



Der Identity Hub für den Mittelstand

Whitepaper zu Identity Governance, automatisiertem Lebenszyklus und Compliance mit neoid

Version
3.0

Stand
Oktober 2026

Herausgeber
neoworx GmbH

Web
www.neoid.eu

Inhalt

01	Executive Summary	3
02	Die Herausforderung: Identitäten im Mittelstand	4
03	neoid im Überblick	6
04	Funktionen	7
05	Integration	15
06	Sicherheit & Compliance	17
07	Einführung	21
08	Pakete & Preise	23
09	Über neoworx	27

Executive Summary

Im Mittelstand verteilen sich digitale Identitäten auf dutzende Systeme. Konten werden per E-Mail und Ticket angelegt, bei Rollenwechseln selten bereinigt und beim Austritt oft vergessen. Das kostet IT-Zeit, verzögert die Einarbeitung und ist – spätestens mit NIS2 – ein Haftungsrisiko für die Geschäftsleitung.

neoid ist der Identity Hub für den Mittelstand. Das HR-System wird zur führenden Quelle; neoid berechnet daraus, wer welche Zugänge braucht, und versorgt alle angebundenen Systeme automatisch – vom ersten Arbeitstag über jeden Abteilungswechsel bis zum Austritt. Anmeldungen erfolgen passwortlos per Passkey, ein Notausschalter sperrt im Ernstfall alle Zugänge in Sekunden, und Rezertifizierung, Funktionstrennung und Audit-Trail liefern die Nachweise für Prüfer.

98 %

Zeitersparnis im
Onboarding

< 3 Sek.

Notausschalter

~500 h

IT-Zeit pro Jahr
gespart

Berechnung: 2,5 Identity-
Tickets × 0,5 h je
Mitarbeitendem, 90 %
Reduktion

6 Wochen

bis produktiv

Kernaussagen

- ✓ Ein zentraler Steuerungspunkt für alle Identitäten, Zugänge und Berechtigungen
- ✓ Automatischer Lebenszyklus (Joiner, Mover, Leaver) direkt aus dem HR-System
- ✓ Passwortlose, phishing-resistente Anmeldung und Single Sign-On
- ✓ Nachweisbare Compliance für NIS2, CRA, ISO 27001, DSGVO und DORA
- ✓ Betrieb in der Cloud (Hosting in Deutschland & EU) oder On-Premises – in jedem Paket
- ✓ Transparente Preise ab 2 € (On-Premises) bzw. 3 € (Cloud) pro aktiver Identität und Monat

Die Herausforderung: Identitäten im Mittelstand

Jede Rolle im Unternehmen spürt fragmentierte Identitäten anders. Diese Schmerzpunkte begegnen uns in nahezu jedem Projekt:

Für die Geschäftsführung

- ✓ Haftung nach NIS2: Die Geschäftsleitung haftet persönlich für Cybersicherheitsmaßnahmen – ohne nachweisbare Zugriffskontrolle ist das kaum zu erfüllen.
- ✓ Konten ehemaliger Mitarbeitender: Jedes vergessene Konto ist ein offenes Tor für Datenabfluss und Angriffe.
- ✓ Teure Routine statt Projekte: Bis zu 500 Stunden IT-Zeit pro Jahr fließen in Onboarding, Passwort-Resets und Offboarding.

Für CISO & Informationssicherheit

- ✓ Identität ist Angriffsvektor Nr. 1: Kompromittierte Zugangsdaten verursachen 80 % aller Sicherheitsvorfälle (Verizon DBIR).
- ✓ Sperren dauert Tage statt Sekunden: Im Ernstfall müssen Zugänge in jedem System einzeln gesperrt werden – wertvolle Zeit für Angreifer.
- ✓ Keine prüffesten Nachweise: Ohne Rezertifizierung und Audit-Trail lassen sich NIS2- und ISO-27001-Anforderungen nicht belegen.

Für HR & Personalwesen

- ✓ Neue Mitarbeitende warten tagelang: Der Vertrag ist unterschrieben, aber E-Mail und Tools sind am ersten Tag nicht eingerichtet.
- ✓ Tickets statt Überblick: Für jede Zugangsfrage braucht es ein Ticket bei der IT – und niemand weiß, ob alles erledigt ist.
- ✓ Offboarding per Excel-Liste: Welche Zugänge beim Austritt deaktiviert werden müssen, wird manuell geprüft – fehleranfällig und riskant.

Für IT-Administration & IT-Leitung

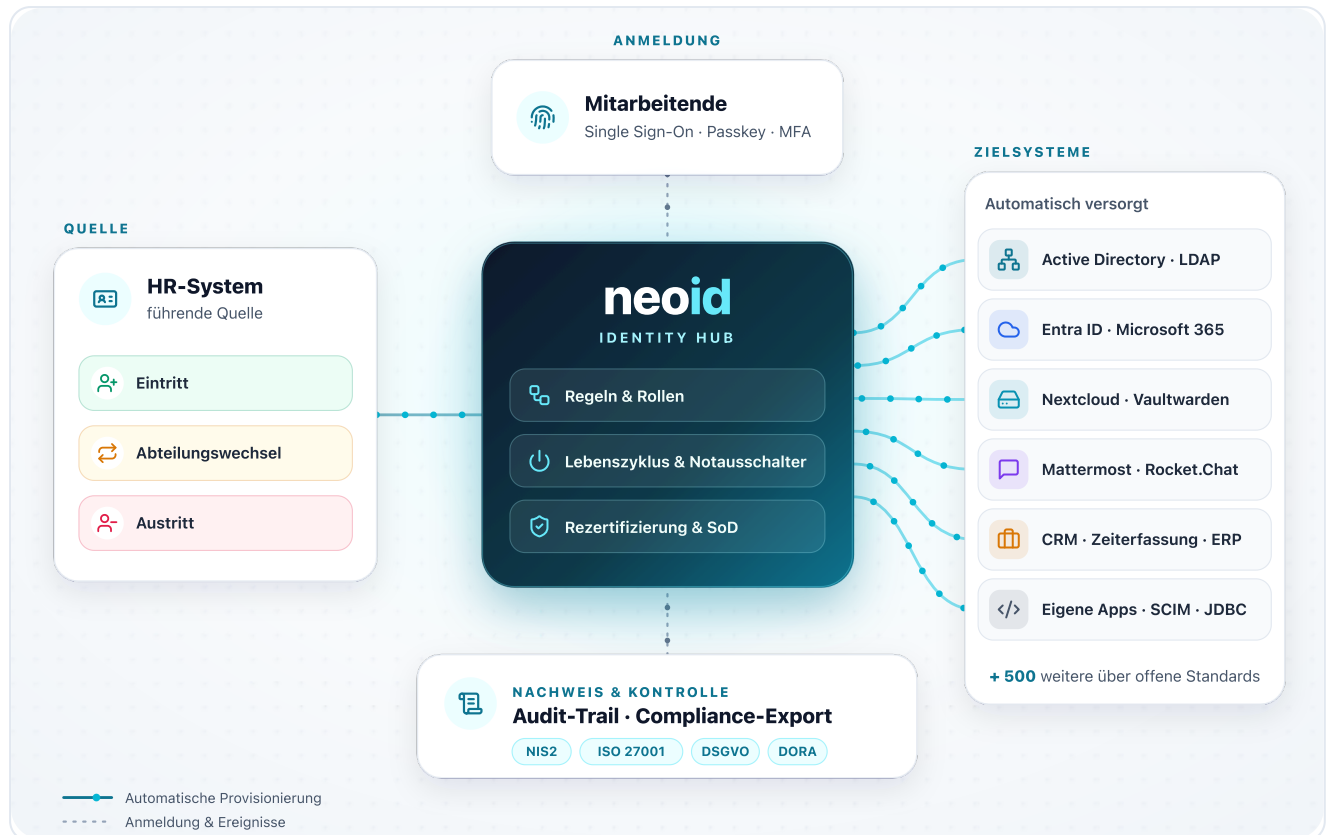
- ✓ Dutzende Systeme, kein Überblick: Benutzerkonten in 20+ Tools manuell verwalten – wer hat worauf Zugriff?
- ✓ ~500 Stunden pro Jahr für Routine: Onboarding, Passwort-Resets und Offboarding fressen Kapazität für strategische Projekte.
- ✓ Schatten-IT außer Kontrolle: Teams nutzen eigenmächtig SaaS-Tools – die IT erfährt es zuletzt oder nie.

