

— KEYNOTE · ENERGIE- & WASSERWIRTSCHAFT

Wenn Logins zum **Risiko** werden

Identitätsschutz für Versorger

Angreifer brechen selten ein, sie melden sich an. Wie zentrale Identitätskontrollen die Logins von Mitarbeitern, Dienstleistern und Kunden wirksam absichern.



Nico Kugelman



Jürgen Zorenc



Willkommen zurück,
Michael

Einloggen

Ein typischer Querverbundversorger

Beispiel: kommunaler Querverbund mit Versorgung, ÖPNV und Entsorgung unter einem Konzerndach — und einer über Jahre gewachsenen Landschaft aus Fachverfahren und Zugängen.

~1 Mio.

versorgte Einwohner

4

Versorgungssparten

~30

Fachverfahren

1

Kundenportal

Strom

Gas

Fernwärme

Trinkwasser

ÖPNV

Entsorgung

DREI IDENTITÄTSWELTEN

→ Mitarbeiter

Verwaltung, Netzbetrieb, Leitstelle, ÖPNV und Entsorgung — jede Sparte mit eigenen Fachverfahren und eigener Benutzerverwaltung.

→ Dienstleister

Wartung an Netzleittechnik und Fachanwendungen — häufig über dauerhafte Zugänge und gemeinsam genutzte Konten.

→ Kunden

Ein Portal für Zählerstand, Abschlag und Vertrag — Self-Registration, Millionen Anmeldungen, hohe Komforterwartung.

Die Einstufung erfolgt je Rechtsträger. Für die Energienetze gelten die §§ 5c bis 5e EnWG mit dem IT-Sicherheitskatalog, für ÖPNV und Entsorgung die Schwellenwerte der BSI-KritisV. Das Kundenportal fällt unter das BfSG, sofern darüber Verträge geschlossen werden.

Das Einfallstor ist fast immer eine Identität.

Wenn es Versorger trifft, beginnt es selten an der Firewall - sondern an einem Konto.

WIRTSCHAFT · NORDRHEIN-WESTFALEN

AUS DER REGION

Fernwärme-Ausbau geht in die nächste Phase

Die Bauarbeiten für den zweiten Abschnitt des Wärmenetzes beginnen im Mai. Anwohner werden über Anschlussmöglichkeiten schriftlich informiert.

Derstand digital: Portal ausgebaut

Der mehr Kunden an Zählerstände statt per Karte. Der Versorger baut Selfservice-Funktion im Kundenbereich weiter aus.

April 2025

Hacker erbeuten Kundendaten - Datensätze im Darknet



Die Stadtwerke Schwerte nach dem Angriff. Foto: Archiv

Schwerte. Im März traf es die Stadtwerke Schwerte: Interne Systeme und das Kundenportal waren wochenlang beeinträchtigt. Wenig später tauchten erbeutete Datensätze im Darknet auf - darunter personenbezogene Kundendaten. Der Versorger schickte Warnbriefe an alle Kunden: Kontobewegungen prüfen, Vorsicht vor Phishing und Identitätsdiebstahl.

B2C · KUNDEN Hunderttausende Kundenkonten sicher betreiben

Energie, ÖPNV, Entsorgung, Glasfaser: jedes Portal ein eigenes Login, jede Registrierung ein Angriffsvektor - und Kunden erwarten den Komfort großer Online-Dienste.

B2B · PARTNER Dienstleister sicher anbinden

Ablesedienste, Abrechnungs- und IT-Dienstleister - der Angriff auf die Vereinigten Stadtwerke kam über einen Dienstleister.

B2E · BESCHÄFTIGTE Identitäten über Abrechnung, ERP und Fachsysteme

On- und Offboarding von Hand, verwaiste Konten, Sammel-Accounts: Das Active Directory allein bildet den Lebenszyklus nicht ab.

MFA und sichere Portale sind gesetzt. **Die eigentliche Aufgabe: Kundenidentitäten sicher und komfortabel managen - CIAM.**

User-Login als Einfallstor für Cyberangriffe



Jede 2.

Organisation wurde in den letzten 3 Jahren Opfer eines erfolgreichen Cyberangriffs.



82%

der Unternehmen erwarten keine Entspannung der Bedrohungslage im kommenden Jahr.



64%

der Mitarbeitenden verwenden ihre Passwörter mehrfach.



80 % der Security-Verantwortlichen sehen Social Engineering & Phishing als größte Bedrohung für ihr Unternehmen.

Jeder 3.

Nutzer klickt auf schädliche Inhalte in Phishing-E-Mails.



Jeder 2.

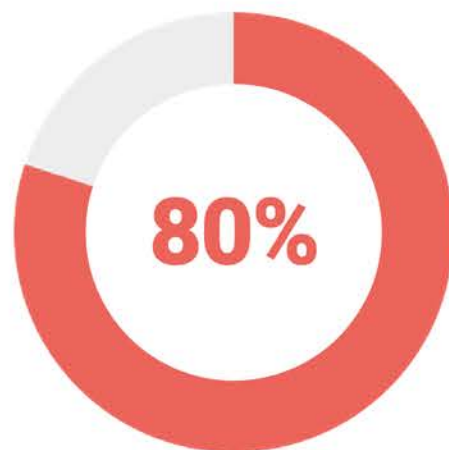
davon gibt anschließend sensible Informationen weiter.

Quellen: heise.de (Passwort-Mehrfachnutzung, 2023) · SoSafe Human Risk Review 2026

Starker Rückenwind für SSO/MFA-Lösungen



Hauptursachen erfolgreicher Angriffe



Schlechte Passwörter sind für **80 % aller Data Breaches** verantwortlich.



