecurity decision-makers. Global study: 3,200 respondents across North America, Europe, Asia-Pacific and the Middle East, Q1 2026. Explore the full findings at keepersecurity.com.