KEEPER®

Identität, KI und Zero Trust

Perspektiven zur Cybersicherheit von der it-sa, Infosecurity Europe und der Black Hat USA

Daten von globalen Konferenzen 2025

Kurzfassung

Im Jahr 2025 befragte Keeper Security mehr als 370 Cybersicherheitsexperten auf drei führenden globalen Veranstaltungen – it-sa in Nürnberg, Infosecurity Europe in London und Black Hat USA in Las Vegas. Trotz Unterschieden in Geographie, Regulierung und der Größe der vertretenen Organisationen zeigen die Ergebnisse eine gemeinsame Realität: Identität ist der neue Perimeter.

In Europa und Nordamerika ist die Identität zum entscheidenden Schlachtfeld für Cybersicherheitsexperten geworden. Mit der Expansion von Unternehmen in hybride, Multi-Cloud- und KI-fähige Umgebungen hat sich die Zahl der digitalen Identitäten stark erhöht. Jedes Benutzer-, Geräte- und Dienstkonto stellt einen potenziellen Einstiegspunkt für Cyberkriminalität dar, und jede nicht verwaltete Anmeldeinformation erhöht das Risiko – wobei die Anzahl nicht-menschlicher Identitäten exponentiell zunimmt.

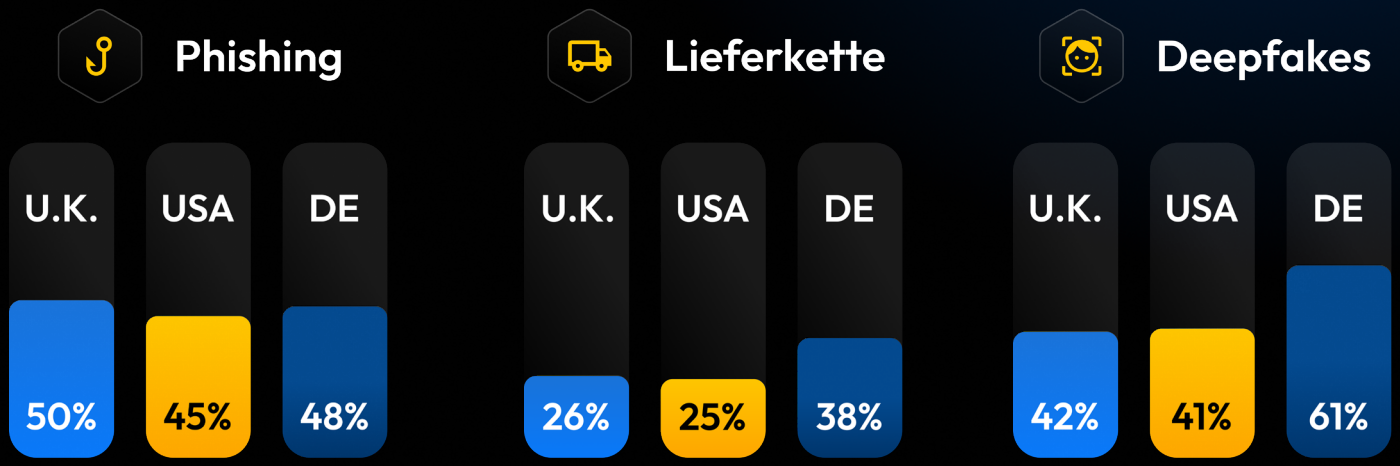
Künstliche Intelligenz (KI) verändert diese Landschaft auf beiden Seiten des Konflikts. Angreifer nutzen KI, um Phishing, Deepfake-Identitätsdiebstahl, Ransomware und Privilegieneskalation zu automatisieren. Gleichzeitig, greifen Verteidiger auf KI-gesteuerte Identitätsvalidierung und Verhaltensanalysen zurück, um die Authentifizierung zu stärken und Anomalien zu erkennen. Das Tempo dieser Entwicklung nimmt zu, und Unternehmen müssen sich schnell anpassen.

