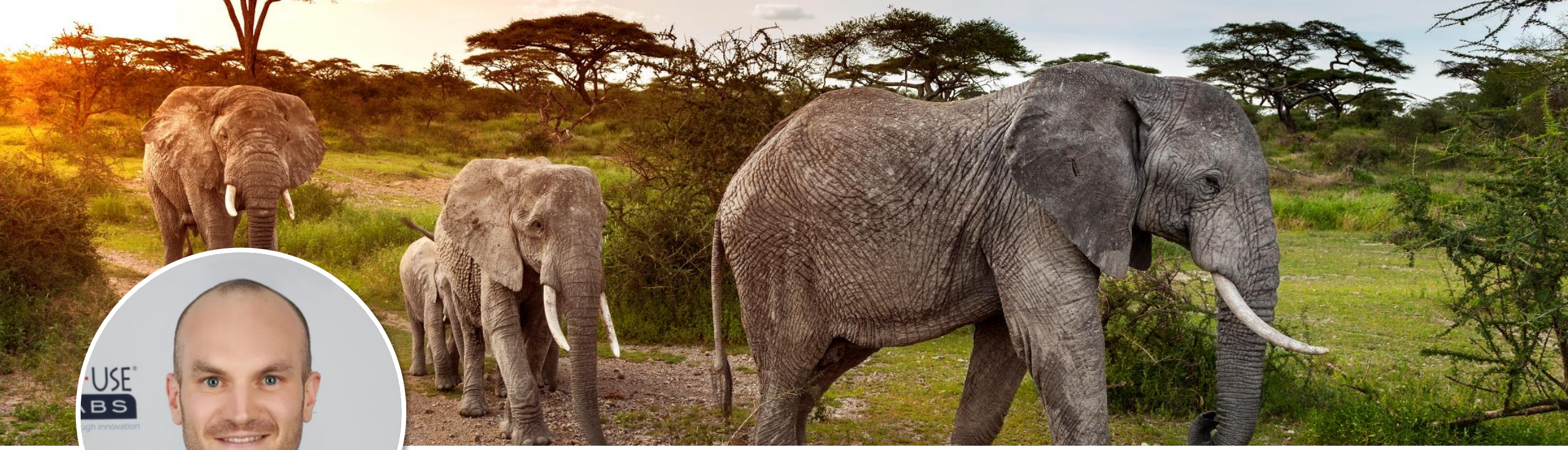
Die drei gängigsten SAP-Systemhacks & wie Sie Ihre Daten dagegen schützen