Was ohne zentralen Identity Hub passiert

- ✓ Neue Mitarbeitende warten tagelang auf Zugänge – ein schlechter erster Eindruck und verlorene Produktivität
- ✓ Rechte werden bei Abteilungswechseln selten entzogen; Berechtigungen wachsen unkontrolliert
- ✓ Konten ehemaliger Mitarbeitender bleiben aktiv – ein offenes Tor für Datenabfluss
- ✓ Schatten-IT entsteht, weil Fachabteilungen eigenmächtig SaaS-Dienste nutzen
- ✓ Für Audits fehlen belastbare Nachweise, wer wann worauf Zugriff hatte

neoid im Überblick

Das HR-System ist die führende Quelle. neoid berechnet daraus, wer welche Zugänge braucht, und versorgt alle angebundenen Systeme automatisch – vom Eintritt über jeden Wechsel bis zum Austritt.



1 Joiner

Eintritt im HR-System → Konten und Rechte in allen Systemen zum ersten Tag.

2 Mover

Abteilungs- oder Rollenwechsel → neue Rechte sofort, alte werden entfernt.

3 Leaver

Austritt → alle Konten deaktiviert, alle Sitzungen beendet.

neoid muss Active Directory oder Microsoft Entra ID nicht ersetzen, sondern steuert sie als übergeordnete Orchestrierungsschicht. Wer später weniger Systeme betreiben möchte, kann Anmeldung und Benutzerverwaltung schrittweise zu neoid verlagern. Alle Anbindungen basieren auf offenen Standards wie SCIM 2.0, OpenID Connect, SAML 2.0, LDAP und WebAuthn – Sie bleiben unabhängig.

Funktionen

Die folgenden Funktionen sind in neoid verfügbar. Rechts steht das kleinste Paket, in dem die Funktion enthalten ist.

Anmeldung & Zugang

Ein Login für alle Anwendungen – passwortlos, phishing-resistent und ohne Helpdesk-Tickets.

Single Sign-On (OIDC & SAML)

[ab Starter](#)

Ein Login für beliebig viele Anwendungen über offene Standards.

Passwortlose Anmeldung

[ab Starter](#)

Passkeys (FIDO2/WebAuthn) per Fingerabdruck, Face ID oder Windows Hello – alternativ Passwort + MFA.

MFA-Richtlinien

[ab Starter](#)

Zweiten Faktor verpflichtend machen – mit Übergangsfrist und gruppenbasierter Pflicht.

Faktoren selbst registrieren

[ab Starter](#)

Passkey oder Authenticator-App direkt beim Login einrichten.

Erstzugang & Wiederherstellung

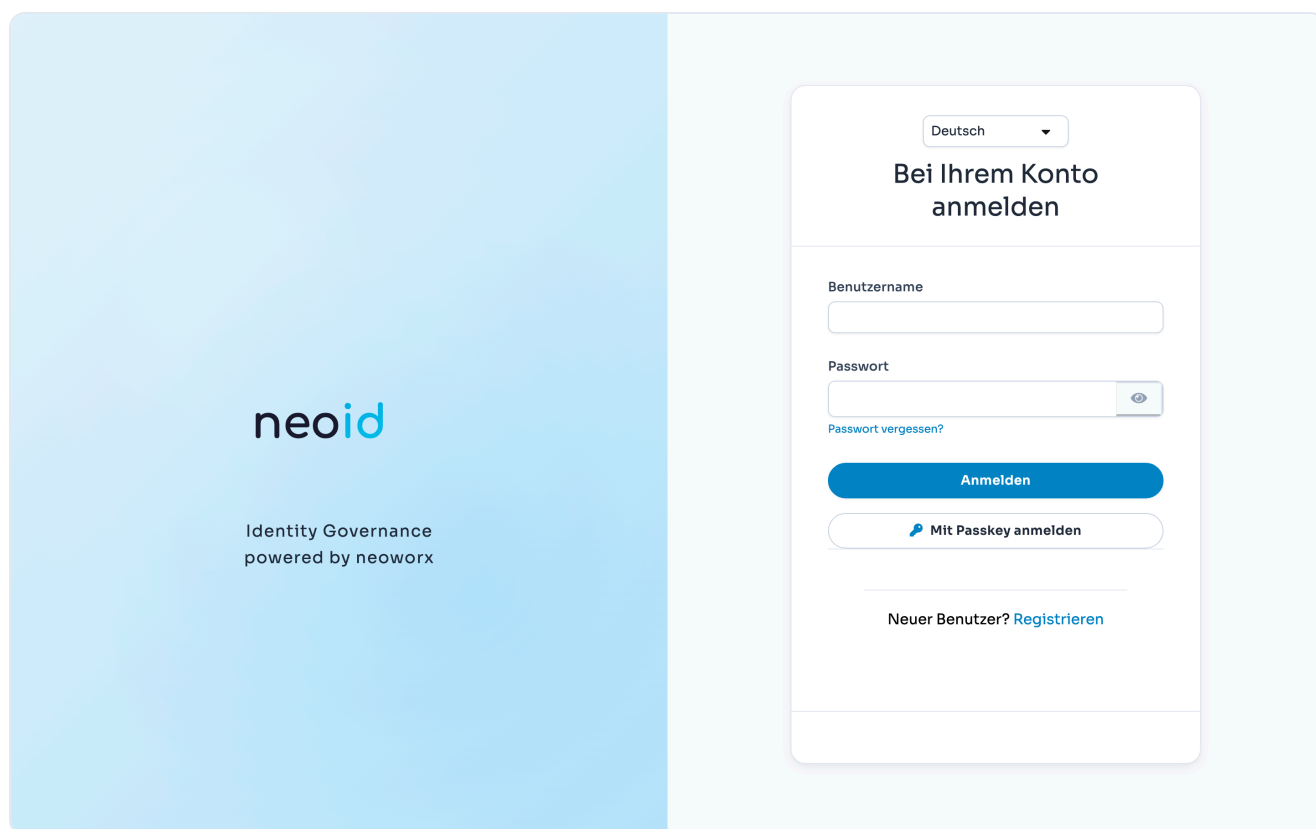
[ab Starter](#)

Erstanmeldung und Wiederherstellung verlorener Faktoren ohne Helpdesk – per Datenabgleich und SMS-Code.

