KEEPER

Identity Security at Machine Speed

UK

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

89%

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

- 12% Extremely challenging
- 29% Very challenging
- 34% Moderately challenging
- 14% Slightly challenging

23% of U.K. organisations face attempted cyber attacks at least once a day, compared to just 25% globally.

What the Data Reveals

67% report disconnected or poorly integrated security tools create exploitable gaps – 10 points higher than the global average

55% say their organisation has an AI security gap, including lack of visibility into the AI tools employees use and oversight of AI-driven access

50% plan to invest in AI security tools in the next 12 months, the top-ranked security investment category among U.K. respondents

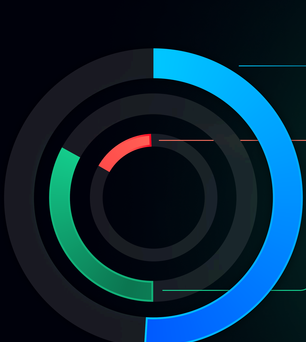
What This Means

U.K. organisations are balancing complex, multi-tool security environments with relatively strong real-time detection – highlighting both progress in visibility and ongoing integration challenges.

60% lack fully deployed privileged access controls – leaving credentials and access pathways exposed.

Most Organisations Are Already Behind When Misuse Begins

U.K. organisations are losing critical time before credential threats are ever detected.



- 51% Within hours
- 33% Within minutes
- 16% Within days

Methodology

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