Sicherheitsverantwortliche wissen, welchen Weg sie einschlagen müssen: Stärkung der privilegierten Zugriffskontrollen, Modernisierung der Authentifizierung und Umsetzung der Zero-Trust-Strategie in die Praxis. Der Fortschritt wird jedoch oft durch die Komplexität, konkurrierende Prioritäten und die mangelnde Abstimmung der Führungskräfte gebremst. Das Ergebnis ist eine Lücke zwischen Bewusstsein und Handeln, und die Bedrohungsakteure nutzen diese schnell und mit Präzision aus.

Obwohl die globale Sicherheitsgemeinschaft die Prinzipien von Identity-First unterstützt, bleibt die Umsetzung uneinheitlich. Dasi Schließenung dieser Lücke wird darüber bestimmen, welche Unternehmen echte Resilienz gegenüber modernen Bedrohungen erreichen können.

© 2025 Keeper Security, Inc

Die besorgniserregendsten identitätsbasierten Bedrohungen nach Region



Identität als primärer Angriffsvektor

Identitätsbasierte Bedrohungen haben alle anderen Formen von Cyberrisiken überholt und sind in allen Regionen die häufigste Ursache für Sicherheitsvorfälle geworden. Phishing, Diebstahl von Zugangsdaten, Deepfakes und Missbrauch von Privilegien rangieren jetzt vor Ransomware als wahrscheinlichste Ursache für einen größeren Sicherheitsvorfall in den nächsten zwölf Monaten.

In Deutschland war die Besorgnis über KI-gestützte Täuschungen am höchsten: 61 % nannten Deepfakes als größte Bedrohung, 48 % Phishing und 38 % die Gefährdung der Lieferkette. Bei der Infosecurity Europe gaben 50 % der Befragten Phishing als die größte identitätsbasierte Bedrohung an, gefolgt von 42 %, die auf Deepfakes verwiesen, und 26 %, die Angriffe auf die Lieferkette nannten. In den Vereinigten Staaten waren die Ergebnisse fast identisch: 45 % nannten Phishing als ihre Hauptsorge, 41 % nannten Deepfakes und 25 % verwiesen auf die Gefährdung der Lieferkette

Diese Ergebnisse unterstreichen den wachsenden Konsens, dass Identität zur universellen Schwachstelle in der Cybersicherheit geworden ist. Angreifer nutzen Schwächen bei der Authentifizierung und Zugriffskontrollen aus, um Benutzer statt Netzwerke anzugreifen. In allen Regionen schaffen uneinheitliche MFA-Durchsetzung, fragmentierte Identitäts-Tools und begrenzte Transparenz privilegierter Anmeldeinformationen weiterhin ausnutzbare Lücken. Effektiver Schutz hängt jetzt von einheitlichen Kontrollen, zentraler Transparenz und starker Authentifizierung ab, verstärkt durch Privileged Access Management mit Echtzeitüberwachung und KI-gestützter Anomalieerkennung.

Die Daten verdeutlichen den dringenden Modernisierungsbedarf. Veraltete Authentifizierungsmethoden und unvollständige Identitätsverwaltung machen Unternehmen Jahr für Jahr anfällig für dieselben Angriffe. Da die Identität den Netzwerkperimeter ersetzt, hängt ein wirksamer Schutz nun von einheitlichen Kontrollen, zentraler Transparenz und starker Authentifizierung ab, die durch Echtzeitüberwachung und Anomalieerkennung verstärkt werden.

© 2025 Keeper Security, Inc

KI ist ein zweischneidiges Schwert

KI hat sich sowohl zu einer transformativen Verteidigung als auch zu einer schnell eskalierenden Bedrohung entwickelt. In allen drei Regionen bleibt das Vertrauen in die Bewältigung von KI-gestützten Angriffen gering. In Deutschland bezeichneten sich 28 % der Befragten als bereit, vollständig auf den Umgang mit KI-gestützten Bedrohungen vorbereitet zu sein. Fast ein Drittel gab an, diesbezüglich nur einigermaßen zuversichtlich zu sein. Nur 12 % der Befragten im Vereinigten Königreich und 16 % in den Vereinigten Staaten gaben an, dass ihre Unternehmen vollständig auf den Umgang mit KI-gestützten Bedrohungen vorbereitet sind.