Sitzungs- & Token-Laufzeiten

[ab Starter](#)

Sicherheit und Komfort verständlich ausbalancieren.

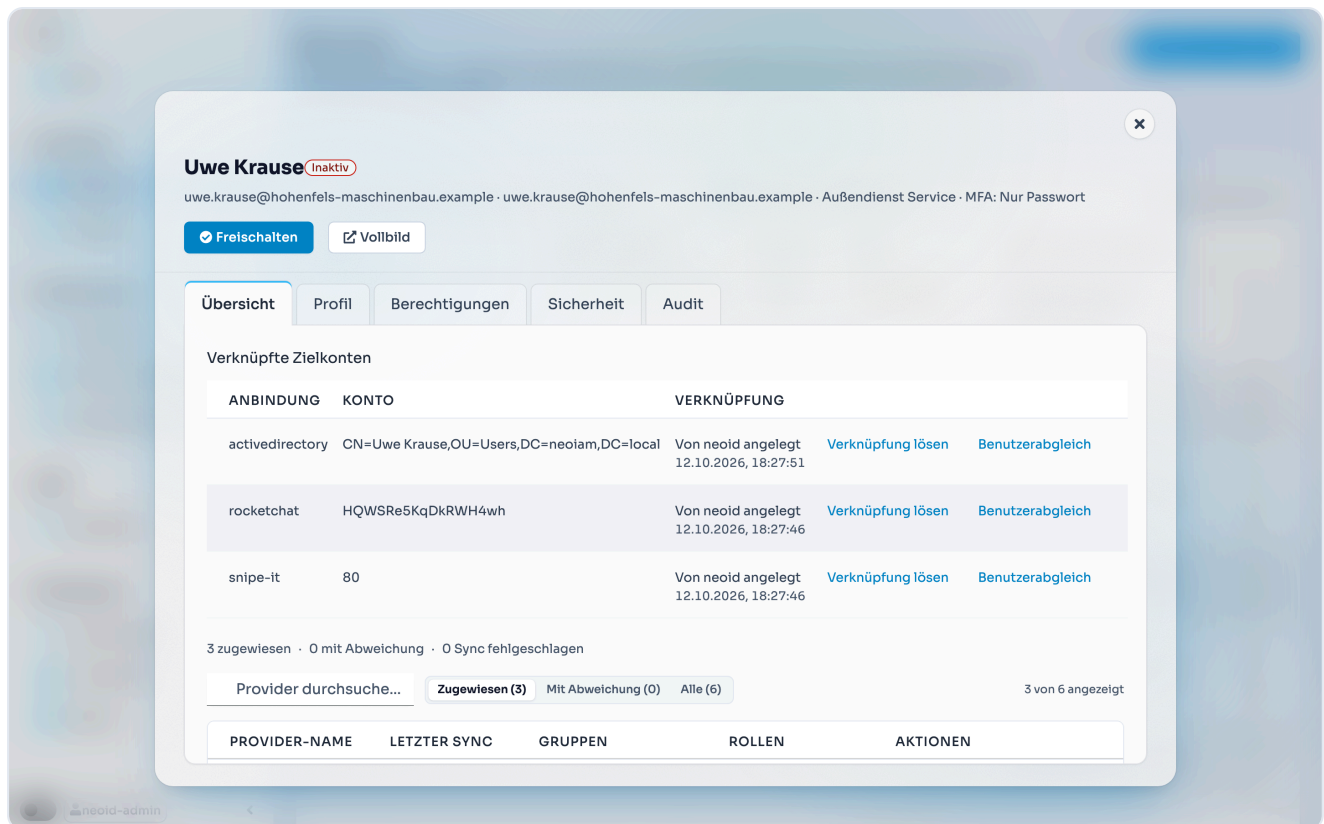


Anmeldung per Passkey – ohne Passwort.

Identitäten & Lebenszyklus

Das HR-System gibt den Takt vor: Zugänge ab dem ersten Arbeitstag und sofort gesperrt beim Austritt.

Zentrales Identitätsverzeichnis Alle Identitäten mit Standort, Land, Beschäftigungsart, Vertragsende und mehreren Abteilungen.	ab Starter
HR-Anbindung Das HR-System als führende Quelle, z. B. neoHR, Paychex, Personio oder per SCIM 2.0.	ab Starter
Automatischer Ein- und Austritt Zugänge zum Eintrittsdatum, Deaktivierung zum Austrittsdatum – ohne Ticket.	ab Starter
Geführte Benutzeranlage Schritt-für-Schritt-Assistent mit Vorschau, welche Rechte die neue Person erhält.	ab Starter
Notausschalter Konto sperren und alle Sitzungen beenden – sofort, in allen angebundenen Systemen.	ab Starter
Benutzerliste mit Sicherheitsstatus Status und Absicherung vieler Konten auf einen Blick.	ab Starter
Dashboard Zentrale Startseite mit den wichtigsten Kennzahlen.	ab Starter
Regelbasierte Gruppenzuweisung neoid-Gruppen automatisch anhand von Attributen zuweisen.	ab Starter



Alle Rechte einer Person in allen Systemen – inklusive Herkunft der Zuweisung.

Anbindungen & Provisionierung

Zielsysteme geführt anbinden, Bestandskonten sauber übernehmen und automatisch versorgen.

Provisionierungs-Anbindungen

ab Starter

Active Directory, Entra ID, LDAP, SCIM, JDBC, Nextcloud, Mattermost, Rocket.Chat, EspoCRM, Clockodo, Vaultwarden u. v. m.

Verbindungstest

ab Starter

Prüfen, ob eine Anbindung ihr Zielsystem erreicht – bevor etwas passiert.

Verschlüsselte Zugangsdaten

ab Starter

Passwörter, Tokens und Client-Secrets werden verschlüsselt gespeichert.

Geführte Einrichtung

ab Business

Bestand sichten, Regeln festlegen, Konten verknüpfen – auf einer Seite.

Kontenabgleich

ab Business

Bestehende Konten im Zielsystem finden und kontrolliert mit neoid-Benutzern verknüpfen.

Vorschau vor dem ersten Sync

ab Business

Sehen, was sich im Zielsystem ändert – inklusive entfernter Berechtigungen.

Nutzerkreis je Anbindung

ab Business

Festlegen, wer eine Anwendung nutzen darf – per Gruppe statt per Hand.

App-Rollen im Token

ab Business

Anwendungen erhalten Gruppen und Rollen direkt beim Login.

Kontenabgleich: activedirectory Active Directory Aktiv

Abgleichsschlüssel: E-Mail · Letzter Abgleich 12.10.2026, 18:26:29

Übersicht Erster Sync

[Erneut abgleichen](#) Getroffene Entscheidungen bleiben erhalten.

