
KEEPER®

# Identity, AI and Zero Trust

## Cybersecurity Perspectives from Infosecurity Europe, Black Hat USA and it-sa Expo & Congress

Global Conference Report 2025

# Executive Summary

In 2025, Keeper Security surveyed more than 370 cybersecurity professionals at three leading global conferences – Infosecurity Europe in London, Black Hat USA in Las Vegas and it-sa in Nuremberg. Despite differences in geography, regulation and representative organisational size, the findings reveal a shared reality: identity is the new perimeter.

Across Europe and North America, identity has become the defining battleground for cybersecurity professionals. As organisations expand into hybrid, multi-cloud and AI-enabled environments, the number of digital identities has proliferated. Every user, device and service account represents a potential entry point, and each unmanaged credential increases risk – with the number of non-human identities increasing exponentially.

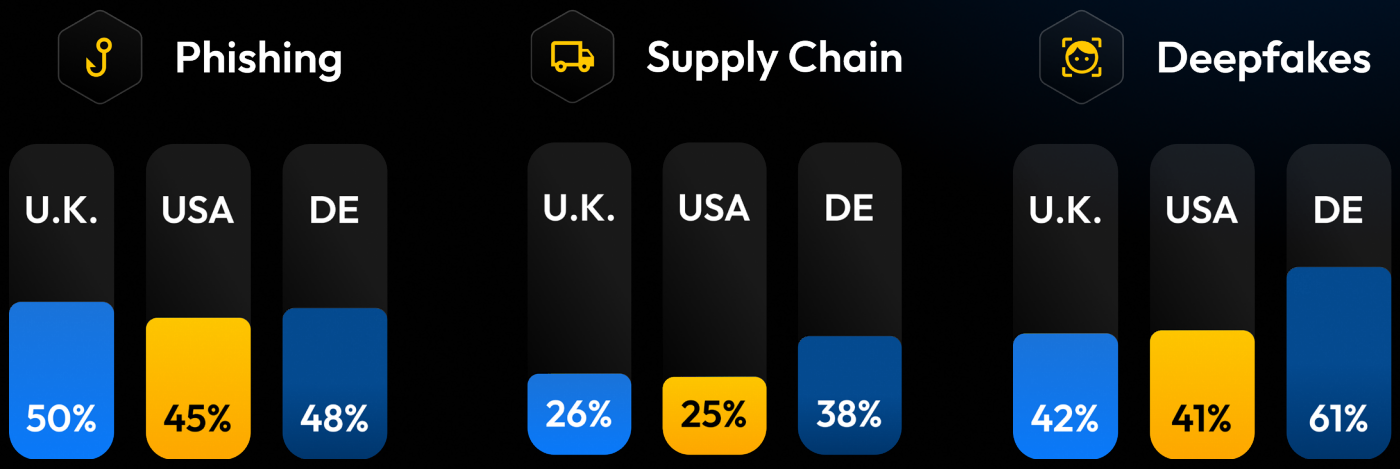
Artificial Intelligence (AI) is reshaping this landscape on both sides of the fight. Attackers are using AI to automate phishing, deepfake impersonations, ransomware and privilege escalation, while defenders are turning to AI-driven identity validation and behavioral analytics to strengthen authentication and detect anomalies. The pace of this evolution is accelerating, and organisations must adapt quickly.

Security leaders understand the path forward: strengthen privileged access controls, modernise authentication and turn zero trust from strategy into practice. Yet progress is often slowed by complexity, competing priorities and lack of executive alignment. The result is an execution gap between awareness and action, and threat actors are exploiting it with speed and precision.

While the global security community has embraced identity-first principles, implementation remains uneven. Closing this gap will determine which organisations can truly achieve resilience against modern threats.

## Most Concerning Identity-Based Threats by Region




# Identity as the Primary Attack Vector

Identity-based threats have overtaken all other forms of cyber risk, emerging as the most common cause of security incidents across every region. Phishing, credential theft, deepfakes and privilege misuse now rank ahead of ransomware as the most likely source of a major breach in the next twelve months.

