Was kann Bare.ID?

Tolleiv Nietsch - 2024-09-16 - Fragen zum Produkt

Der Einsatz von Bare.ID bringt mehr Sicherheit für alle Nutzer:innen und deren Daten, die bei den verbundenen Drittanbieter-Applikationen hinterlegt sind.

Als **Single Sign-On-Lösung** ersetzt es viele Anmeldungen bei unterschiedlichen Web-Anwendungen und Diensten durch eine zentrale Anmeldung bei Bare.ID. Dadurch stellt es eine zusätzliche Sicherheitsebene dar, die mittels selbst festgelegter Passwortrichtlinien, Brute-Force-Schutz, moderner Mehr-Faktor-Authentifizierung (MFA) uvm. an die eigenen Standards angepasst werden kann. Gleichzeitig erhöht es den Komfort der Nutzer:innen und sorgt dadurch für hohe Akzeptanz in der täglichen Nutzung.

Als **Identity- und Access-Management-Lösung** stellt Bare.ID außerdem breite Möglichkeiten der Rollen- und Rechteverwaltung zur Verfügung. So können beispielsweise Nutzerkonten in Gruppen zusammengefasst, applikationenspezifisch Zugangs- und Zugriffsrechte an Nutzerkonten, Gruppen oder Nutzer:innen mit bestimmten Rollen erteilt und Anmeldeaktivitäten und aktive Sessions eingesehen werden. Dabei spielt es keine Rolle, ob die Nutzerkonten über die Bare.ID-Benutzeroberfläche verwaltet oder durch einen externen Identity-Provider eingespielt werden.

Tarife

Bare.ID wird zu verschiedenen Tarifen mit unterschiedlichen Funktions- und Serviceumfängen angeboten. Diese Tarife können in Form von Subscriptions gebucht werden, wobei auch die Buchung mehrerer Subscriptions in unterschiedlichen Tarifstufen möglich ist. Alle Tarifoptionen und deren Leistungsumfänge sind unter https://www.bare.id/#tarife beschrieben. Zur Integration von Bare.ID in eine bestehende IT-Landschaft werden zudem Beratung und individuelle Software-Entwicklungsleistungen angeboten.

Instanzen

Für die gebuchten Subscriptions lassen sich sogenannte Instanzen anlegen und per Administrator-Konto verwalten. Dabei stellt jede Instanz ein eigenes Keycloak-Realm dar, also einen isolierten Datensatz innerhalb einer Keycloak-Installation. Ab dem Tarif "Professional Edition" befindet sich dieses Realm auf einem eigenen, dedizierten Cluster.

Benutzeroberfläche

Jede erstellte Bare.ID-Instanz kann individuell über die Benutzeroberfläche von Bare.ID unter https://app.bare.id/ konfiguriert und überwacht werden. Hier werden die verbundenen

Applikationen verwaltet, Sicherheits- und Brandingeinstellungen vorgenommen, aber auch alle Nutzerkonten administriert und Zugriffsrechte, Rollen und Gruppen zugewiesen. Auf einem Dashboard lassen sich außerdem verschiedene Metriken, wie Anmeldeversuche von Nutzern und Clients verfolgen und alle relevanten URLs der Instanz aufrufen.

Applikationen
Damit sich Nutzer:innen abgesichert durch Bare.ID bei der Applikation eines Drittsystems anmelden können, werden zunächst über die Benutzeroberfläche entsprechende Applikationen mit Bare.ID verbunden. Viele Applikationen sind bereits vorkonfiguriert und können aus einer Liste vorhandener Dienste ausgewählt werden. Weitere Dienste können per OpenID Connect (OIDC)- oder Security Assertion Markup Language (SAML)-Standard verknüpft oder vom Bare-ID-Entwicklungsteam integriert werden.

Identitätsquellen
Nutzerkonten und Zugriffsrechte können sowohl über die Benutzeroberfläche von Bare.ID gepflegt, als auch über den OpenID Connect- oder den Lightweight Directory Access Protocol-Standard (LDAP) aus externen Identitätsquellen eingespeist werden. Dabei kann es sich um ein Active Directory (AD), aber auch um ein weiteres Single Sign-On-System (SSO) handeln.

Mehr-Faktor-Authentifizierung
Zusätzliche Sicherheit bringt die Verwendung von Mehr-Faktor-Authentifizierung (MFA). Dabei helfen einheitliche Identifikationsfaktoren den Aufwand beim Anmelden gering zu halten und führen zu hoher Akzeptanz bei den Nutzer:innen. Bare.ID unterstützt u.a. One-Time Passwords (OTP), Gesichtserkennungs- und Fingerabdrucksensoren, Hardwaretoken und andere Komponenten nach FIDO2/WebAuthN- und protect4use-Standards.

Design
Alle für die Nutzer:innen sichtbaren Oberflächen und E-Mails der Bare.ID-Integration können per Benutzeroberfläche an jedes Corporate Design angeglichen werden. Die Verwendung von Bare.ID stellt sich daher für die Nutzer:innen als vollintegrierter, vertrauenswürdiger Teil seiner Organisation dar oder ist für diese gar unsichtbar.

Entwickler-APIs
Für Entwickler:innen steht ab der "Premium Edition" sowohl eine Authentifizierungs-API zur Verfügung, um Bare.ID per OIDC- oder SAML-Protokoll in bestehende Systeme zu integrieren, als auch eine Management-API für die programmatische Verwaltung.

Zertifizierungen
Bare.ID wird ausschließlich in und aus Deutschland gehostet, betrieben und entwickelt und ist somit 100% DSGVO-konform. Die SaaS-Lösung bildet zudem standardisierte gesetzliche und branchenspezifische Sicherheitsanforderung ab und kann dadurch selbst in stark regulierten Bereichen konform eingesetzt werden.

Ausfallsicherheit
Von DevOps-Expert:innen betrieben, garantiert Bare.ID eine Verfügbarkeit von 99,9%. Diese

besonders hohe Ausfallsicherheit wird durch ein mehrfach redundantes Setup ermöglicht. Datenbanken und Applikationsserver sind mit mehreren Nodes im Cluster-Betrieb und über unterschiedliche Rechenzentren verteilt gehostet. Alle Applikationen werden als Container mit Kubernetes betrieben und physikalisch getrennte Backups verhindern dabei einen Datenverlust. Selbst die hohen Anforderungen für Kritische Infrastruktur (KRITIS) werden durch die Einhaltung der in der KRITIS-Verordnung geforderten Georedundanz ab dem Tarif "Premium Edition" erfüllt.

Service

Bei Fragen, Auffälligkeiten oder Problemen, steht ein Serviceteam bereit, welches auf Monitoring und Alerting reagiert, Hilfestellung leistet und Fragen über unser Support-Center unter https://support.bare.id/de beantwortet.