● 97 zugeordnet

Alles zugeordnet
Es ist nichts mehr zu entscheiden.

Bereits erledigt

97 verbunden
Mit ihrem Konto in Active Directory verbunden. [Ansehen >](#)

Wie werden Konten erkannt?
E-Mail [Ändern >](#)

Geführte Einrichtung: Bestand sichten, Regeln festlegen, Konten verknüpfen.

Regeln & Automatisierung

Wer welche Rechte bekommt, entscheiden nachvollziehbare Regeln – nicht E-Mails und Tickets.

Zuweisungsregeln für Gruppen & Rollen

ab Business

Attribute wie Abteilung oder Standort steuern automatisch Rechte in Zielsystemen – auch beim Rollenwechsel.

Einfacher & erweiterter Regel-Modus

ab Business

Geführter Formular-Modus oder verschachtelte UND/ODER-Bedingungen für komplexe Fälle.

Regelvorschläge

ab Business

neoid leitet nachvollziehbare Regeln aus dem bestehenden Berechtigungsbestand ab.

Simulation & Auswirkungsvorschau

ab Business

Vorab sehen, wen eine Regel betrifft – Entwürfe werden erst mit Freigabe wirksam.

Gezielte Ausführung

ab Business

Regeln kontrolliert außerhalb des automatischen Ablaufs anwenden.

Rollen- & Gruppenkatalog

ab Business

Sehen, welche Gruppen und Rollen ein Zielsystem tatsächlich anbietet.

Fremdzuweisungen erkennen & heilen

ab Business

Rechte, die am Hub vorbei vergeben wurden, aufdecken und bereinigen.

Delegierte Administration

ab Business

Verwaltung einzelner Anbindungen an Fachverantwortliche übergeben.

neoid

Start

Verwaltung

Benutzer

Gruppen

ID-Governance

Zuweisung

Prüfung & Freigaben

Funktionstrennung

Audit

Ereignisse

Einstellungen

Anbindungen

Anmeldung

System

neoid-admin

Zuweisung

Weist Benutzern automatisch Gruppen und Rollen anhand ihrer Attribute zu.

RegelnMeine Rezertifizierungen

Zielsystem

neoid

neoid

9

- 9 mit

Regeln Handlungsbedarf

Externe Provider

activedirectory

21

- 21 mit

Regeln Handlungsbedarf

openldap

3

- 3 mit

Regeln Handlungsbedarf

espocrm

4

- 4 mit

Regeln Handlungsbedarf

legacy-erp

6

- 6 mit

Regeln Handlungsbedarf

rocketchat

17

- 17 mit

Regeln Handlungsbedarf

snipe-it

2

- 2 mit

Regeln Handlungsbedarf

Handlungsbedarf

9 von 9 Regeln brauchen Aufmerksamkeit

0

Regeln mit Ausnahmen

0

Regeln laufen bald ab

0

Prüfungen überfällig

9

Regeln ohne Verantwortliche

Provider-Katalog (neoid)

Gruppen 10

Rollen

Gruppen filtern ...

Von diesem Provider nicht unterstützt.

Regeln, Bedingungen, Ziele durchsuchen ...

Alle

Aktiv

Inaktiv

9 von 9 Regeln

Zuweisungsregeln im geführten Formular-Modus – ohne Programmierkenntnisse.

Audit & Nachvollziehbarkeit

Jede Änderung ist dokumentiert: wer, was, wann – mit Vorher-/Nachher-Vergleich.

Audit-Log

Anmelde- und Administrationsereignisse lückenlos protokolliert.

ab Starter

Änderungsdetails mit Vorher/Nachher

Strukturierte Zusammenfassung und Attribut-Diff zu jeder Änderung.

ab Business

Unveränderliche Regel-Historie

Jeder Regelstand ist jederzeit nachvollziehbar.

ab Business

neoid

Start

Verwaltung

Benutzer

Gruppen

ID-Governance

Zuweisung

Prüfung & Freigaben

Funktionstrennung

Audit

Ereignisse

Einstellungen

Anbindungen

Anmeldung

System

neoid-admin

Provisionierungs-Events, synchronisierte Benutzer und angebundene Provider.

Event-Log

Benutzer

Provider

Übersicht für die aktuellen Filter

2 Fehlgeschlagen

796 Zurückgehalten

3.519 Ereignisse

Akteur

Nach Akteur filt...

Zielsystem

Nach Zielsystem...

Kategorie

Alle Kategorien

Datumsbereich

Benutzerdefi...

Von

mm/dd/yyyy, --:--:--

Bis

mm/dd/yyyy, --:--:--

ZEITPUNKT

EREIGNISTYP

EREIGNIS

Heute · Dienstag, 13.10.2026

09:52:27
Nr. 3519

Sperr
Provisionierung

petra.lange@hohenfels-n
Skipped: no linked accou
Akteur: service-account-ne
Request-ID 6fc547b5 ...

09:52:27
Nr. 3518

Sperr
Provisionierung

petra.lange@hohenfels-n
Skipped: no linked accou
Akteur: service-account-ne
Request-ID 6fc547b5 ...

09:52:27
Nr. 3517

Aktualisieren
Provisionierung

petra.lange@hohenfels-n
Provisioning successful
Akteur: service-account-ne
Request-ID 6fc547b5 ...

Aktualisieren: petra.lange@hohenfels-maschinenbau.example

snipe-it | 13.10.2026, 09:52:27

Aktionsübersicht

Benutzerattribute aktualisiert

Ereignis

ID

3517

Erstellt am

13.10.2026, 09:52:27

Kategorie

Provisionierung

Operation

Aktualisieren

Status

Erfolgreich

Akteur

service-account-neoiam-scim-provisioner

Ziel-Benutzer

petra.lange@hohenfels-maschinenbau.example
956c9a07-9ca8-4e2d-bb2d-32d302c2e521

Zielsystem

snipe-it
423d9ce8-7e08-48f9-85e0-710375d76770

Request-ID

6fc547b5-a91e-43e6-83f7-d426f6db241e

Nachricht

Provisioning successful

Attributänderungen (Vorher / Nachher)

Keine Attributänderungen erfasst.

> Benutzerinformationen

Schließen

Gleiche Anfrage

Jede Änderung mit Vorher/Nachher – revisionssicher.

Governance & Compliance

Zugriffe regelmäßig bestätigen, Funktionstrennung durchsetzen und Nachweise auf Knopfdruck liefern.