At Infosecurity Europe, 50% of respondents identified phishing as the top identity-based threat, followed by 42% who pointed to deepfakes and 26% who cited supply-chain attacks. In the United States, the results were nearly identical: 45% named phishing as their primary concern, 41% highlighted deepfakes and 25% referenced supply-chain compromise. In Germany, concern around AI-enhanced deception was even higher, with 61% identifying deepfakes as their leading threat, 48% citing phishing and 38% citing supply-chain compromise.

These findings underscore a growing consensus that identity has become the universal vulnerability in cybersecurity. Attackers are exploiting weaknesses in authentication and access controls to target users rather than networks. Across regions, inconsistent MFA enforcement, fragmented identity tools and limited visibility into privileged credentials continue to create exploitable gaps.

The data highlights an urgent need for modernisation. Outdated authentication methods and incomplete identity governance have left organisations vulnerable to the same attacks year after year. As identity replaces the network perimeter, effective protection now depends on unified controls, centralised visibility and strong authentication reinforced by real-time monitoring and anomaly detection.

# AI Is a Double-Edged Sword

AI has become both a transformative defence capability and a rapidly escalating threat. Across all three regions, confidence in managing AI-powered attacks remains low. Only 12% of respondents in the UK and 16% in the United States said their organisations are fully prepared to handle AI-enhanced threats. In Germany, 28% described themselves as ready, although nearly one-third said they remain only somewhat confident.

Despite these concerns, optimism toward AI's defensive potential is strong. Respondents across every region identified AI-driven identity validation and authentication as the most transformative technology for identity and access security in the next three to five years. In the UK, 53% selected AI-driven validation as the most impactful innovation, compared with 57% in the United States and 60% in Germany. Other emerging technologies, including passwordless authentication, automated identity management and quantum-resistant encryption, ranked significantly lower by comparison.

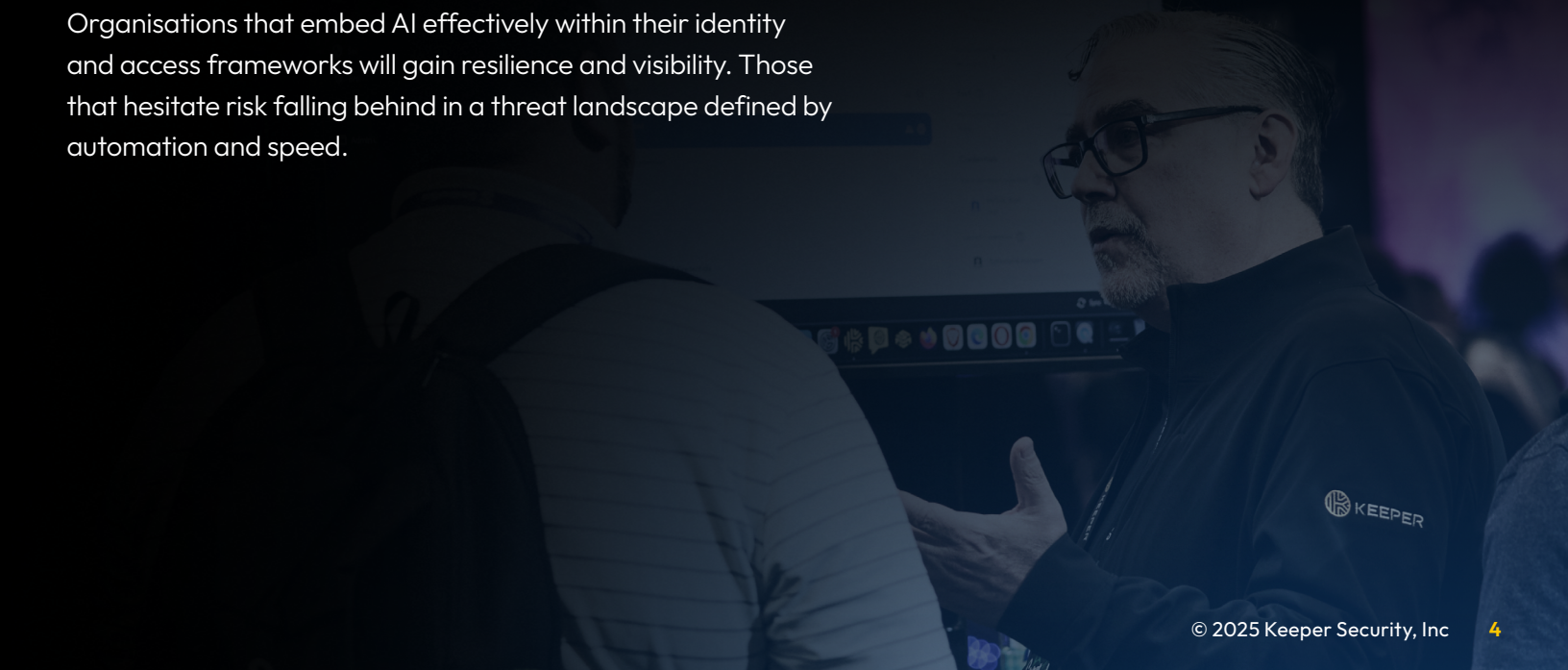
AI is simultaneously rewriting both the offensive and defensive playbooks. Threat actors are leveraging it to craft more convincing phishing campaigns, deepfakes and credential attacks, while defenders are adopting AI to identify anomalies, validate identities and predict malicious behavior in real time. Organisations that embed AI effectively within their identity and access frameworks will gain resilience and visibility. Those that hesitate risk falling behind in a threat landscape defined by automation and speed.