Kompromittierte Nutzerkonten



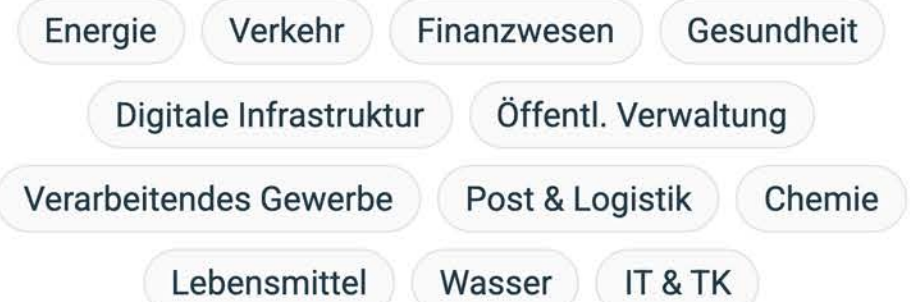
2025 wurden weltweit **425,7 Millionen** Nutzerkonten kompromittiert – 18,6 Millionen davon in Deutschland. Im ersten Halbjahr 2026 kamen **313,4 Millionen** hinzu.



2026: NIS2-EU-Richtlinie

MFA ist in § 30 Abs. 2 Nr. 10 BSIG ausdrücklich als Mindestmaßnahme genannt. **SSO** ist ein etablierter Weg, die in Nr. 9 geforderte Zugriffskontrolle umzusetzen.

AB 2026 VERPFLICHTEND FÜR U. A.:



Audits mit persönlicher Management-Haftung – Sicherheitsmaßnahmen für IT & Netzwerke sind **verpflichtend**.

Bare.ID bietet die einzige vollständig souveräne, hochsichere Login- und Multi-Factor-Authentication-SSO-Lösung mit Open-Source-Kern.

Sie kommen aus der Microsoft-Welt? Auch kein Problem.

Active Directory, Outlook, Microsoft 365 - gelebte Realität in der Stadtwerke-IT. Bare.ID ersetzt das nicht, sondern setzt davor an: als souveräne Zwischenschicht, so kann Microsoft über eine CLOUD-Act-Anfrage nicht auf alle Ihre Systeme zugreifen.



Active Directory & Entra ID bleiben führend

Vorkonfigurierte Konnektoren nach Broker-Prinzip: Passwörter bleiben im Quellverzeichnis - es wird nichts migriert, bevor Sie es entscheiden.



MFA & Passkeys als Managed Service

Policies aktivieren statt Spezialteam aufbauen: Von Passkeys über OTP-Apps bis Hardware-Token - Bare.ID unterstützt alle Verfahren.



Sicheres MFA auch beim Windows-Login am Arbeitsplatz möglich

Direkter Windows-Login mit zusätzlicher Sicherheitsschicht von Bare.ID - gemeinsam mit einem spezialisierten Partner umgesetzt, schützt Ihren Windows-Login.



Eine souveräne Schicht für alles andere

Kundenportal, Abrechnung, Marktpartner-Zugänge: Was die Microsoft-Welt nicht abdeckt, läuft über die souveräne Bare.ID Login-Schicht - betrieben in Deutschland.



01

— KAPITEL 01

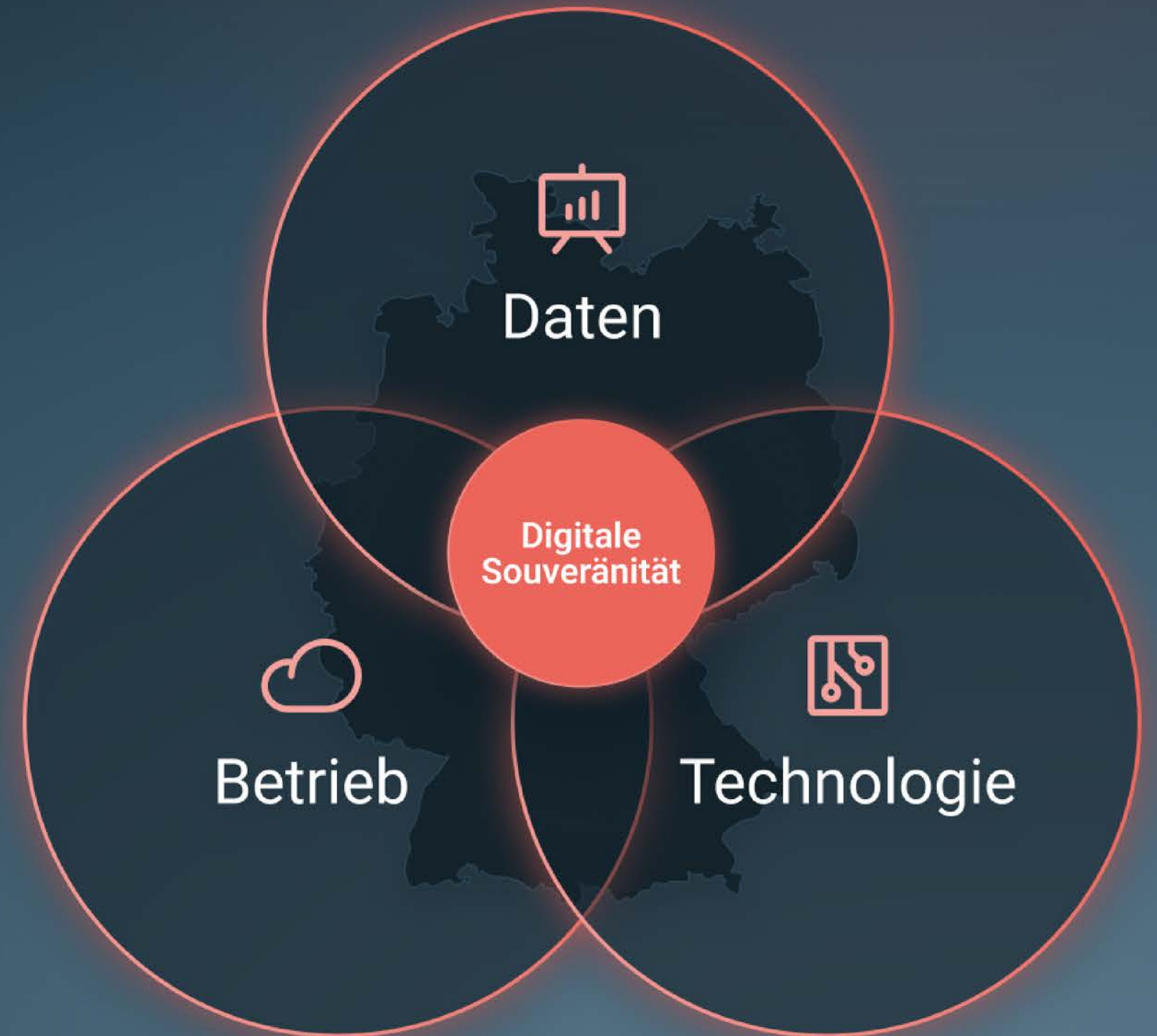
Die souveräne Plattform.

