



Extern · für Zscaler-erfahrene Entscheider

CentaurNexus

Single Pane of Glass für Zscaler — Plattform-
Überblick

01 Was ist CentaurNexus?

CentaurNexus ist eine mandantenfähige SaaS-Plattform, die **ZIA, ZPA und ZDX** (sowie die übrigen Zscaler-Produktfamilien) unter einer einzigen, rollenbasierten Oberfläche bündelt. Ziel: Enterprise-IT-Teams und Helpdesk arbeiten produktiv mit Zscaler, **ohne** dass jeder Vollzugriff auf die Zscaler-Admin-Konsole braucht.

- Gehostet auf **STACKIT** (europäische Cloud, DSGVO-konform).
- Harte Mandantentrennung über PostgreSQL Row-Level-Security.
- Capability-gesteuert: jeder Kunde sieht genau die Funktionen seiner lizenzierten Zscaler-Produkte.

02 Die Oberflächen für Ihre Teams

Self-Service

End-User lösen URL-Freigaben, App-Zugänge, BYOD-Onboarding & Co. selbst — entlastet den Helpdesk.

Helpdesk & IT-Admin

360°-Suche, Diagnose, Freigabe-Queues, Policy-Workflows, Backup/Restore, Compliance — der Arbeitsplatz fürs Tagesgeschäft.

Extend (Partner/M&A)

Clientloser Partnerzugang, Vendor-Sessions und M&A-Clean-Rooms für externe Beteiligte.

ADMIN

Kein Kontakt zum Lizenzserver seit 3 Tagen. Noch 2 Tage Grace Period verbleibend. Bitte kontaktieren Sie uns: support@centaurnexus.com

Helpdesk Overview

Offene Freigaben: 0

Gesamt Freigaben: 0

Audit-Events heute: 0

Stale / Konflikte: 11

Ausstehende Freigaben

Alle anzeigen →

URL	VON	DATUM	STATUS
Keine offenen Anträge			

Schnellzugriff

- 360° Unified Overview
Alle Zscaler-Daten zu einem User
- VIP Fast-Lane
ZDX-Diagnose für VIP-User starten
- Ruleset Optimizer
11 Regeln zu bereinigen
- Freigaben-Queue
0 Anträge ausstehend

Letzte Audit-Events

Alle anzeigen →

Keine Einträge.

Admin-Dashboard mit kapazitätsbewusstem Menüband nach Arbeitsbereichen.

Kein Kontakt zum Lizenzserver seit 3 Tagen. Noch 2 Tage Grace Period verbleibend. Bitte kontaktieren Sie uns: support@centaurmexus.com

360° Unified Overview

Vollständige Zscaler-Sicht auf einen User – ZDX Telemetrie, ZIA Risiko-Analyse und Policy Audit. ZPA Posture & App-Zugang auf einem Screen.

Suche: Suchen

Alle Bereiche sichtbar Ansicht anpassen

AN **Anon-1d5516**
b5932376of26@anon.centaurmexus.local
Frankfurt/Main - Security Operations

ZIA (WEB & CLOUD)
● **Eingeschränkt**
7 Requests blockiert

ZPA (PRIVATE APPS)
● **Eingeschränkt**
Posture-Check fehlgeschlagen CrowdStrike Falcon Agent

ZDX (DIGITAL EXP.)
● **51** /100
Performance-Probleme

ZDX Endgeräte-Telemetrie & Hardware-Health
Aggregierte Live-Daten via OneAPI Endpoint: /v1/users/devices Host-ID: NB-MUC-VOL2820

GERÄT & OS	SYSTEM-AUSLASTUNG	LOKALES NETZWERK (WI-FI)	ZSCALER EDGE ROUTING
Dell XPS 15 9530 Windows 11 Enterprise (23H2) Zscaler Client Ver. 4.4.1.1	CPU-Last: 51% RAM (32GB): 51%	FRA-Office-Corp 91% Lokale IP: 10.140.33.0 Schnittstelle: Intel Wi-Fi 6 AX201	Fra-Edge-1A (Frankfurt) Tunnel Latenz: 6ms DNS Auflösung: 2ms

ZDX Cloud Path — Hop-für-Hop-Latenz
Netzwerk-Pfad Endgerät → Zscaler Edge → Ziel-App (ZDX Cloud Path Probe)

Hop	Endgerät	GESAMT-LATENZ (RTT)	MAX. PAKETVERLUST
1	Anon-f3bb44 10.148.1.2 - Frankfurt/Main	69 ms	1 ms
2	Anon-ae4101 10.148.1.1 - Frankfurt/Main		5 ms
3	Anon-518a7 de-isp-1.t-ispnet.de - AS3320 - DE-Backbone		19 ms
4	Anon-e1fdcd3 zen-fra-edge.zscaler.net - AS62907 - Fra-Edge-1A (Frankfurt)		16 ms

360°-Suche: ZIA/ZPA/ZDX-Status, ZDX-Telemetrie und Cloud-Path Hop-für-Hop in einer Ansicht.