Frederik Ried & Nicolas Wrobel | November 2021

groupelephant.com
BEYOND CORPORATE PURPOSE

EPI-USE LABS
value through innovation

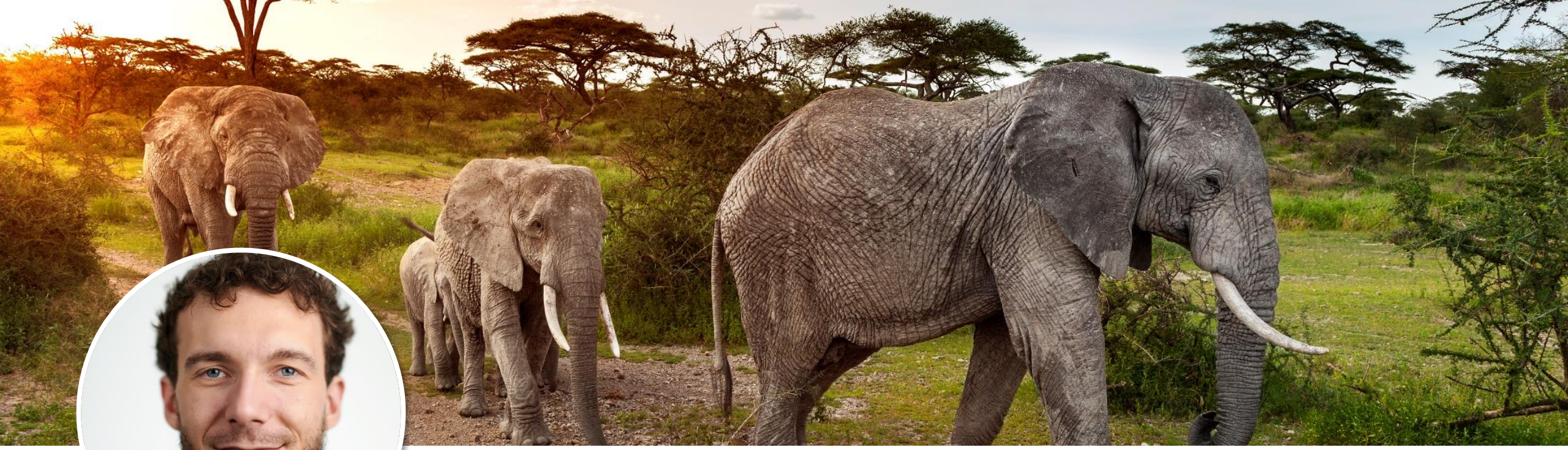


Connect with me on

Nico Wrobel

Sales Manager Central & Eastern Europe

Berlin, Deutschland

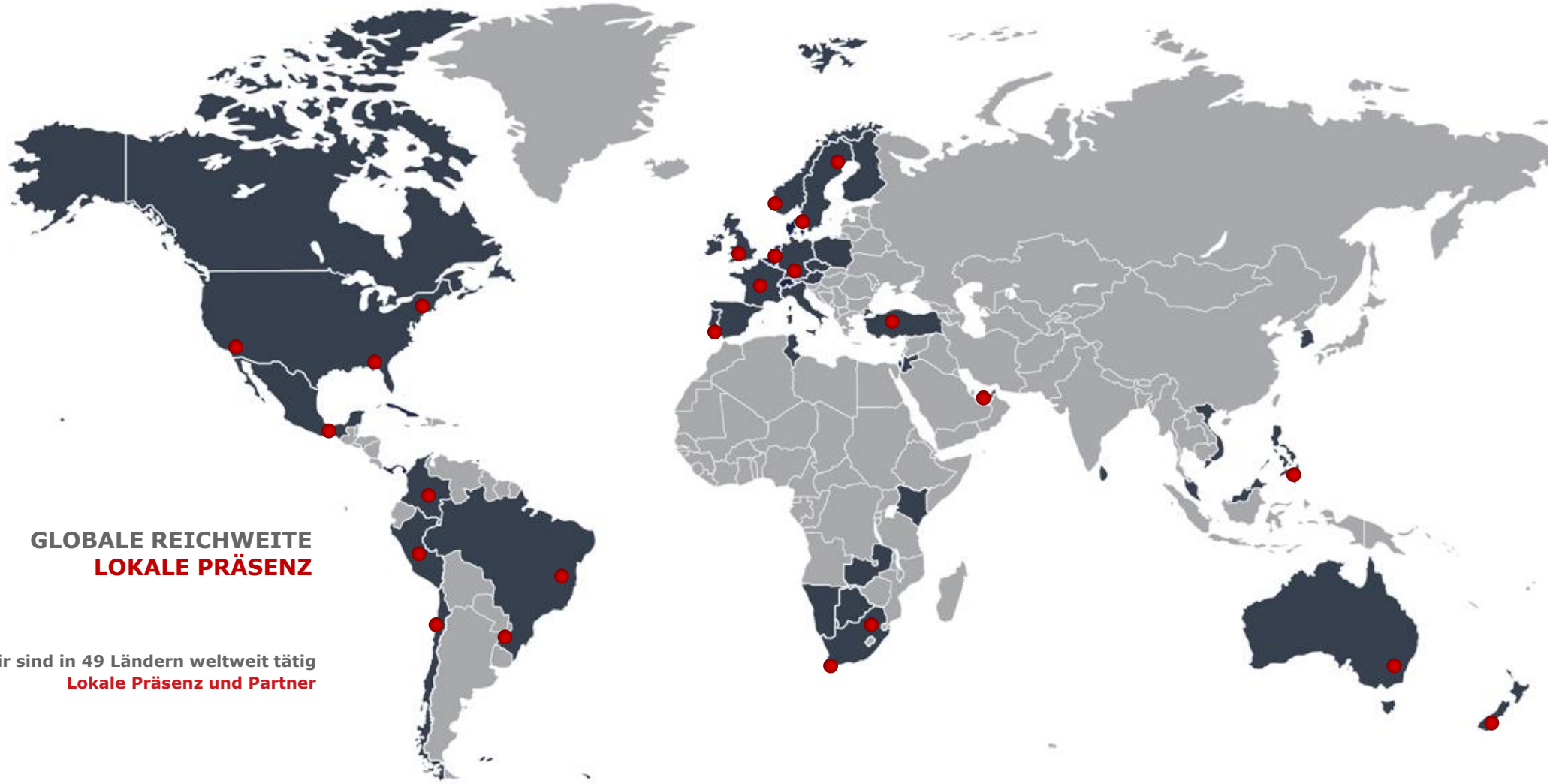


Connect with me on

Frederik Ried

Technical Consultant ALM/SLO

Walldorf, Deutschland



GLOBALE REICHWEITE
LOKALE PRÄSENZ

Wir sind in 49 Ländern weltweit tätig
Lokale Präsenz und Partner

VALUE THROUGH INNOVATION

GLOBAL FOOTPRINT

1,250+ KUNDEN WELTWEIT

VERTRETEN IN 49 LÄNDERN

6,200+ VERKAUFTE LIZENZEN

23% DES UMSATZES FLIEßEN IN R&D

97% Vertragsverlängerungen unserer Kunden