Alle IAM-Bausteine in einer Lösung — Open Source im Kern, betrieben ausschließlich in Deutschland. Komplett deutsche Lieferkette.

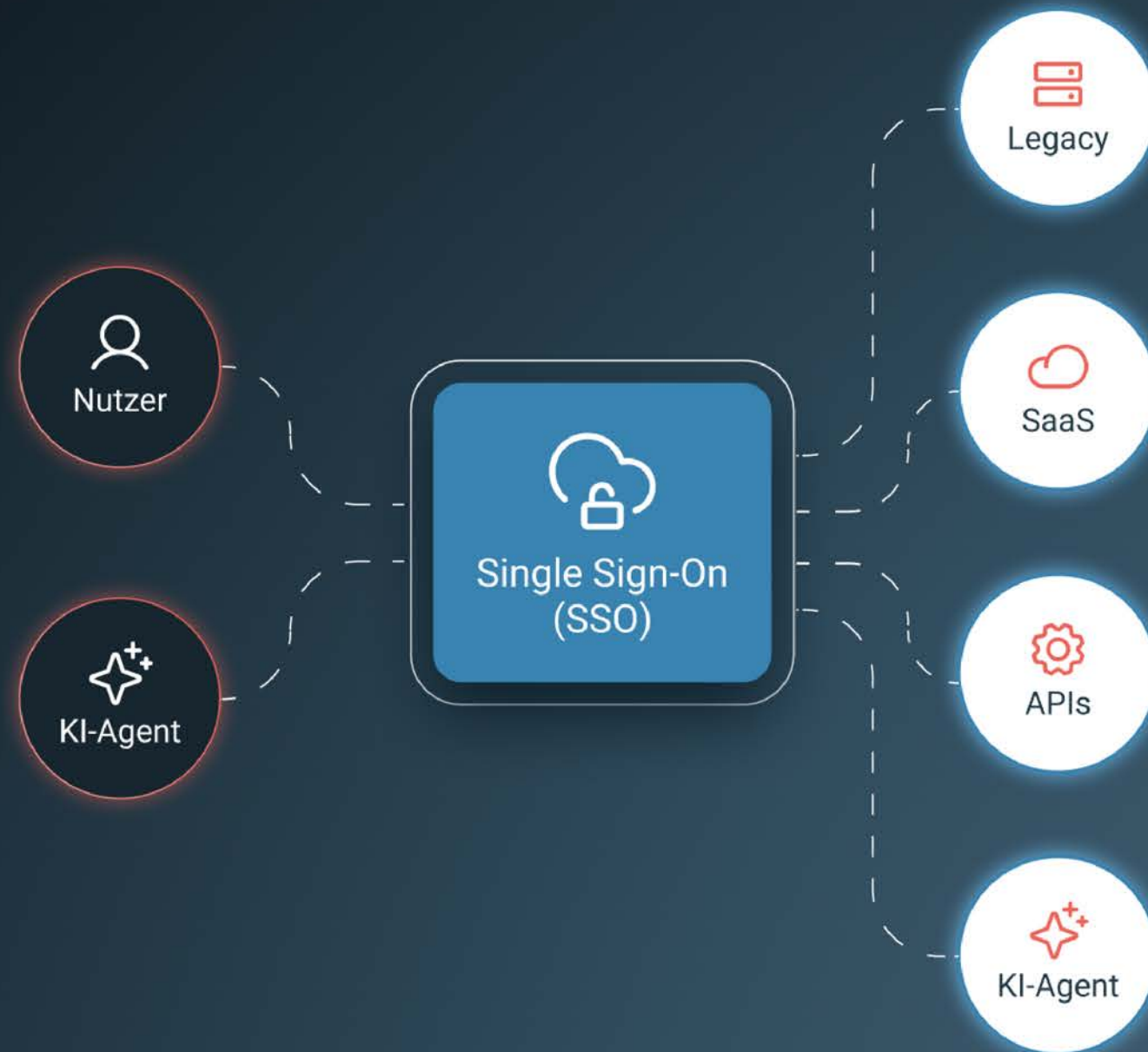
Open-Source-Kern

SaaS-Betrieb

Self-Hosted



Eine Plattform für alle Identitäten Ihres Stadtwerks.