## Confidence in Handling AI-Driven Threats


U.K.

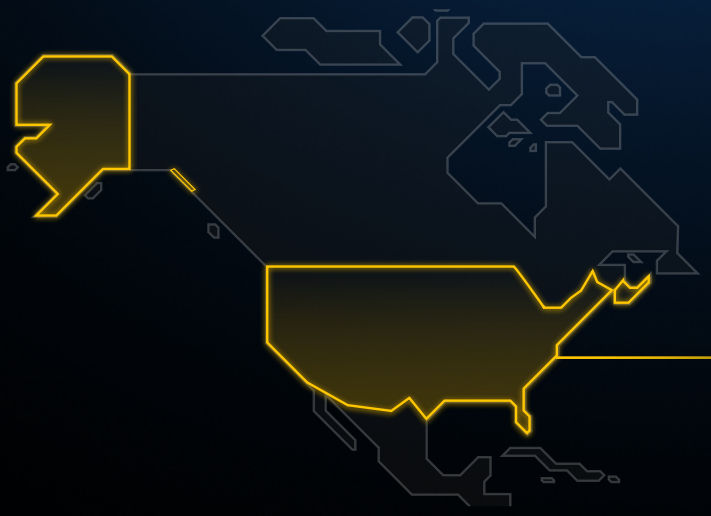

United States


Germany



# Technology Expected to Transform Identity Security



## USA

**57%** AI-driven identity validation and authentication

**26%** Automated identity management

**38%** Passwordless authentication

**28%** Quantum-resistant encryption

## U.K.

**53%** AI-driven identity validation and authentication

**30%** Automated identity management

**39%** Passwordless authentication

**24%** Quantum-resistant encryption

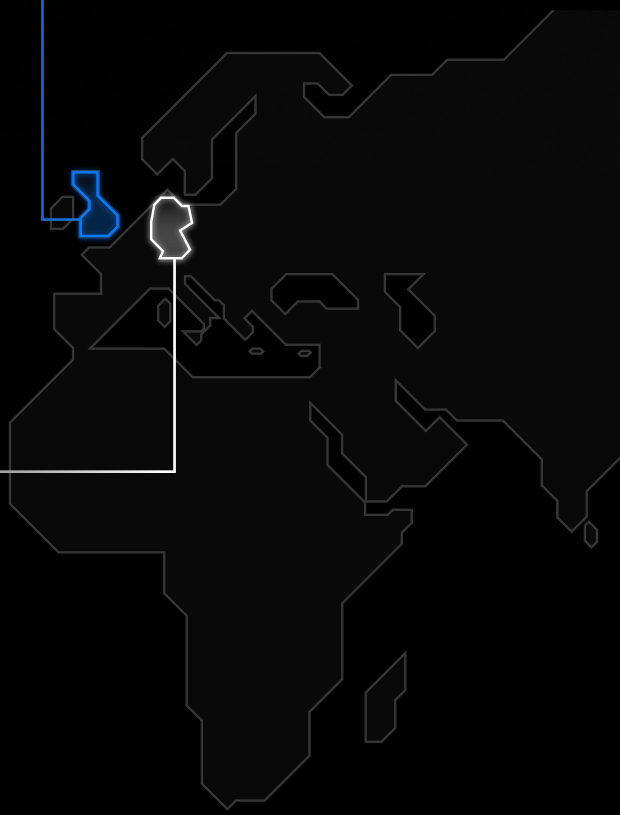