GLOBALES SUPPORT TEAM

IN-HOUSE SUPPORT TEAM

ZUFRIEDENE KUNDEN

24-hr SUPPORT VON MO - FR

MEHRSPRACHIGER SUPPORT

98% BEANTWORTETE TICKETS IN 30 MIN

CLIENT CENTRAL: UNSERE ONLINE-COMMUNITY

EXKLUSIVES ONLINE PORTAL

ZUGANG FÜR ALLE KUNDEN

17,000+ AKTIVE USER

WIR SIND TEIL DER groupelephant.com

35+ JAHRE ERFAHRUNG

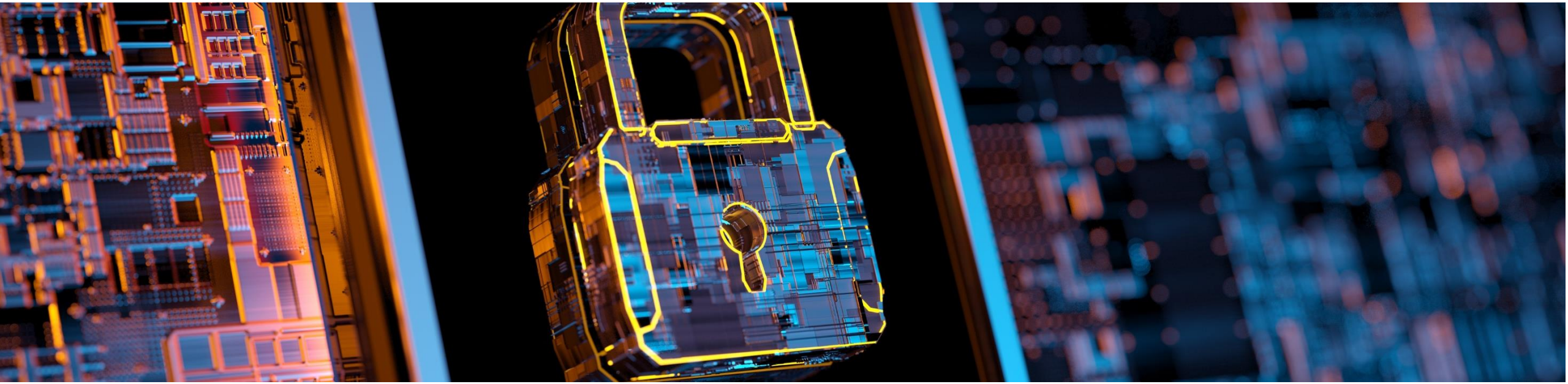
3,000+ MITARBEITER

1% DES UMSATZES SPENDEN WIR ERP
(NON-PROFIT-ORGANISATION "ELEPHANTS, RHINOS AND PEOPLE")

Agenda

- Hack 1: Transaktion SE16N
- → Soterion: Elevated Rights Manager
- Hack 2: Debugging
- → Cenoti: Monitoring mit Splunk
- Hack 3: Zugriff von einem anderen Mandanten
- → Data Sync Manager: Daten verfremden oder löschen
- Zusammenfassung