03 Capability- & Lizenzmodell

Funktionen sind an **Capability-Domänen** (ZIA, ZPA, ZDX, ZCC, ZTW, ZIdentity, ZBI, EASM) und an **Lizenzklassen** gekoppelt: **Light** **Starter** **Advance** **Enterprise** (kumulativ). Ein Tenant mit nur einer Domäne sieht ausschließlich die dafür sinnvollen Funktionen — keine toten Menüpunkte.

04 Use-Case-Katalog

Auszug der zentralen Capabilities — je Funktion, Beschreibung und der konkrete Mehrwert gegenüber der nativen Zscaler-Bedienung. Der vollständige Katalog umfasst über 60 Use Cases.

360°-Suche

Starter

Helpdesk-Vollsicht je User über ZIA/ZPA/ZDX

Eine Suche bündelt Web-Security-Status, private App-Zugänge, Geräte-Telemetrie, Cloud-Path-Latenz und Policy-Audit in einer Ansicht — ohne Zscaler-Admin-Rechte.

Unterschied zu Zscaler nativ: CentaurNexus korreliert die Signale aus ZIA, ZPA und ZDX rollenbasiert in einer Helpdesk-Ansicht — als Cockpit auf der Zscaler-Plattform.

OmniLens (360° v2)

Enterprise

Erweiterte Vollsicht inkl. Identität & Angriffsfläche

Alles aus der 360°-Suche plus ZIdentity-Status, privilegierte Sessions (PRA), externe Angriffsfläche (EASM) und Cloud-Workloads (ZTW).

Unterschied zu Zscaler nativ: Verbindet sechs Zscaler-Produktdomänen zu einem rollenbasierten Persona-Profil.

Deep-Trace on Demand

Advance

Aktive ZDX-Tiefendiagnose

Startet on-demand einen Hop-für-Hop-Trace (WLAN → ISP → Zscaler-Edge → Ziel) und liefert ein Ursachen-Verdikt mit Konfidenz.

Unterschied zu Zscaler nativ: Ergänzt die ZDX-Telemetrie um eine sofort getriggerte, gezielte Tiefendiagnose mit Ursachen-Verdikt.

Ruleset Optimizer

Advance

Ungenutzte & konfliktvolle Regeln finden

Erkennt veraltete (stale) Firewall-/URL-Regeln und Any-Any-Konflikte und schlägt Bereinigungen vor.

Unterschied zu Zscaler nativ: Liefert die Regel-Hygiene-Analytik (stale Regeln, Konflikte) als Cockpit obendrauf auf die Zscaler-Regelwerke.

DLP-Engine-Studio

Advance

DLP-Engines mit Validate-vor-Speichern

Dictionaries, Engines und E-Mail-Templates verwalten; Engine-Ausdrücke werden vor dem Speichern auf Syntax und gegen die Dictionaries validiert.

Unterschied zu Zscaler nativ: Validierung vor dem Deploy; fehlerhafte DLP-Ausdrücke werden vor dem Push nach ZIA abgefangen.

SafePoint / SafePoint+

Advance / Enterprise

Regelsatz-Backup & Restore

Lade → Auswahl → Beschreiben → Sichern: gezielte Snapshots je Domäne; SafePoint+ cross-service (ZIA/ZPA/ZTW/URL), AES-256-GCM verschlüsselt mit Integritäts-Hash.

Unterschied zu Zscaler nativ: Ergänzt die Plattform um ein integriertes, verschlüsseltes Cross-Service-Backup mit Tamper-Evidence beim Restore.

Change-Activation-Orchestrator

Advance

Gebündelte Vier-Augen-Aktivierung

Dienstübergreifende Änderungen sammeln, als Diff prüfen und gebündelt aktivieren (Super-Admin sofort, sonst Vier-Augen).

Unterschied zu Zscaler nativ: Ein orchestrierter, auditierter Sammel-Deploy dienstübergreifender Änderungen — gebündelt statt einzeln.

Compliance-Evidence-Collector

Enterprise

Auditorenfertige Evidence-Packs

Erzeugt aus realen Plattform-Signalen Evidence-Packs für NIS2, DORA und ISO 27001 — einzeln (JSON) oder gebündelt als ZIP.

Unterschied zu Zscaler nativ: Übersetzt technische Zscaler-Signale in auditorenfertige regulatorische Nachweise (NIS2/DORA/ISO).

PRA Onboarding & Approval

Enterprise

Privileged Remote Access mit Saga & Vier-Augen

Provisioniert PRA in einer 7-Schritt-Saga mit automatischer Kompensation bei Fehlern; Zugriffe laufen über Vier-Augen-Freigabe mit Auto-Expiry.