## DE

**60%** AI-driven identity validation and authentication

**30%** Automated identity management

**28%** Passwordless authentication

**18%** Quantum-resistant encryption



# Zero Trust Aspirations vs. Reality

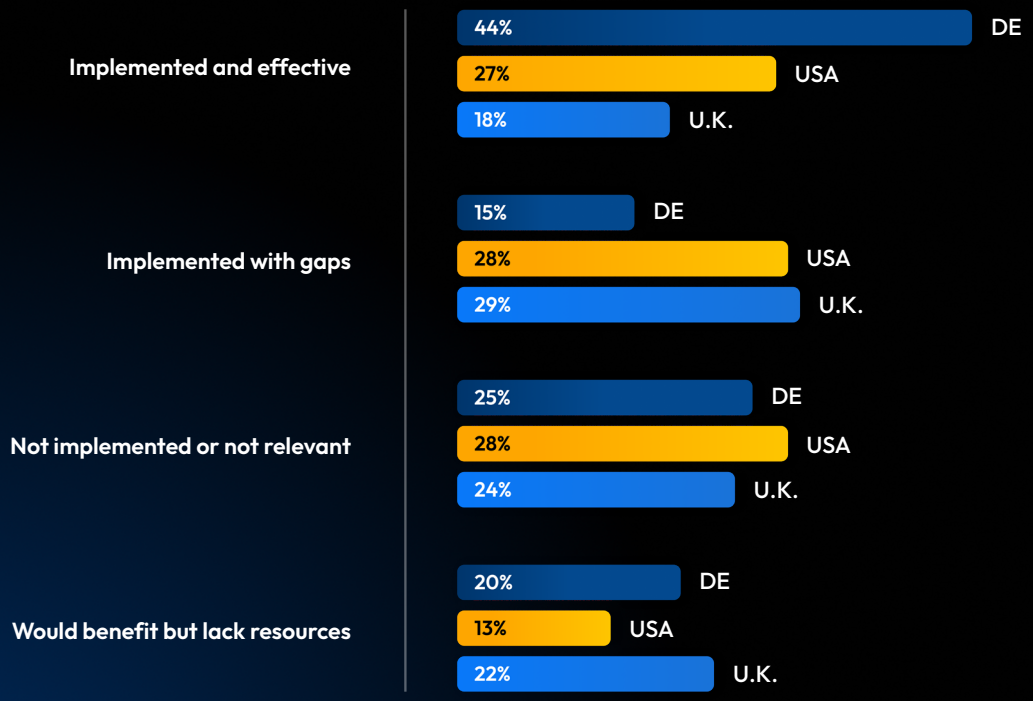
Zero trust has become critical to modern cybersecurity, but implementation continues to lag. At Infosecurity Europe, only 18% of respondents said their organisations have fully implemented an effective zero-trust model. At Black Hat USA, the figure was slightly higher at 27%, while at it-sa in Germany, 44% reported effective implementation – more than twice the rate of their UK peers.