Hack 1: SE16N

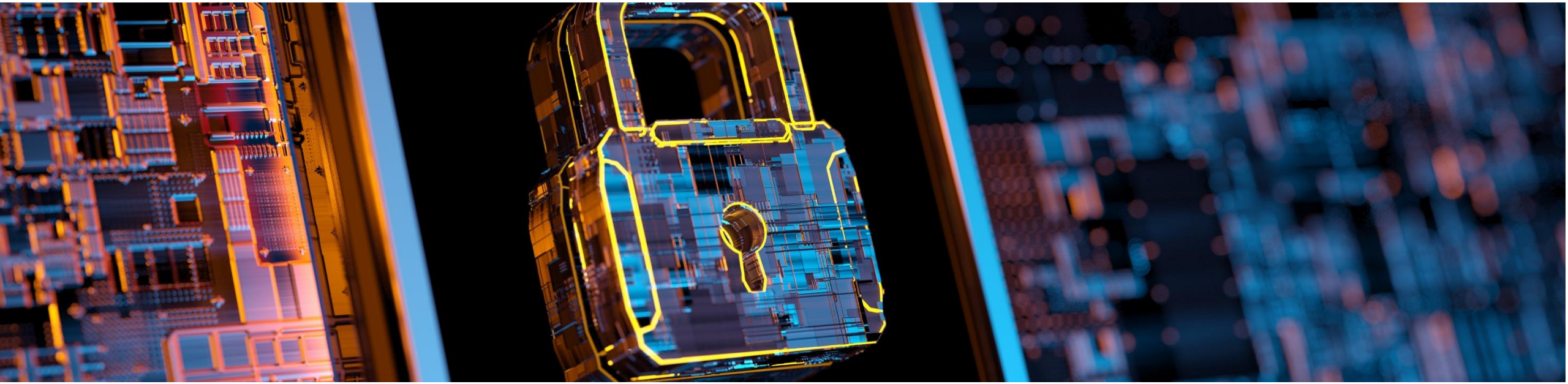


soterion | GRC-Lösungen für SAP-Unternehmen jeder Art und Größe

Access Risk Manager bietet die Möglichkeit, das SAP-Zugangsrisiko über eine benutzerfreundliche Webanwendung zu ermitteln. Mit dem Dashboard für Datenschutzrisiken und dem "Was-wäre-wenn"-Zuordnungssimulator erhalten Sie einen klaren Überblick über Ihr Zugriffsrisiko.

Access Risk Dashboard (Beispiel)

Hack 2: Debug



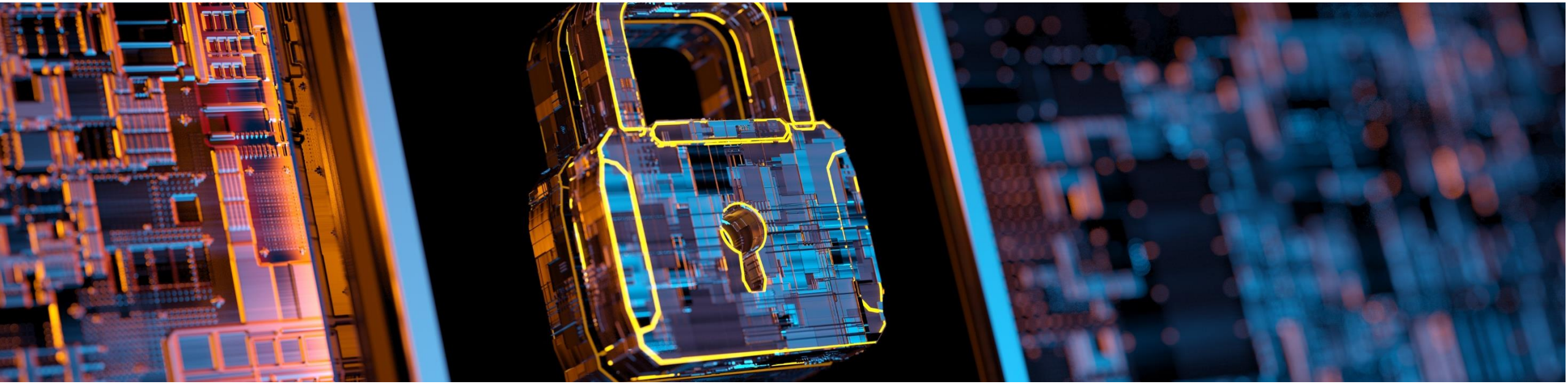
Cenoti

Mit Sicherheits- und Eventüberwachung die SAP-Daten innerhalb des Unternehmens verstehen und schützen