B2C · KUNDEN

Ein Konto für alle Portale

Energie, Wasser, Glasfaser, Ladestrom: Self-Registration, Passkeys, Social Login und Consent Management - skaliert auf Millionen Kundenkonten, im Branding Ihres Stadtwerks.



B2B · PARTNER

Föderiert statt fremdverwaltet

Ablesedienste, Netzpartner und IT-Dienstleister melden sich mit den Konten ihrer eigenen Organisation an - Sie vergeben nur Rechte, keine Passwörter.



B2E · BESCHÄFTIGTE

Eintritt → Wechsel → Austritt, alles geregelt

On-/Offboarding über SCIM und AD-Anbindung, SSO + MFA für Abrechnung, ERP und alle Fachanwendungen - keine verwaisten Konten mehr.



Betriebsfertig auf Open-Source-Basis

IAM und CIAM auf einer Instanz: Bare.ID betreibt, patcht und supportet den Keycloak-Standard - MFA inklusive, ohne Vendor Lock-in, jederzeit rückmigrierbar.

Login in Unternehmen: Früher vs. heute

ALTE WELT

Jeder Dienst benötigt seine **eigene Benutzerverwaltung und MFA**. Berechtigungen müssen pro Anwendung verwaltet werden.



Eigenes Verzeichnis · eigene MFA ·
eigene Authentisierung

○ KEIN SSO



Eigenes Verzeichnis · eigene MFA ·
eigene Authentisierung

○ KEIN SSO



Eigenes Verzeichnis · eigene MFA ·
eigene Authentisierung

○ KEIN SSO

...

Jede weitere Anwendung mit eigener
Insel-Lösung

○ KEIN SSO

NEUE WELT

Zentrale Zugangskontrolle per Single Sign-On für alle Anwendungen — made and (opt.) hosted in Germany.

 **Bare.ID Login + MFA + Benutzerverzeichnis(se)**



SSO-LOGIN



SSO-LOGIN



SSO-LOGIN

...

SSO-LOGIN

Passt in Ihre bestehende IT - ohne Systembruch.



Ausschließlich offene Standards

- OpenID Connect, OAuth 2.0, SAML 2.0, SCIM und WebAuthn - was Standards spricht, funktioniert sofort
- Bereit für KI-Agenten: delegierte, kontrollierte Zugriffe nach UMA 2.0
- Auch gewachsene Fachanwendungen: LDAP, RADIUS & Kerberos werden unterstützt
- Kein Vendor Lock-in

Ihre Systemlandschaft unterstützt

- 35+ vorkonfigurierte Integrationen aus der App-Galerie und volle Kompatibilität mit allen Industriestandards
- Microsoft 365, Zoom, Salesforce, AWS, Dropbox, TYPO3, Personio u. v. m. - Standardsoftware sofort angebunden
- Microsoft 365 & Entra ID vorkonfiguriert - siehe Ausgangslage



Schon Keycloak im Einsatz?

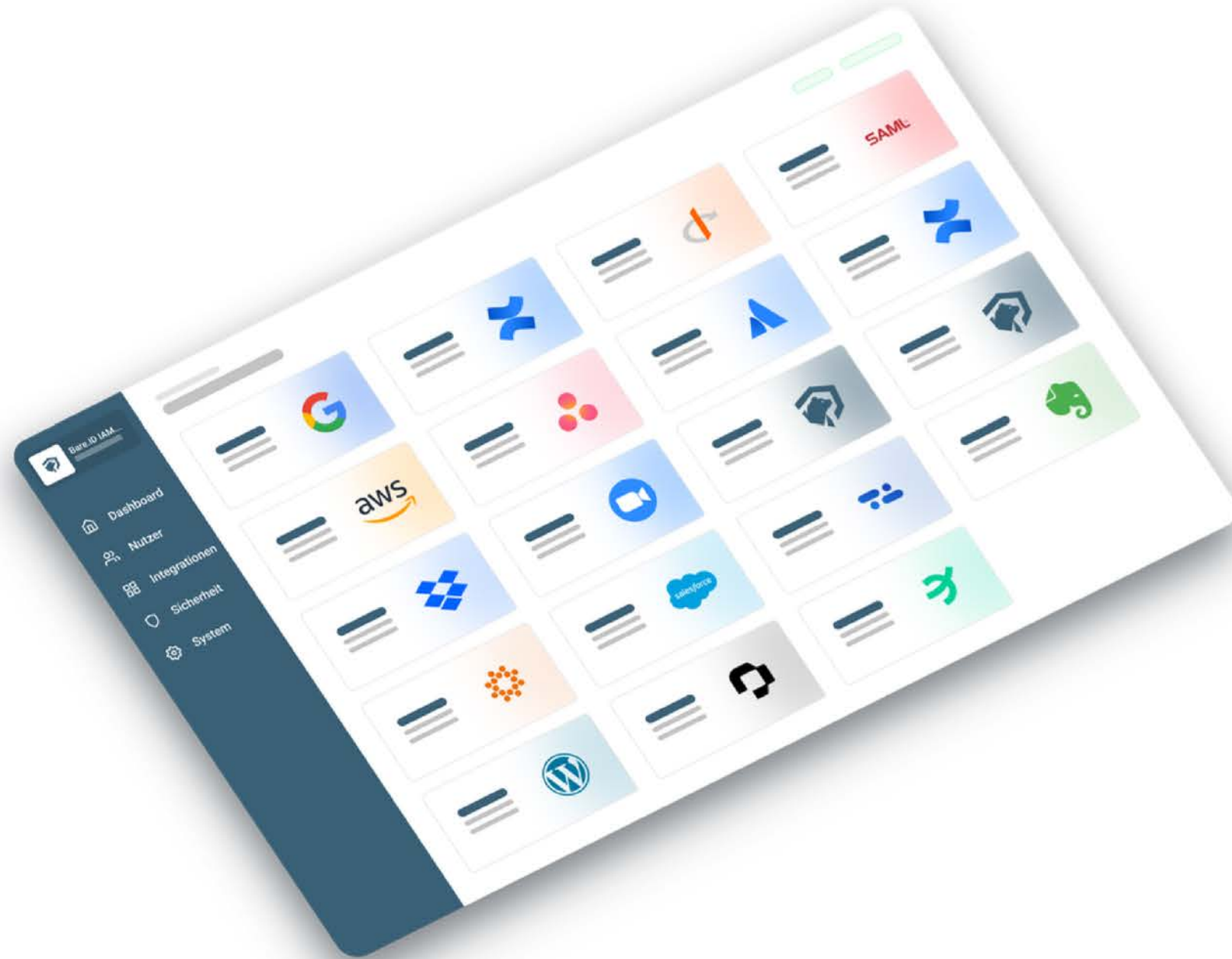
- Bestehende Setups 1:1 übernehmen - Realm, Client-IDs, Konfiguration inkl. Signaturschlüssel
- Angebundene Fachverfahren laufen unverändert weiter
- Rückweg jederzeit offen - kein Vendor Lock-in