Rezertifizierung

Periodische und anlassbezogene Kampagnen inkl. Rollen-Review, Drift-Erkennung, Erinnerungen und Ausnahmen.

ab Governance

Prüfkontrollen

Keine Selbst-Rezertifizierung, Begründungspflicht bei Bestätigungen.

ab Governance

Funktionstrennung (SoD)

Konfliktregeln über Systeme hinweg – geprüft bei jeder Regeländerung.

ab Governance

SoD-Überwachung

Regelmäßige Hintergrundprüfung mit Benachrichtigung, Ausnahmen als dokumentierte Risiken, Vorschlagsassistent und SoD-Dashboard.

ab Governance

Regel-Verantwortliche

Jede Regel hat einen Owner, der sie regelmäßig bestätigt.

ab Governance

Revisionssicherer Compliance-Export

Regeln, Rezertifizierungen und SoD-Status als Nachweis für Prüfer.

ab Governance

Schatten-IT erkennen

E-Mail-Domain-Monitoring, SSO-Adoption-Flow und zentrales App-Verzeichnis.

ab Governance

Fällige Prüfungen, SoD-Status und Handlungsbedarf auf einen Blick.

neoid

Start

Verwaltung

Benutzer

Gruppen

ID-Governance

Zuweisung

Prüfung & Freigaben

Funktionstrennung

Audit

Ereignisse

Einstellungen

Anbindungen

Anmeldung

System

neoid-admin

Prüfung & Freigaben

Regelmäßige Überprüfung von Gruppen-Mitgliedschaften und Rollenzuweisungen in neoid und angebundenen Providern.

Kampagnen

Meine Prüfungen

Provisionierungslücken

Konfiguration

Laufend

1

Überfällig

0

Abgeschlossen

0

Offene Alerts

0

Kampagne starten

Alle Status

Suchen ...

CSV exportieren

1-1 of 1

KAMPAGNEN-ID	AUSLÖSER	UMFANG	STATUS	GESTARTET	FÄLLIG	FORTSCHRITT
0f883df0-55ee-436c-b8e8-54492087abca	Manuell	Alle Benutzer ⌵ Abteilung beginnt mit „Vertrieb“	Offen	12.10.2026, 18:29:44	10.4.2027, 18:29:44	0 / 117

1-1 of 1

<< < 1 of 1 > >>

Rezertifizierungskampagnen mit Fortschritt und Fristen.

KI-Assistent neoassist

Zugriffsprobleme in Sekunden verstehen – mit Vorschlägen, die erst nach Ihrer Bestätigung wirken.

360°-Zugriffsdiagnose

ab Business

Warum hat jemand keinen Zugriff? neoassist erklärt die Ursache und erkennt Abweichungen.

Vorbereitete Aktionen mit Bestätigung

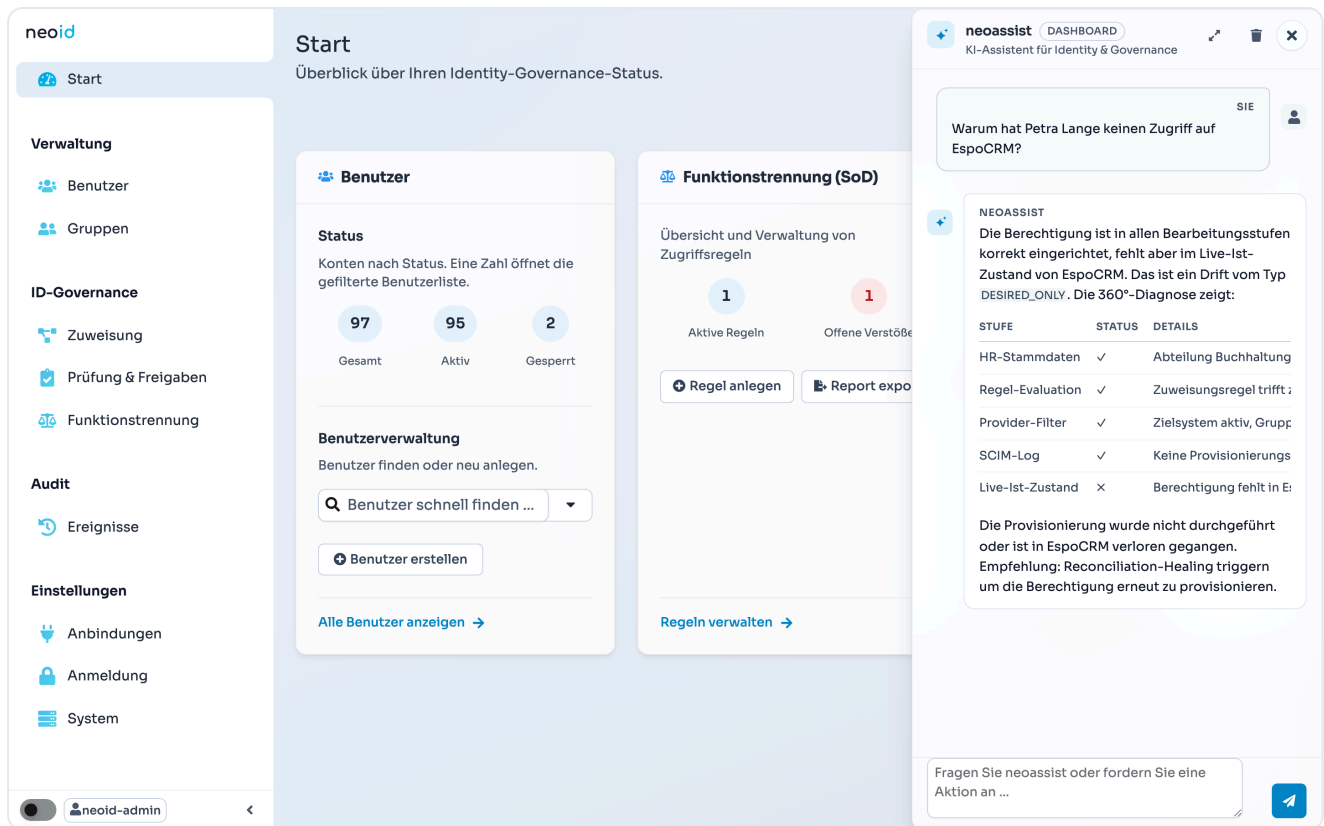
ab Business

neoassist ändert nichts selbstständig – jede Korrektur wird erst nach Ihrer Freigabe ausgeführt.

Eigenes KI-Modell

ab Business

Wahl des Sprachmodells, auch selbst gehostet (z. B. Ollama).



neoassist erklärt die Ursache und bereitet die Korrektur zur Freigabe vor.

Betrieb & Sicherheit

Zero-Knowledge, offene Standards und freie Wahl zwischen Cloud und On-Premises – in jedem Paket.

Zero-Knowledge-Architektur

ab Starter

Ende-zu-Ende-Verschlüsselung – auch neoworx kann Ihre Geheimnisse nicht lesen.

Cloud oder On-Premises

ab Starter

Als Cloud-Service in zertifizierten Rechenzentren in Deutschland und der EU oder On-Premises bzw. hybrid in Ihrer Infrastruktur – in jedem Paket.

Offene Standards

ab Starter

SCIM 2.0, OIDC, SAML, LDAP und WebAuthn – kein Vendor Lock-in.

Support

ab Starter

Deutschsprachiger Support direkt vom Hersteller.

Mehr als 5.000 Identitäten & Mandanten

ab Enterprise

Mehrere Mandanten bzw. Realms in einer Installation.

Individuelle Anbindungen

ab Enterprise

Anbindung von Fachsystemen ohne Standardschnittstelle.

SLA & Implementierungsbegleitung

ab Enterprise

Garantierte Reaktionszeiten, fester Ansprechpartner, begleitete Einführung.