**More than one-third of German organisations cite leadership support as their biggest obstacle to achieving zero trust.**

The barriers to progress are consistent across markets. In the UK, 31% cited budget and resource constraints as the most significant obstacle, followed by 29% who said leadership buy-in is lacking. In the United States, 30% pointed to implementation complexity as the top barrier, while 27% cited difficulty integrating with legacy systems. In Germany, 34% said leadership support remains the greatest challenge, and 32% identified limited budgets as a continuing constraint.

Across every region, zero trust has achieved universal acceptance as a strategic imperative but with uneven maturity in execution. Organisations struggle to balance cost, complexity and internal alignment while integrating modern frameworks with legacy systems.

In the UK, progress toward zero trust is increasingly being shaped by regulatory and strategic frameworks such as the NCSC's Cyber Assessment Framework, the National Cyber Strategy 2022–2030 and the evolving UK alignment with NIS2. These frameworks emphasise identity assurance and access control as the foundation for cyber resilience – yet data reveals many organisations still lack the practical mechanisms to achieve them.



# Privileged Access Controls Remain Inconsistent

Across all three markets, four in ten organisations lack either consistent MFA enforcement or comprehensive PAM coverage. The data reinforces a clear truth: organisations recognise that PAM is essential but continue to underfund and underprioritise it. Without consistent oversight and automation, least-privilege access remains a goal, rather than a guaranteed control.