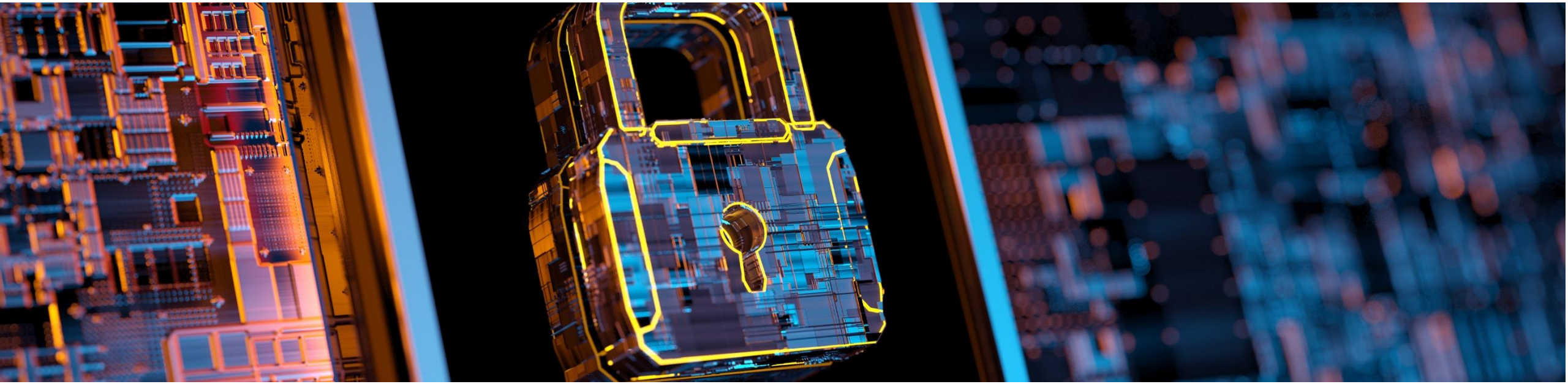
- Vorteile von Splunk nutzen
- Einfache Erweiterung von Kollektoren @SAP-Systeme
- Markierung und Anonymisierung sensibler Daten (Data Access Report + Alert Library)
- 24+ Dashboards | Out of the Box
- Schnelle und einfache Implementierung

groupelephant.com
BEYOND CORPORATE PURPOSE

Hack 3: Zugriff von einem anderen Mandanten



Bonus Hack: Weitere Zugriffsmöglichkeit von einem anderen Mandanten



Zusammenfassung

Hack 1:
Ein Programm oder Funktionsbaustein direkt ausführen

- Nicht ausschließlich auf S_TCODE verlassen
- SE38/SA38/SE37/SE80 nicht erlauben

Hack 2:
Berechtigungsprüfung im Debugger umgehen

- Keine Entwickler-/Debugberechtigung auf Systemen mit Produktiven Daten
- Falls zwingend erforderlich nur temporär oder bsp. Elevated Rights Management verwenden
- Monitoring aktivieren

Hack 3:
Daten eines anderen Mandanten auslesen

- Entwicklerschlüssel bedacht vergeben
- Keine Produktivdaten unverfremdet in Nicht-Produktive-Systeme halten

soterion

CENOTI
CONNECT SAP® WITH SPLUNK®

Data Secure
part of the Data Sync Manager Suite

groupelephant.com
BEYOND CORPORATE PURPOSE

EPI-USE LABS
value through innovation

FRAGEN

www.epiuselabs.de | vertrieb@labs.epiuse.com | clientcentral.io

LINKEDIN: EPI-USE Labs | XING: EPI-USE Labs GmbH | FACEBOOK: EPI-USE Labs DACH

TWITTER: @EPIUSELabs | INSTAGRAM: epiuselabs

groupelephant.com
BEYOND CORPORATE PURPOSE

EPI-USE LABS
value through innovation