Integration

Nicht jede Anwendung unterstützt moderne Standards gleich gut. neoid bietet abgestufte Möglichkeiten – von nativem Single Sign-On bis zum Workaround für Altsysteme.

1

STUFE 1 · OPTIMAL

Nativer Support (OIDC, SAML, SCIM)

Die Anwendung spricht offene Standards.

- ✓ Benutzerverwaltung in neoid
- ✓ Import aus dem HR-System
- ✓ Anmeldung über neoid inkl. Passkey und MFA

2

STUFE 2 · GUT

Vorhandene Standard-API

Ein vorgefertigter Konnektor nutzt die Schnittstelle der Anwendung.

- ✓ Benutzerverwaltung in neoid
- ✓ Import aus dem HR-System
- ✓ Synchronisation von Konten, Gruppen und Rollen

3

STUFE 3 · MÖGLICH

Hybrid & On-Premises

Lokale Verzeichnisse, Datenbanken und Fachsoftware – über sichere Anbindung, ohne eingehende Firewall-Ports.

- ✓ Active Directory und LDAP
- ✓ Datenbanken per generischem JDBC-Konnektor
- ✓ Zentrale Steuerung auch für Altsysteme

4

STUFE 4 · WORKAROUND

Keine direkte Integration

Auch ohne Schnittstelle bleibt kein System unkontrolliert.

- ✓ Zugriff auf die Datenbank
- ✓ File-Export und -Import
- ✓ Strukturierter Prozess mit Benachrichtigung

Vorgefertigte Konnektoren

Active Directory	Benutzer, Passwörter und Gruppen in On-Premises-AD.
Microsoft Entra ID	Cloud-Identitäten und Gruppen für Microsoft 365.
LDAP v3	OpenLDAP und kompatible Verzeichnisdienste.
SCIM 2.0 (generisch)	Jeder SCIM-fähige Dienst – inkl. Gruppen.
JDBC (generisch)	Eigenentwicklungen und Fachanwendungen mit Datenbank.
Nextcloud	Konten, Gruppen, Speicher und Profilbilder.
Mattermost	Konten sowie Team- und Kanalzuweisung.
Rocket.Chat	Konten und Rollen für Team-Kommunikation.
EspoCRM	Benutzer, Teams und Rollen im CRM.
Clockodo	Zeiterfassung mit automatischem Ein- und Austritt.
Vaultwarden	Passwort-Tresor für Altsysteme und geteilte Zugänge.
S3	Ablage von Profilbildern und Medien.

HR- und Quellsysteme

neoHR, Paychex, Personio, HRworks, SAP SuccessFactors, BambooHR, Workday und weitere – oder per SCIM 2.0, REST, CSV-Import und Webhooks.

Beispiel: vom HR-System bis Active Directory und Entra ID

1 Eintritt im HR-System

Eine neue Mitarbeiterin wird in neoHR mit Abteilung Vertrieb und Eintrittsdatum angelegt.

2 Regeln in neoid

Die Zuweisungsregel „Abteilung = Vertrieb“ ergibt die Gruppe „Vertrieb“ in Active Directory und Entra ID sowie den Zugang zum CRM.

3 Provisionierung

Zum Eintrittsdatum legt neoid die Konten an und setzt die Gruppen. Am ersten Tag richtet die neue Kollegin ihren Passkey ein.

4 Austritt

Mit dem Austrittsdatum deaktiviert neoid alle Konten und beendet alle Sitzungen – dokumentiert im Audit-Trail.

Sicherheit & Compliance

Notausschalter

Ein Klick – oder ein API-Aufruf – sperrt alle Zugänge einer Person oder Gruppe in Echtzeit, über alle angebundenen Systeme hinweg.

1

Konto sperren

Auslösung in der neoid-Oberfläche oder per API.

2

Token-Invalidierung

Aktive Access- und Refresh-Tokens werden gesperrt.

3

Backchannel-Logout

OIDC-fähige Anwendungen beenden laufende Sitzungen.

4

De-Provisionierung

Alle angebundenen Zielsysteme erhalten die Deaktivierung.

5

Audit-Log

Zeitgestempelter Eintrag mit auslösender Person.

6

Benachrichtigung

Alerts an Security-Team, IT-Leitung oder SIEM.

Passwortlose Anmeldung

neoid ermöglicht den Weg in eine passwortlose Zukunft – auf Basis offener Standards wie FIDO2, WebAuthn und Passkeys.

80 %

aller Datenschutzverletzungen
gehen auf kompromittierte
Passwörter zurück
Verizon DBIR

100+

Passwörter hat ein
durchschnittlicher Nutzer
NordPass

65 %

nutzen dasselbe Passwort für
mehrere Dienste
Google Security Study

Zero-Knowledge-Architektur

Zero-Knowledge ist eine architektonische Garantie: neoworx hat technisch keinen Zugriff auf Ihre Zugangsdaten oder Geheimnisse.

AES-256-GCM

Verschlüsselung
ruhender Daten

PBKDF2

600.000+ Iterationen
zur Schlüsselableitung

FIDO2

Phishing-resistente
Authentifizierung

TLS 1.3

Transport mit Perfect
Forward Secrecy

Regulatorik

1 NIS2-Richtlinie

Pflichten für wichtige und besonders wichtige Einrichtungen.

- ✓ Art. 21 Abs. 2 (b): Zugangskontrolle und Identitätsmanagement
- ✓ Art. 21 Abs. 2 (e): Sicherheit in der Lieferkette (externe Zugänge)
- ✓ Art. 21 Abs. 2 (i): Multi-Faktor-Authentifizierung
- ✓ Art. 23: Meldepflichten mit lückenlosen Incident-Logs

2 ISO 27001:2022

Der Standard für Informationssicherheits-Managementsysteme.

- ✓ A.5.15 / A.5.16: Zugriffskontrolle und Identitätsverwaltung
- ✓ A.5.18: Zugriffsrechte (Provisionierung und Deprovisionierung)
- ✓ A.8.2: Privilegierte Zugriffsrechte
- ✓ A.8.15: Logging – unveränderliche Audit-Trails

3 DSGVO

Anforderungen an Verarbeitung, Speicherung und Löschung personenbezogener Daten.

- ✓ Art. 5: Datensparsamkeit
- ✓ Art. 17: Recht auf Löschung
- ✓ Art. 25: Privacy by Design – Zero-Knowledge-Architektur
- ✓ Art. 30: Verzeichnis der Verarbeitungstätigkeiten

4

DORA

IKT-Risikomanagement für Finanzunternehmen.

- ✓ Regelmäßige Überprüfung von Zugriffsrechten
- ✓ Funktionstrennung über Systeme hinweg
- ✓ Keine Selbst-Rezertifizierung, Begründungspflicht
- ✓ Revisionssicherer Nachweis für Prüfer

Der CRA gilt schon – die Meldepflicht läuft seit September 2026

Der Cyber Resilience Act (EU 2024/2847) betrifft Hersteller, Importeure und Händler von Hardware und Software mit digitalen Elementen – von der vernetzten Maschine bis zur Fachanwendung. Seit dem 11. September 2026 müssen aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle gemeldet werden, auch für Produkte, die schon auf dem Markt sind.