Trotz dieser Bedenken ist der Optimismus hinsichtlich des Verteidigungspotenzials der KI groß. Die Befragten aus allen Regionen identifizierten die KI-gesteuerte Identitätsvalidierung und -authentifizierung als die transformativste Technologie für Identitäts- und Zugriffssicherheit in den nächsten drei bis fünf Jahren. In Deutschland wählten 60 % die KI-gesteuerte Validierung als die einflussreichste Innovation, verglichen mit dem Vereinigten Königreich mit 53 % und mit 57 % in den Vereinigten Staaten. Andere aufkommende Technologien, darunter passwortlose Authentifizierung, automatisiertes Identitätsmanagement und quantenresistente Verschlüsselung, wurden im Vergleich deutlich niedriger eingestuft.

Die KI schreibt gleichzeitig sowohl das offensive als auch das defensive Drehbuch neu. Bedrohungsakteure nutzen KI, um überzeugendere Phishing-Kampagnen, Deepfakes und Anmeldeinformationsangriffe zu entwickeln, während Verteidiger KI einsetzen, um Anomalien zu erkennen, Identitäten zu überprüfen und bösartiges Verhalten in Echtzeit zu identifizieren. Unternehmen, die KI effektiv in ihre Identitäts- und Zugriffssysteme einbinden, werden an Ausfallsicherheit und Transparenz gewinnen. Ein Zögern birgt das Risiko, in einer von Automatisierung und Geschwindigkeit geprägten Bedrohungslandschaft ins Hintertreffen zu geraten.

Sicherheit im Umgang mit KI-gesteuerten Bedrohungen

Völlig Sicher

U.K.