## U.K.

**43%**
No MFA for privileged accounts

**37%**
No PAM solution

**34%**
Privileges not removed

## USA

**40%**
No MFA for privileged accounts

**33%**
No PAM solution

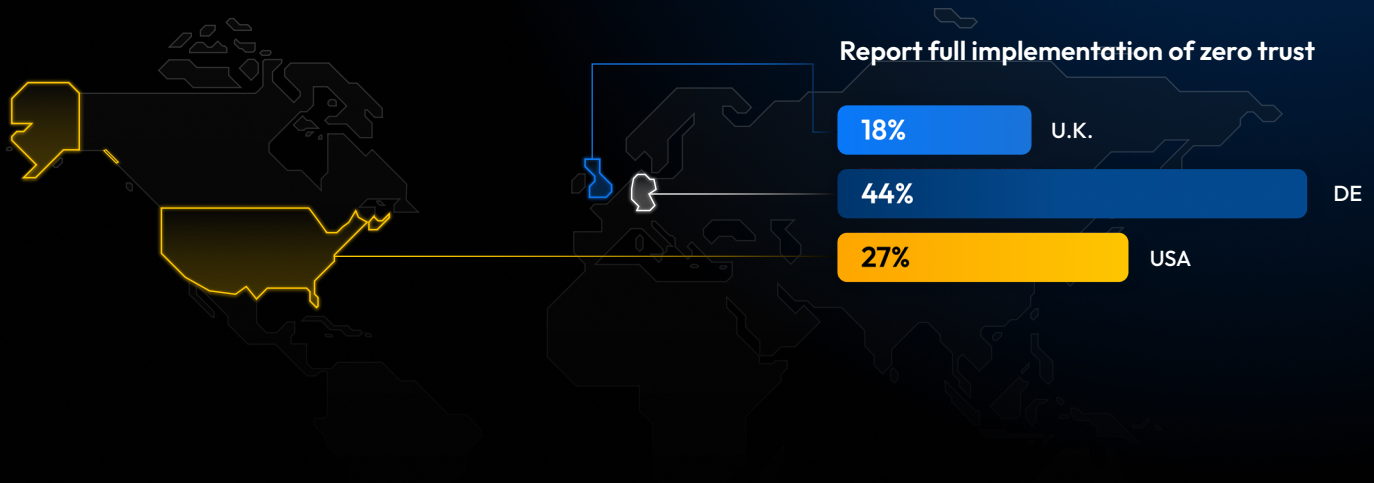
**34%**
Privileges not removed

## DE

**49%**
No PAM solution

**41%**
No monitoring or auditing

**33%**
Weak third-party vetting




# Regional Perspectives

## United Kingdom: Infosecurity Europe

Infosecurity Europe respondents demonstrated strong awareness of identity-related risk but limited readiness to address it. Only 18% reported fully effective zero-trust programs, and just 12% said they feel confident managing AI-generated threats. While 50% identified phishing as their primary concern, more than half also believe that the media exaggerates the severity of AI-driven risks. This disconnect between perception and preparedness suggests that while awareness is high, many UK organisations have yet to translate strategy into measurable action.

## United States: Black Hat USA

Cybersecurity professionals at Black Hat USA reported moderate gains in zero-trust implementation but continue to face similar obstacles. Twenty-seven percent of respondents said their zero-trust models are fully implemented, while 40% acknowledged that MFA is not consistently enforced for privileged accounts. Phishing and deepfakes remain the leading identity-based threats, cited by 45% and 41% of respondents respectively. Despite greater familiarity with AI-driven risks, many United States organisations still struggle to operationalise defences across hybrid environments.

## Germany: it-sa Expo & Congress

Respondents at it-sa displayed higher levels of confidence in their zero-trust maturity and greater optimism about AI's defensive potential. Forty-four percent said zero trust is effectively implemented, and 60% believe AI-driven identity validation will be the most transformative security technology in the next three to five years. However, 34% cited lack of leadership support as their top barrier, and 32% pointed to limited budgets as a persistent challenge. Nearly half (49%) said their organisations lack a dedicated PAM solution. Germany's progress reflects strong strategic alignment with identity-first principles but uneven operational follow-through.

> **Identity has become the control point of cybersecurity. The organisations that lead in zero trust and PAM are not only protecting access but building the foundation for secure, scalable growth in the age of AI.**
>
> **Darren Guccione,**
> **CEO and Co-founder, Keeper Security**

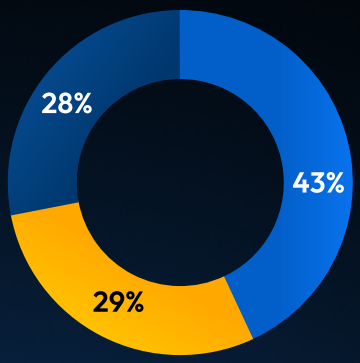
# Keeper Security Insight

Modern cybersecurity is built on the convergence of identity controls, privilege management and intelligent automation. These three forces are redefining how organisations defend their users, data and infrastructure in a constantly evolving threat landscape.

Zero trust and privileged access management are no longer optional. They are the frameworks that enable operational resilience, governance and scalability in modern enterprises. Organisations that move beyond policy statements to execution will not only strengthen their defence but set a new global standard for cybersecurity leadership.

The insights gathered from London, Las Vegas and Nuremberg point to a defining truth: identity is the new perimeter. Resilience now depends on disciplined execution, continuous measurement and the responsible use of AI across every layer of defences. The organisations that act decisively by securing identity, enforcing least privilege and embracing intelligent automation will not simply endure today's threats, they will define the future of cybersecurity worldwide.

## Survey Methodology




**U.K. - 43%**
160 respondents

**United States - 29%**
110 respondents

**Germany - 28%**
103 respondents

Keeper Security collected insights from 373 cybersecurity and IT professionals through anonymous, in-person surveys conducted at Infosecurity Europe in London, Black Hat USA in Las Vegas and it-sa in Nuremberg