1

10. DEZEMBER 2024

In Kraft getreten

Die Verordnung gilt unmittelbar in allen EU-Mitgliedstaaten – ohne nationales Umsetzungsgesetz.

2

11. SEPTEMBER 2026 · GILT BEREITS

Meldepflichten

Aktiv ausgenutzte Schwachstellen und schwere Vorfälle gehen an das zuständige CSIRT und an ENISA.

- ✓ Frühwarnung innerhalb von 24 Stunden
- ✓ Meldung innerhalb von 72 Stunden
- ✓ Abschlussbericht nach 14 Tagen bzw. einem Monat

3

11. DEZEMBER 2027

Alle Pflichten

Neue Produkte kommen nur noch mit CE-Kennzeichnung nach CRA auf den Markt.

- ✓ Security by Design und Risikobewertung
- ✓ Schwachstellenmanagement über den Support-Zeitraum
- ✓ Technische Dokumentation für die Marktüberwachung

- ✓ Vorfälle schnell eindämmen: Der Notausschalter sperrt ein kompromittiertes Konto in allen angebundenen Systemen und beendet alle Sitzungen – in Sekunden statt Stunden.

- ✓ **Fristgerecht melden:** Der Audit-Trail zeigt, wer wann worauf Zugriff hatte. Damit stehen die Fakten für Frühwarnung, Meldung und Abschlussbericht bereit.
- ✓ **Entwicklung absichern:** Zugänge zu Repositories, Build-Servern und Signierschlüsseln nur nach Rolle, mit Passkeys und regelmäßiger Rezertifizierung.
- ✓ **Externe im Blick:** Konten von Dienstleistern und externen Entwicklern sind zentral erfasst, rezertifizierbar und mit einem Klick gesperrt.

Identitätsmanagement-Systeme zählen nach Anhang III des CRA zu den wichtigen Produkten der Klasse I und unterliegen damit strengeren Anforderungen an die Konformitätsbewertung. Wir bereiten neoid auf die CRA-Pflichten vor. Diese Übersicht ersetzt keine Rechtsberatung. Ob und in welcher Rolle Ihr Unternehmen betroffen ist, hängt von Ihren Produkten ab.

Governance-Funktionen

- ✓ **Rezertifizierung:** Periodische und anlassbezogene Kampagnen: Verantwortliche bestätigen oder entziehen Zugriffe – mit Erinnerungen, Fristen und Ausnahmen.
- ✓ **Funktionstrennung (SoD):** Konfliktregeln über Systeme hinweg, Prüfung bei jeder Regeländerung, nächtliche Überwachung und dokumentierte Ausnahmen.
- ✓ **Unveränderliche Audit-Logs:** Zeitgestempelte Protokolle aller Zugriffsänderungen mit Vorher/Nachher – exportierbar.
- ✓ **Compliance-Export:** Regelstände, Rezertifizierungen und SoD-Status als revisionssicherer Nachweis.
- ✓ **Regel-Verantwortliche:** Jede Zuweisungsregel hat einen Owner, der sie regelmäßig bestätigt.
- ✓ **Governance-Dashboard:** Fällige Prüfungen und offene Konflikte auf einen Blick.

Einführung

Kein Big-Bang-Rollout: neoid wird iterativ eingeführt – Abteilung für Abteilung, System für System.

1

WOCHE 1-2

Discovery & Analyse

Gemeinsamer Überblick über Systeme, Nutzer und Zugriffsrechte.

- ✓ Bestandsaufnahme aller Anwendungen
- ✓ Ist-Analyse von Identitäten und Rechten
- ✓ Verwaiste Konten und Schatten-IT identifizieren
- ✓ Rollenkonzept-Workshop mit HR und IT

2

WOCHE 2-3

Pilot-Integration

Anbindung des ersten Zielsystems – typischerweise Microsoft 365 oder Active Directory – mit 5-10 Testnutzern.

- ✓ HR-System anbinden (lesend)
- ✓ Erstes Zielsystem integrieren
- ✓ Joiner, Mover, Leaver im Test validieren

3

WOCHE 3-5

Schrittweiser Rollout

System für System und Abteilung für Abteilung – nichts wird ohne Prüfung und Freigabe übernommen.

- ✓ Weitere Zielsysteme anbinden
- ✓ Abteilungen schrittweise übernehmen
- ✓ HR- und IT-Ansprechpartner schulen
- ✓ Audit-Trail und Compliance-Berichte aktivieren

Optimierung & Betrieb

Feinabstimmung: Self-Service, Rezertifizierung und Monitoring werden aktiviert.

- ✓ Self-Service für Wiederherstellung
- ✓ Periodische Zugriffsprüfungen
- ✓ SIEM-Anbindung und Alarmer
- ✓ Übergabe in den Betrieb

Der dargestellte Plan ist ein typisches Beispiel. Die tatsächliche Dauer hängt von Unternehmensgröße und Anzahl der Anwendungen ab.

Was passiert mit bestehenden Konten?

- ✓ Bestehende Konten werden gefunden und nach Ihrer Bestätigung mit den richtigen Personen verknüpft.
- ✓ Verwaiste Konten werden sichtbar und zur Prüfung vorgelegt.
- ✓ Vor dem ersten Sync zeigt neoid, was sich im Zielsystem ändern würde.
- ✓ Ab Stichtag übernimmt neoid die Steuerung aller neuen Ereignisse – Altbestände folgen in Ihrem Tempo.

Was wir vorab von Ihnen brauchen

- ✓ Zugang zum HR-System (API-Key oder Webhook)
- ✓ Service-Konto für AD/Entra ID – wir zeigen Ihnen die genauen Berechtigungen
- ✓ Liste der anzubindenden Systeme (Top 3–5 zuerst)
- ✓ Rollenkonzept – wir liefern eine Vorlage
- ✓ Je eine Ansprechperson aus IT und HR für wöchentliche 30-Minuten-Termine

Pakete & Preise

Alle Pakete wahlweise als Cloud-Service (Hosting in Deutschland & EU) oder On-Premises bzw. hybrid in Ihrer Infrastruktur. Abgerechnet wird pro aktiver Identität und Monat (jährliche Abrechnung, zzgl. USt.), Mindestabnahme 50 Identitäten.

Cloud: Wir betreiben neoid für Sie – Hosting in Deutschland & EU, inklusive Betrieb, Monitoring, Backups, Updates und Support.

On-Premises: Sie betreiben neoid in Ihrer eigenen Infrastruktur (auch hybrid) – rund 30 % günstiger, Updates und Support inklusive.

Starter

3 € Cloud

2 € On-Premises

pro aktiver Identität / Monat · ab 150 € / 100 € / Monat

Für Unternehmen, die mit sicherem Login und automatischem Ein- und Austritt starten.