Völlig Sicher

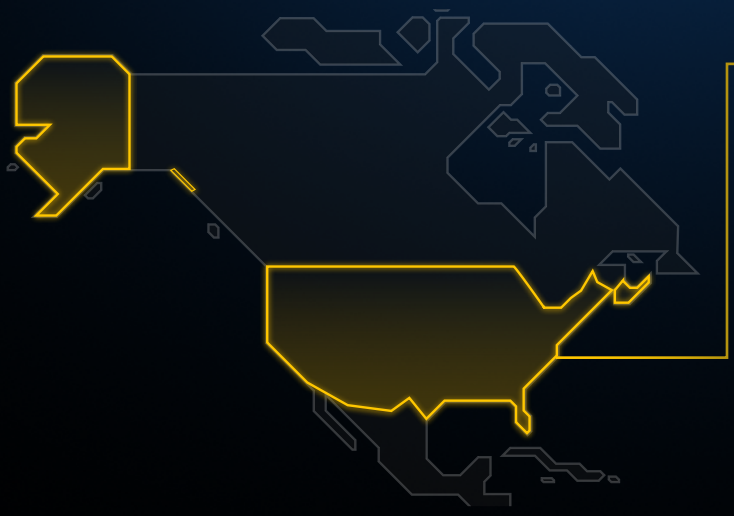
USA

Völlig Sicher

DE

© 2025 Keeper Security, Inc

Technologie, die die Identitätssicherheit voraussichtlich verändern wird



USA

57% KI-gesteuerte Identitätsvalidierung und -authentifizierung

26% Automatisiertes Identitätsmanagement

38% Passwortlose Authentifizierung

28% Quantenresistente Verschlüsselung

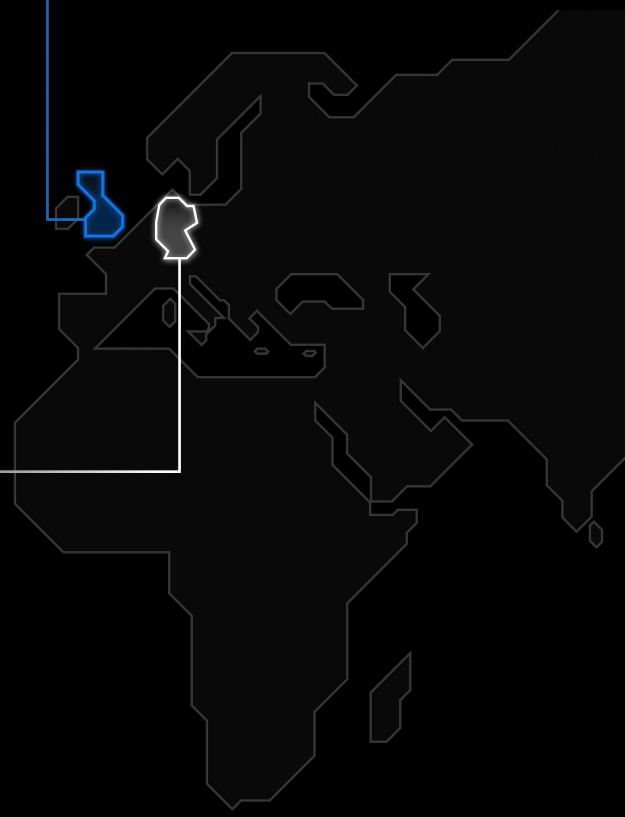
U.K.