— INTEGRATIONEN

Vollständig integriert mit allen wichtigen Software-Lösungen:

Vorkonfiguriert in der Application Gallery — in Minuten angebunden, ohne technisches Know-how.



DRACON

Personio

zoom

Dropbox

Confluence

salesforce

TYP03

Google Workspace

HubSpot

ExplicitTrust

asana

Grafana

EVERNOTE

Office 365

citrix

Nextcloud

Mattermost

BigBlueButton

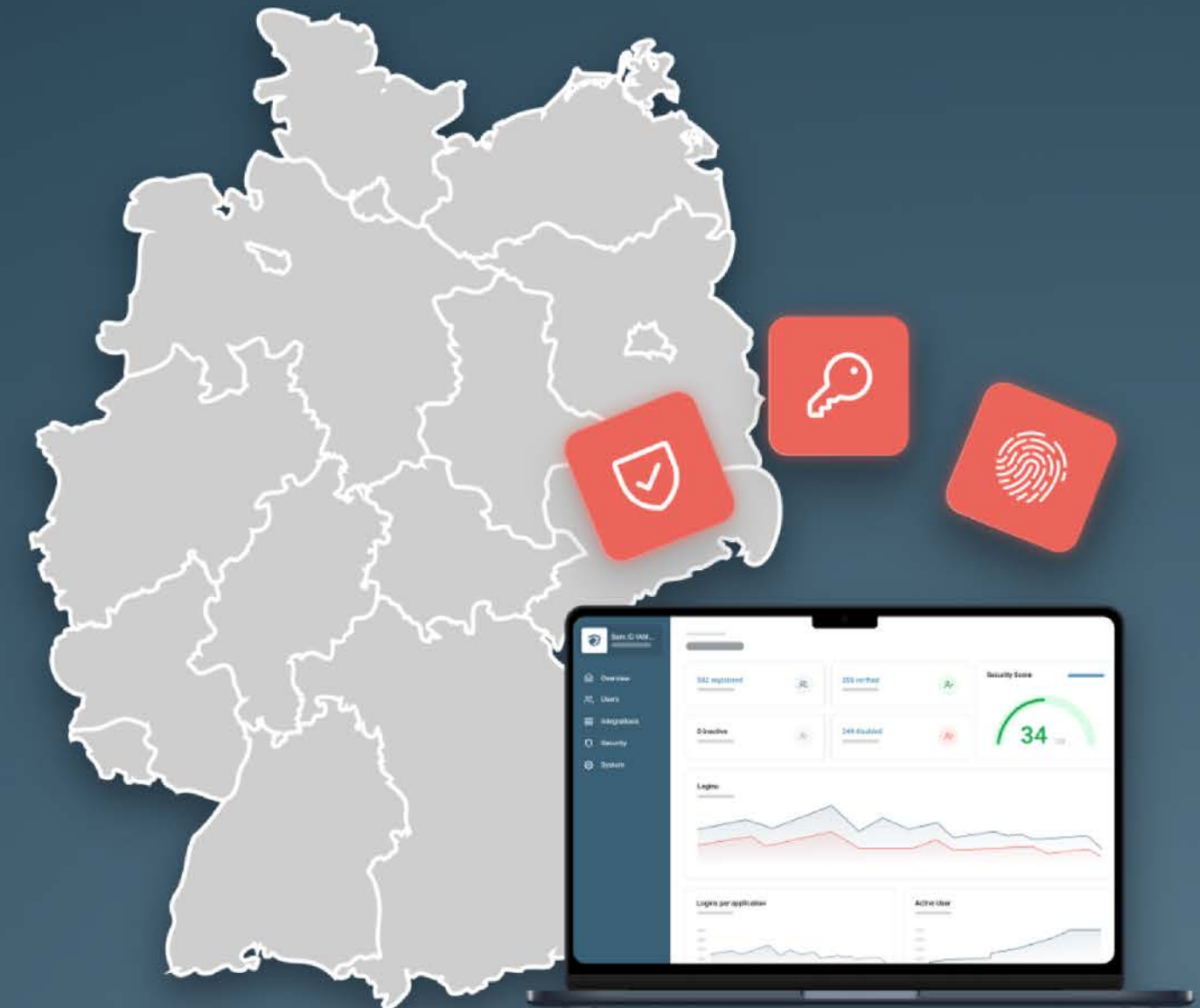
WORDPRESS

+50 weitere



100 % Deutschland. Nachweisbar.