- ✓ Single Sign-On für beliebig viele Apps
- ✓ Passwortlos mit Passkeys oder Passwort + MFA
- ✓ HR-Anbindung mit automatischem Ein- und Austritt
- ✓ Notausschalter für alle Sitzungen
- ✓ Bis zu 3 Anbindungen an Zielsysteme
- ✓ Cloud oder On-Premises

Business

6 € Cloud

4 € On-Premises

pro aktiver Identität / Monat · ab 300 € / 200 € / Monat

Für Unternehmen, die alle Systeme regelbasiert und ohne Tickets versorgen wollen.

- ✓ Unbegrenzte Anbindungen aus dem Konnektor-Katalog
- ✓ Zuweisungsregeln für Rollenwechsel (Mover)
- ✓ Simulation & Auswirkungsvorschau
- ✓ Kontenabgleich & geführte Einrichtung
- ✓ KI-Assistent neoassist inkl. eigenem KI-Modell

Governance

11 € Cloud

8 € On-Premises

pro aktiver Identität / Monat · ab 550 € / 400 € / Monat

Für Unternehmen, die Zugriffe nach NIS2, ISO 27001 oder DORA nachweisen müssen.

- ✓ Rezertifizierungskampagnen
- ✓ Funktionstrennung (SoD) mit Überwachung
- ✓ Revisionssicherer Compliance-Export
- ✓ Schatten-IT erkennen
- ✓ Governance-Dashboard

Enterprise

Preis auf Anfrage

Für große oder regulierte Organisationen mit individuellen Anforderungen.

- ✓ Mehr als 5.000 Identitäten & Mandanten
- ✓ Individuelle Anbindungen
- ✓ SLA & fester Ansprechpartner

Funktionsvergleich

Funktion	Starter	Business	Governance	Enterprise
ANMELDUNG & ZUGANG				
Single Sign-On (OIDC & SAML)	✓	✓	✓	✓
Passwortlose Anmeldung	✓	✓	✓	✓
MFA-Richtlinien	✓	✓	✓	✓
Faktoren selbst registrieren	✓	✓	✓	✓
Erstzugang & Wiederherstellung	✓	✓	✓	✓
Sitzungs- & Token-Laufzeiten	✓	✓	✓	✓
IDENTITÄTEN & LEBENSZYKLUS				
Zentrales Identitätsverzeichnis	✓	✓	✓	✓
HR-Anbindung	✓	✓	✓	✓
Automatischer Ein- und Austritt	✓	✓	✓	✓
Geführte Benutzeranlage	✓	✓	✓	✓
Notausschalter	✓	✓	✓	✓
Benutzerliste mit Sicherheitsstatus	✓	✓	✓	✓
Dashboard	✓	✓	✓	✓
Regelbasierte Gruppenzuweisung	✓	✓	✓	✓

Funktion	Starter	Business	Governance	Enterprise
ANBINDUNGEN & PROVISIONIERUNG				
Provisionierungs-Anbindungen	bis zu 3	✓	✓	✓
Verbindungstest	✓	✓	✓	✓
Verschlüsselte Zugangsdaten	✓	✓	✓	✓
Geführte Einrichtung	–	✓	✓	✓
Kontenabgleich	–	✓	✓	✓
Vorschau vor dem ersten Sync	–	✓	✓	✓
Nutzerkreis je Anbindung	–	✓	✓	✓
App-Rollen im Token	–	✓	✓	✓
REGELN & AUTOMATISIERUNG				
Zuweisungsregeln für Gruppen & Rollen	–	✓	✓	✓
Einfacher & erweiterter Regel-Modus	–	✓	✓	✓
Regelvorschläge	–	✓	✓	✓
Simulation & Auswirkungsvorschau	–	✓	✓	✓
Gezielte Ausführung	–	✓	✓	✓
Rollen- & Gruppenkatalog	–	✓	✓	✓
Fremdzuweisungen erkennen & heilen	–	✓	✓	✓
Delegierte Administration	–	✓	✓	✓
AUDIT & NACHVOLLZIEHBARKEIT				
Audit-Log	✓	✓	✓	✓
Änderungsdetails mit Vorher/Nachher	–	✓	✓	✓
Unveränderliche Regel-Historie	–	✓	✓	✓
GOVERNANCE & COMPLIANCE				
Rezertifizierung	–	–	✓	✓
Prüfkontrollen	–	–	✓	✓
Funktionstrennung (SoD)	–	–	✓	✓
SoD-Überwachung	–	–	✓	✓
Regel-Verantwortliche	–	–	✓	✓

Funktion	Starter	Business	Governance	Enterprise
Revisionssicherer Compliance-Export	–	–	✓	✓
Schatten-IT erkennen	–	–	✓	✓
Governance-Dashboard	–	–	✓	✓
KI-ASSISTENT NEOASSIST				
360°-Zugriffsdiagnose	–	✓	✓	✓
Vorbereitete Aktionen mit Bestätigung	–	✓	✓	✓
Eigenes KI-Modell	–	✓	✓	✓
BETRIEB & SICHERHEIT				
Zero-Knowledge-Architektur	✓	✓	✓	✓
Cloud oder On-Premises	✓	✓	✓	✓
Offene Standards	✓	✓	✓	✓
Support	E-Mail	E-Mail & Telefon, priorisiert	E-Mail & Telefon, priorisiert	SLA, fester Ansprechpartner
Mehr als 5.000 Identitäten & Mandanten	–	–	–	✓
Individuelle Anbindungen	–	–	–	✓
SLA & Implementierungsbegleitung	–	–	–	✓

Einführung, Rollenkonzept-Workshop und individuelle Anbindungen bieten wir nach Aufwand an – mit Festpreisangebot nach einem gemeinsamen Workshop. Typisch: produktiv in 6 Wochen.

Über neoworx

neoid wird von neoworx in Deutschland entwickelt und in Deutschland und der EU gehostet – oder läuft On-Premises in Ihrer Infrastruktur. Unser Anspruch: Identity Governance auf Enterprise-Niveau, die zum Mittelstand passt – schnell eingeführt, transparent bepreist und auf offenen Standards gebaut.

- ✓ Entwickelt in Deutschland: Von neoworx entwickelt, gehostet in Deutschland und der EU – mit deutschsprachigem Support.
- ✓ Cloud oder On-Premises: In jedem Paket: Hosting in Deutschland & EU mit AV-Vertrag – oder Betrieb in Ihrer eigenen Infrastruktur, rund 30 % günstiger.
- ✓ Offene Standards: SCIM 2.0, OIDC, SAML, LDAP und WebAuthn – Sie bleiben unabhängig.
- ✓ Zero-Knowledge: Ende-zu-Ende-Verschlüsselung: Auch neoworx kann Ihre Geheimnisse nicht lesen.
- ✓ In 6 Wochen produktiv: Iterative Einführung – System für System, ohne Big-Bang-Rollout.
- ✓ Direkt mit den Architekten: Sie sprechen mit den Menschen, die neoid bauen – nicht mit einem Callcenter.

Sprechen Sie mit uns

In einer 20-minütigen Live-Demo zeigen wir Ihnen neoid an echter Software und klären, wie es in Ihre Systemlandschaft passt.

www.neoid.eu/kontakt · identityhub@neoworx.eu · +49 (0) 61 96 / 7 80 93 80
neoworx GmbH · Mergenthalerallee 73–75 · 65760 Eschborn