53% KI-gesteuerte Identitätsvalidierung und -authentifizierung

30% Automatisiertes Identitätsmanagement

39% Passwortlose Authentifizierung

24% Quantenresistente Verschlüsselung



DE

60% KI-gesteuerte Identitätsvalidierung und -authentifizierung

30% Automatisiertes Identitätsmanagement

28% Passwortlose Authentifizierung

18% Quantenresistente Verschlüsselung

© 2025 Keeper Security, Inc

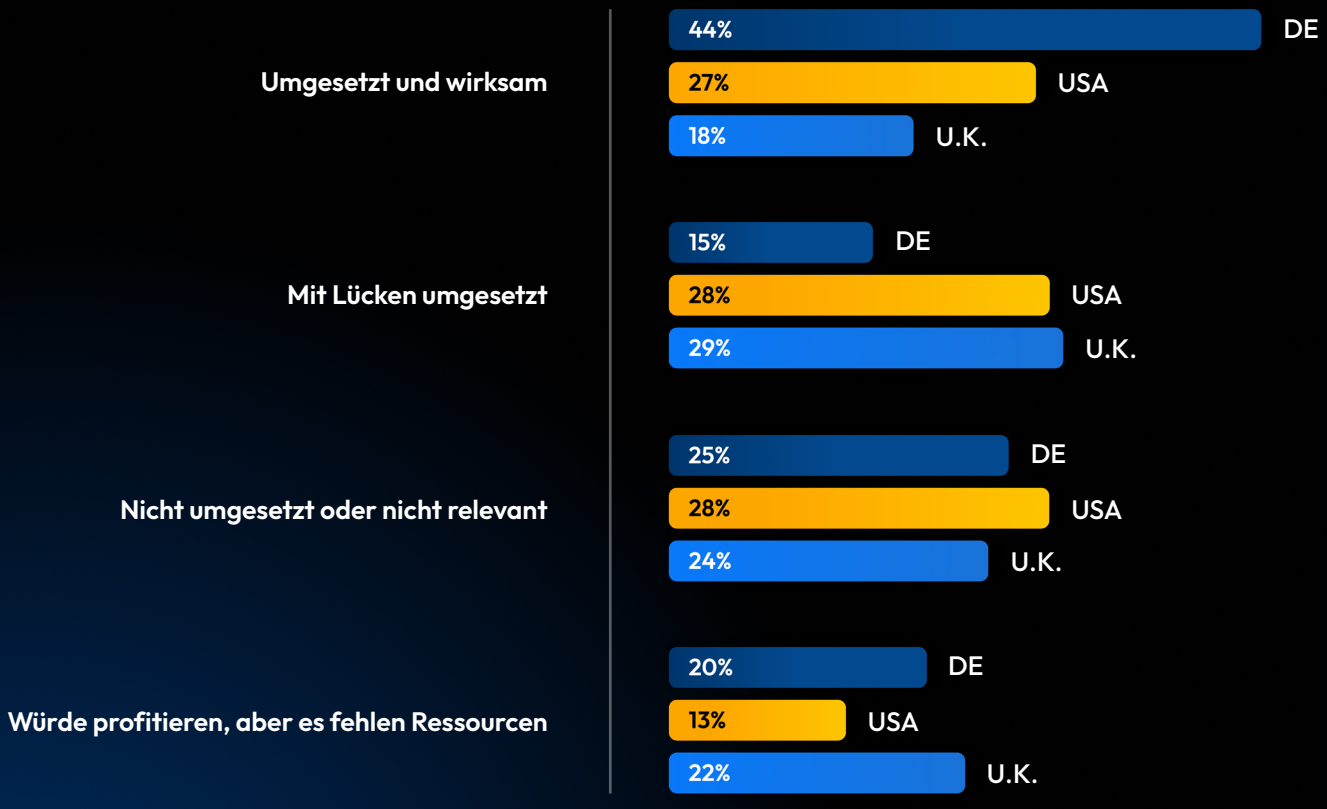
Zero Trust – Anspruch und Wirklichkeit

Zero Trust ist für die moderne Cybersicherheit von entscheidender Bedeutung geworden, aber die Implementierung hinkt weiterhin hinterher. Auf der der it-sa in Deutschland berichteten 44 % der Befragten von einer effektiven Umsetzung. Dieses Ergebnis ist mehr als doppelt so hoch wie auf der Infosecurity Europe mit nur 18 %. Auf der Black Hat USA lag die Zahl mit 27 % als, im Vereinigten Königreich

Mehr als ein Drittel der deutschen Organisationen nennt fehlende Unterstützung durch die Geschäftsführung als größtes Hindernis bei der Umsetzung von Zero Trust.

Die Hindernisse für den Fortschritt sind in allen Märkten gleich. In Deutschland gaben 34 % an, dass die Unterstützung der Führungsebene nach wie vor die größte Herausforderung darstellt, und 32 % nannten begrenzte Budgets als anhaltende Einschränkung. Im Vereinigten Königreich nannten 31 % Budget- und Ressourcenknappheit als größtes Hindernis, gefolgt von 29 %, die angaben, dass es an der Unterstützung der Führungsebene mangelt. In den Vereinigten Staaten nannten 30 % die Komplexität der Implementierung als größtes Hindernis, während 27 % Schwierigkeiten bei der Integration mit Altsystemen anführten.

In allen Regionen hat sich Zero Trust als strategischer Imperativ durchgesetzt, allerdings mit ungleicher Reife in der Umsetzung. Unternehmen kämpfen damit, ein Gleichgewicht zwischen Kosten, Komplexität und interner Abstimmung zu finden, während sie moderne Frameworks mit Altsystemen integrieren. Daher bleibt Zero Trust eher ein Ziel als ein vollständig umgesetztes Modell.



Privilegierte Zugriffskontrollen bleiben uneinheitlich

In allen drei Märkten fehlt es vier von zehn Unternehmen entweder an einer konsequenten MFA-Durchsetzung oder an einer umfassenden PAM-Abdeckung. Die Daten unterstreichen eine klare Tatsache: Unternehmen erkennen zwar die Bedeutung von PAM, investieren jedoch weiterhin zu wenig in diesen Bereich und räumen ihm keine Priorität ein. Ohne konsistente Überwachung und Automatisierung bleibt der Zugriff mit geringsten Rechten ein Ziel und keine garantierte Kontrolle.

U.K.