Unterschied zu Zscaler nativ: Ergänzt Zscaler PRA um robuste Provisionierung (kein Halbzustand) und einen geführten Freigabe-Workflow.

AC Zero-Touch / CC-Template

Advance

Connector-Deployment ohne Handarbeit

App-Connector via One-Time-Provisioning-Key (nie geloggt) ausrollen; wiederverwendbare Cloud-Connector-Vorlagen für den Sammel-Deploy.

Unterschied zu Zscaler nativ: Bündelt die manuellen Connector-Schritte zu einem sicheren, auditierten Klick.

Microtenant-Manager

Enterprise

Native ZPA-Mandantentrennung

Ein Tenant verwaltet 1..N Microtenants (z. B. Abteilungen) mit eigenem Isolationsmodus — MSP-fähig vorbereitet.

Unterschied zu Zscaler nativ: Hebt die ZPA-Microtenant-Fähigkeit in eine self-service Mandantenverwaltung.

Audit-Stream & Export

Advance

Asynchroner Audit-Export

Auditorenfähiger Export des Tenant-Audit-Trails (CSV/JSON) — großer Zeitraum läuft asynchron mit Status-Polling, dann Download.

Unterschied zu Zscaler nativ: Tenant-gebundener, RLS-gesicherter Audit-Export, fein an Rollen delegierbar.

IAM Self-Service

Advance

Delegierter ZIdentity-Helpdesk

Passwort-Reset/-Update und temporärer MFA-Skip ohne IdP-Admin-Konsole — jede Aktion auditiert.

Unterschied zu Zscaler nativ: Delegiert eng begrenzte IdP-Aktionen an den Helpdesk, statt Vollzugriff auf die ZIdentity-Konsole zu vergeben.

Vier-Augen-Freigaben

Starter

Helpdesk-Sandbox mit Super-Admin-Freigabe

URL-/App-/Cloud-/DLP-/Travel-Anträge laufen in typisierten Queues; kritische Änderungen erfordern eine zweite Person.

Unterschied zu Zscaler nativ: Bringt ein durchgängiges, typisiertes Freigabe-Modell als Workflow-Schicht auf der Zscaler-Plattform.

ADMIN

Kein Kontakt zum Lizenzserver seit 3 Tagen. Noch 2 Tage Grace Period verbleibend. Bitte kontaktieren Sie uns: support@centaurnexus.com

Omniflex · 360°-Suche v2

Alle Dienste in einer Sicht: die volle 360°-Analyse (ZIA/ZPA/ZDX) plus Identität (ZIdentity), privilegierte Sessions (PRA), externe Angriffsfläche (EASM) und Cloud-Workloads (ZTW).

ada.wong@umbrella-corp.local **Suchen**

AN Anon-bbdef4
11826e0cb065@anon.centaurnexus.local
Remote (DE) · Intelligence

- ZIA (WEB & CLOUD) **Eingeschränkt**
8 Requests blockiert
- ZPA (PRIVATE APPS) **Eingeschränkt**
Posture-Check fehlgeschlagen: Zscaler Client Connector
- ZDX (DIGITAL EXP.) **52** /100
Performance-Probleme

ZDX Endgeräte-Telemetrie & Hardware-Health

Aggregierte Live-Daten via OneAPI Endpoint /v1/users/devices Host-ID: NB-BER-VOL2821

GERÄT & OS	SYSTEM-AUSLASTUNG	LOKALES NETZWERK (WI-FI)	ZSCALER EDGE ROUTING
ThinkPad X1 Carbon Gen 11 Windows 11 Enterprise (23H2) Zscaler Client Ver. 4.3.2.2	CPU-Last 52% RAM (32GB) 52%	BER-Campus-Secure 92% Lokale IP: 10.140.34.0 Schnittstelle: Broadcom BCM94360	Ber-Edge-3C (Berlin) Tunnel Latenz 7ms DNS Auflösung 3ms

ZDX Cloud Path — Hop-für-Hop-Latenz

Netzwerk-Pfad Endgerät → Zscaler Edge → Ziel-App (ZDX Cloud Path Probel)

	GESAMT-LATENZ (RTT)	MAX. PAKETVERLUST
1 Anon-f3bb44 10.140.2.3 · Remote (DE)	74 ms	0%
2 Anon-ae4101 10.140.2.1 · Remote (DE)	1 ms	6 ms
3 Anon-5118a7 de-isp-2.t-ispnet.de · AS3320 · DE-Backbone	20 ms	17 ms
4 Anon-3a13dd zen-ber-edge.zscaler.net · AS62907 · Ber-Edge-3C (Berlin)	17 ms	22 ms
5 Anon-f96adc		

Omniflex (360° v2): volle 360°-Analyse plus ZIdentity, PRA, EASM und Cloud-Workloads.