- ✓ **Entwicklung, Betrieb und Support** ausschließlich in und aus Deutschland - durchgängig deutsche Lieferkette, deutscher muttersprachlicher Support.
- ✓ **Deutsche Rechenzentren:** SysEleven (Berlin) und optional STACKIT (Schwarz Gruppe) - BSI-C5-testiert, EN 50600, georedundant über getrennte Standorte.
- ✓ **Kein CLOUD Act:** Zugriffs- und Identitätsdaten verlassen den deutschen Rechtsraum nicht - im Gegensatz zu US-Anbietern und Hyperscaler-Lösungen.
- ✓ **ISO 27001** (TÜV Rheinland), NIS2- und DSGVO-compliant by design, 99,9 % Verfügbarkeit im Betrieb — geeignet für KRITIS-Betreiber.
- ✓ **Betriebsmodell nach Wahl:** SaaS, On-Prem im eigenen Rechenzentrum oder eigener Host, auch hybrid - gleiche Plattform, gleiche Funktionen.



02

KAPITEL 02

Bare.ID Praxisdemo.

Die wichtigsten Funktionen direkt aus dem Produkt – vom Dashboard über MFA und SCIM bis zu DSGVO-Werkzeugen.

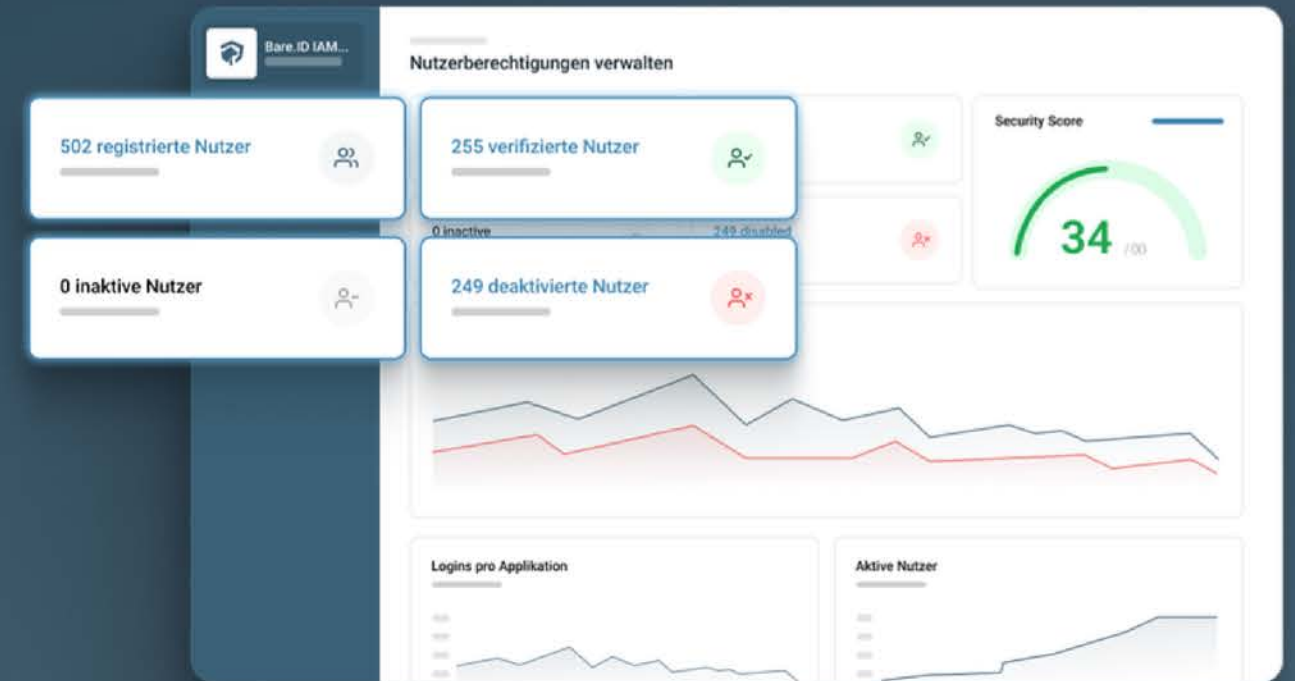
Dashboard

MFA

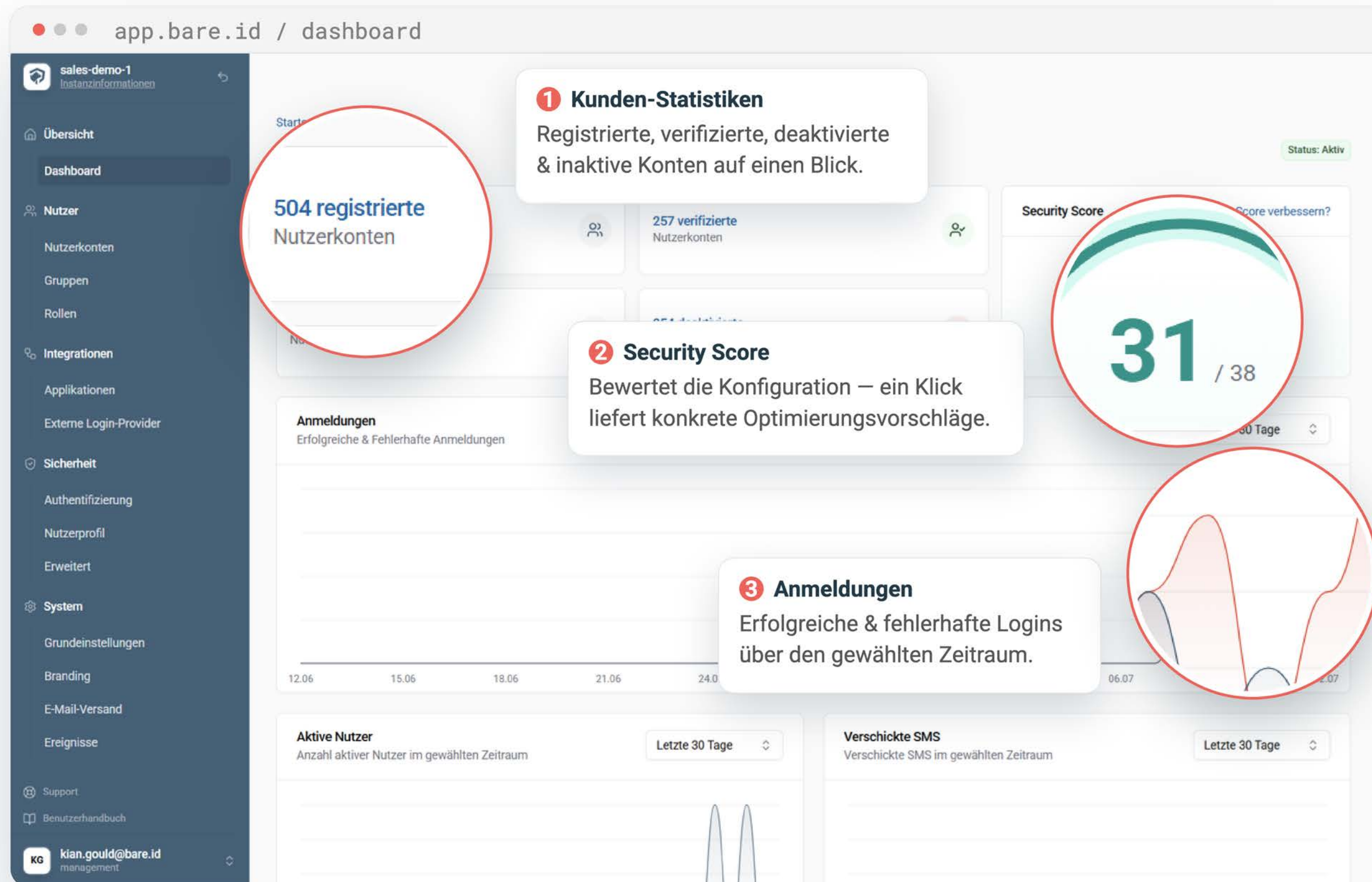
SCIM

DSGVO

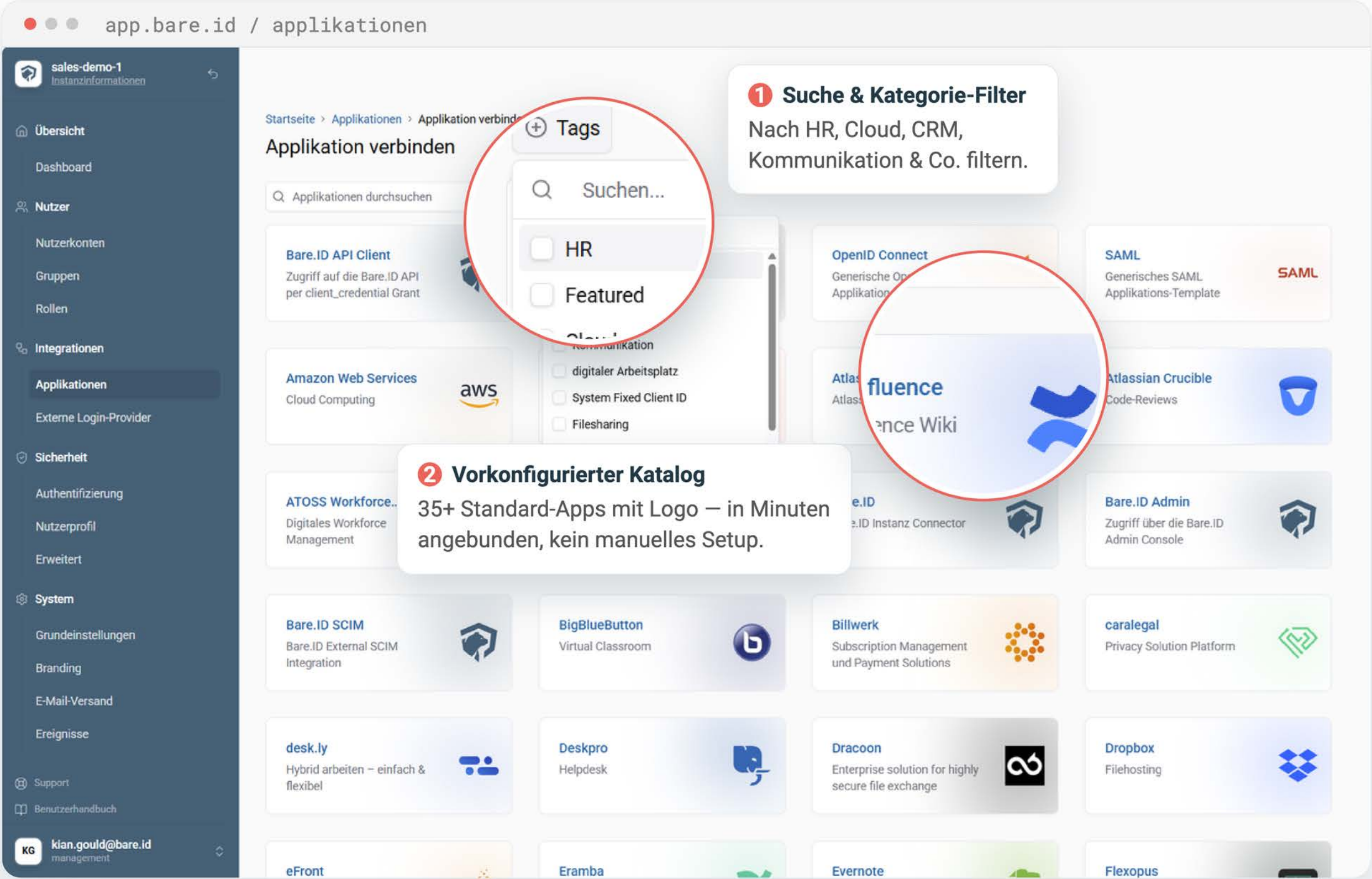
RBAC



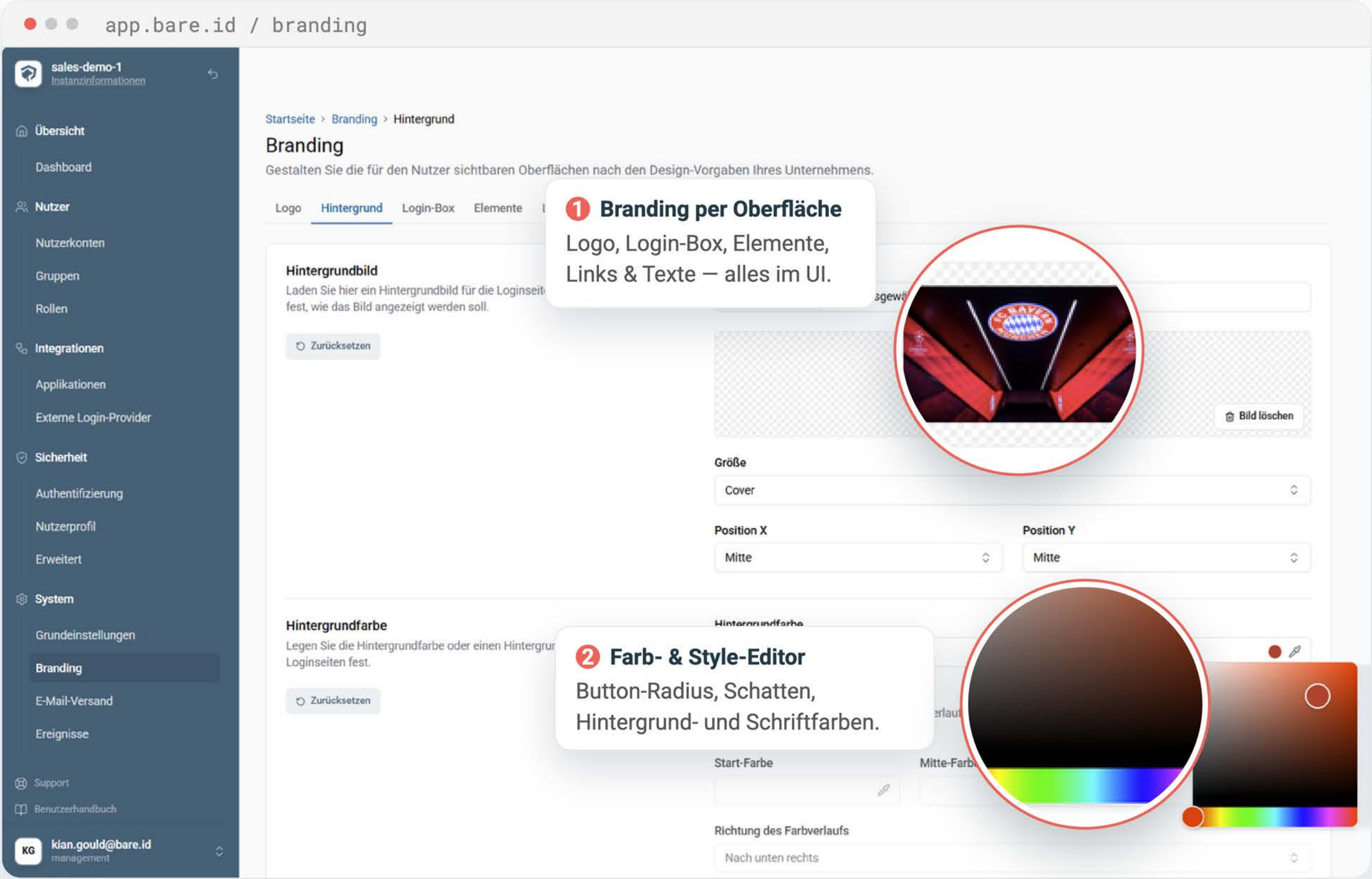
Bare.ID: Dashboard



Bare.ID: Application-Gallery



Bare.ID: White Label



— REFERENZEN

Diese Unternehmen vertrauen uns

Öffentlicher Sektor, KRITIS und Privatwirtschaft — vom Bundesministerium bis zur Bundesliga.

— PRIVATER SEKTOR



— ÖFFENTLICHER SEKTOR



— NÄCHSTE SCHRITTE

Sprechen wir über Ihre Identitäten.

Souveränes IAM ist kein Mammutprojekt: Vom kostenlosen Test bis zum produktiven Betrieb - mit dediziertem Projektmanager an Ihrer Seite.

- 1 Kostenlose Testphase mit vollem Funktionsumfang - PoC am echten Anwendungsfall
- 2 In wenigen Wochen produktiv - Migration ohne Umstellung für Ihre Nutzer
- 3 Transparente, faire Preise nach monatlich-aktiven Nutzern (MAU)
- 4 Ein deutscher Partner, der wirklich zuhört und an Ihrer Seite steht



Nico Kugelman
nico.kugelman@bare.id



Direkt vernetzen - QR-Code scannen · www.bare.id



Jürgen Zorenc