43%
Keine MFA für privilegierte Konten

37%
Keine PAM-Lösung

34%
Berechtigungen nicht entfernt

USA

40%
Keine MFA für privilegierte Konten

33%
Keine PAM-Lösung

34%
Berechtigungen nicht entfernt

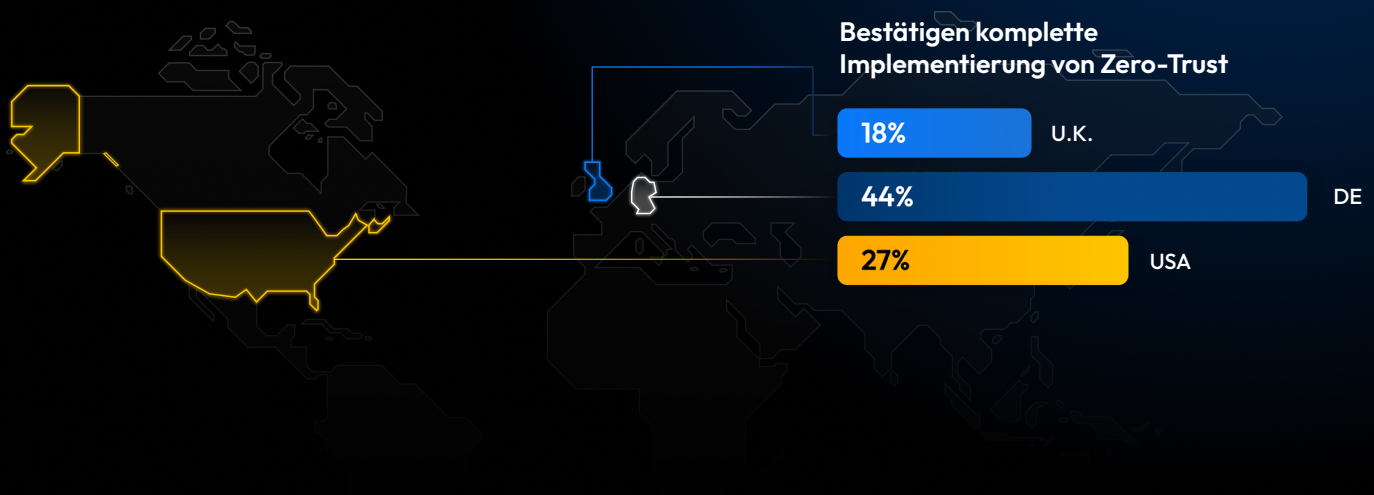
DE

49%
Keine PAM-Lösung

41%
Keine Überwachung oder Prüfung

33%
Schwache Drittpartei-Überprüfung

© 2025 Keeper Security, Inc



Regionale Perspektiven

Vereinigtes Königreich: Infosecurity Europe

Die Befragten der Infosecurity Europe zeigten ein starkes Bewusstsein für identitätsbezogene Risiken, aber eine begrenzte Bereitschaft, diese anzugehen. Nur 18 % berichteten über vollständig wirksame Zero-Trust-Programme, und nur 12 % gaben an, dass sie sich im Umgang mit KI-generierten Bedrohungen sicher fühlen. Während 50 % Phishing als ihre größte Sorge bezeichneten, glaubt mehr als die Hälfte zudem, dass die Medien das Ausmaß der KI-bedingten Risiken übertreiben. Diese Diskrepanz zwischen Wahrnehmung und Bereitschaft deutet darauf hin, dass das Bewusstsein zwar hoch ist, viele britische Unternehmen ihre Strategie aber noch nicht in messbare Maßnahmen umgesetzt haben.

Vereinigte Staaten: Black Hat USA

Cybersicherheitsexperten auf der Black Hat USA berichteten von moderaten Fortschritten bei der Zero-Trust-Implementierung, stehen jedoch weiterhin vor ähnlichen Hindernissen. 27 % der Befragten gaben an, dass ihre Zero-Trust-Modelle vollständig implementiert sind, während 40 % einräumten, dass MFA für privilegierte Konten nicht konsequent durchgesetzt wird. Phishing und Deepfakes bleiben mit 45 % bzw. 41 % der Befragten die größten identitätsbasierten Bedrohungen. Trotz größerer Vertrautheit mit KI-gesteuerten Risiken haben viele Unternehmen in den Vereinigten Staaten immer noch Schwierigkeiten, Verteidigungsmaßnahmen in Hybridumgebungen zu operationalisieren.

Deutschland: it-sa Expo & Congress

Die Befragten der it-sa zeigten ein höheres Vertrauen in ihre Zero-Trust-Reife und einen größeren Optimismus hinsichtlich des Verteidigungspotenzials von KI. 44 % gaben an, dass Zero-Trust effektiv umgesetzt wird, und 60 % glauben, dass die KI-gesteuerte Identitätsüberprüfung die transformativste Sicherheitstechnologie in den nächsten drei bis fünf Jahren sein wird. Allerdings nannten 34 % die mangelnde Unterstützung durch die Führung als größtes Hindernis und 32 % nannten begrenzte Budgets als anhaltende Herausforderung. Fast die Hälfte (49 %) gab an, dass ihrem Unternehmen eine dedizierte PAM-Lösung fehlt. Die Fortschritte Deutschlands spiegeln eine starke strategische Ausrichtung auf die Identitätsprinzipien wider, aber eine uneinheitliche operative Umsetzung.

© 2025 Keeper Security, Inc

> **Identität ist zum Kontrollpunkt der Cybersicherheit geworden. Die Unternehmen, die bei Zero-Trust und PAM führend sind, schützen nicht nur den Zugriff, sondern schaffen auch die Grundlage für sicheres, skalierbares Wachstum im Zeitalter der KI.**
>
> **Darren Guccione,**
> **CEO and Co-founder, Keeper Security**

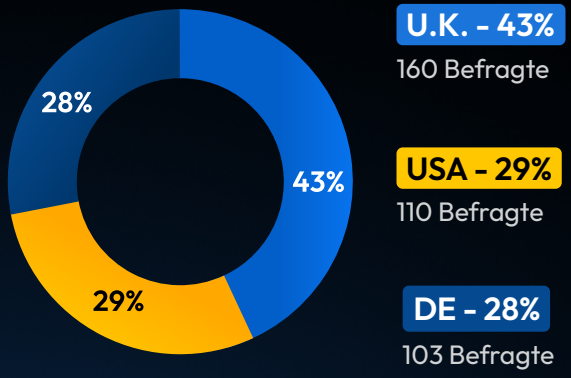
Keeper Security Insight

Moderne Cybersicherheit basiert auf der Konvergenz von Identitätskontrollen, Privilegienmanagement und intelligenter Automatisierung. Diese drei Kräfte definieren neu, wie Unternehmen ihre Benutzer, Daten und Infrastruktur in einer sich ständig weiterentwickelnden Bedrohungslandschaft schützen.

Zero-Trust und Privileged Access Management sind nicht mehr optional. Sie sind die Rahmenwerke, welche die operative Stabilität, Governance und Skalierbarkeit in modernen Unternehmen ermöglichen. Unternehmen, die über die Erklärung von Richtlinien hinausgehen und diese umsetzen, werden nicht nur ihre Abwehrkräfte stärken, sondern auch einen neuen globalen Standard für die Cybersicherheit setzen.

Die in Nürnberg, London und Las Vegas gewonnenen Erkenntnisse weisen auf eine entscheidende Wahrheit Tatsache hin: Identität ist der neue Perimeter. Die Widerstandsfähigkeit hängt jetzt von disziplinierter Ausführung, kontinuierlicher Messung und verantwortungsvollem Einsatz von KI auf allen Ebenen der Verteidigung ab. Die Unternehmen, die entschlossen handeln, indem sie Identitäten sichern, das Least-Privilege-Prinzip durchsetzen und intelligente Automatisierung nutzen, werden den heutigen Bedrohungen nicht nur standhalten, sondern auch die Zukunft der Cybersicherheit weltweit bestimmen.

Umfragemethodik



Keeper Security sammelte Erkenntnisse von 373 Cybersicherheits- und IT-Experten durch anonyme, persönliche Befragungen, die auf der it-sa in Nürnberg, der Infosecurity Europe in London und, der Black Hat USA in Las Vegas durchgeführt wurden.

© 2025 Keeper Security, Inc