05 Beispiel: DLP-Studio & Compliance

Zwei Beispiele für den „Validate/Evidence vor Deploy“-Ansatz der Plattform:

DLP-Engine-Studio
Dictionaries, Engines und Templates verwalten. Engine-Ausdrücke werden **vor dem Speichern** gegen die Dictionaries und auf Syntax validiert — fehlerhafte Engines gehen gar nicht erst nach ZIA.

Neue Engine
Ausdruck erst validieren, dann stagen

Engine-Name (z. B. Finanzdaten)

(SSN OR Credit-Card) AND NOT Public

Validieren Speichern

Dictionaries

SSN	pattern	VORDEF.	1
Credit-Card	pattern	VORDEF.	6
IBAN	pattern	VORDEF.	34
PII	phrase		120
Public	exact		8

Engines

- Finanzdaten **AKTIV**
(SSN OR credit-Card OR IBAN) AND ...
- PII-Schutz **AKTIV**
PII AND NOT Public

Templates

- Block-Benachrichtigung email
- Warn-Banner banner

DLP-Engine-Studio: Ausdruck wird vor dem Speichern validiert — fehlerhafte Engines gehen nie nach ZIA.

Compliance-Evidence-Collector
Auditorenfertige Evidence-Packs aus realen Tenant-Signalen — NIS2, DORA und ISO 27001 gemeinsam.

Alle als ZIP

NIS2 JSON

Erfüllungsgrad: 4/4 erfüllt

- Lückenlose Protokollierung (NIS2-AUDIT - 30 Audit-Events) erfüllt
- Zugangskontrolle & MFA (NIS2-ACCESS - MFA-Policy aktiv) erfüllt
- Business Continuity / Backup (NIS2-BCM - 4 Konfig-Backups) erfüllt
- Vier-Augen-Governance (NIS2-GOV - 1 bearbeitete Freigaben) erfüllt

DORA JSON

Erfüllungsgrad: 3/3 erfüllt

- Operationelle Resilienz (Backup) (DORA-RESIL - 4 Wiederherstellungspunkte) erfüllt
- Audit-Trail-Aufbewahrung (DORA-LOG - 30 Audit-Events) erfüllt
- Datenraum-Nachweis (EU) (DORA-REGION - Datenraum: eu) erfüllt

Compliance-Evidence-Collector: NIS2/DORA/ISO 27001 gestapelt, Download einzeln oder als ZIP.

06 Einstellungen & Rollenmodell

Administratoren konfigurieren Rollen, Freigabe-Workflows, ITSM-Anbindung und Datenschutz selbst. Die RBAC-Matrix spiegelt das Menüband wider — Rechte sind nach denselben Arbeitsbereichen gruppiert.

- **RBAC-Matrix:** granulare Rechte je Rolle; Super-Admin behält stets alle Rechte (nicht abwählbar).
- **Time-Travel-Retention, Vier-Augen-Schwellen, Vendor-TTL** je Tenant einstellbar.
- **ITSM-Bridge** (ServiceNow/JSM/Freshservice/Zendesk) mit AES-256-GCM-Secrets.

Kein Kontakt zum Lizenzserver seit 3 Tagen. Noch 2 Tage Grace Period verbleibend. Bitte kontaktieren Sie uns: support@centaurmexus.com

Einstellungen

EINSTELLUNGEN

- Übersicht
- Favoriten
- Rollen & Rechte
- Use Case Policies
- Whitelabeling
- Benachrichtigungen
- Zscaler-Verbindung
- Sicherheit
- ITSM-Anbindung

Rollen-Matrix

Klick auf eine Zelle, um die Berechtigung zu ändern

BERECHTIGUNG	SUPER-ADMIN	MSP-ADMIN	HELPPESK	ANALYST	NEWBEE
SUPPORT					
360° User-Suche	✓	✓	✓	✓	✓
OmniLens	✓	✓	✓	—	—
URL-Diagnose	✓	✓	✓	—	—
VIP Fast-Lane	✓	✓	✓	—	—
RootCause	✓	✓	✓	—	—
Deep-Trace	✓	✓	✓	—	—
IAM Self-Service	✓	✓	✓	—	—
Alle Freigaben	✓	✓	✓	—	—
Freigabe genehmigen	✓	✓	—	—	—
Freigabe ablehnen	✓	✓	—	—	—
ANALYSE					
Ruleset Optimizer	✓	✓	✓	✓	—

RBAC-Matrix nach Arbeitsbereichen — dieselbe Gliederung wie das Navigations-Menüband.

07 Sicherheit & Compliance

- **Mandantentrennung:** PostgreSQL RLS (WITH CHECK) auf jeder Tabelle.
- **Verschlüsselung:** sensible Daten und Backups AES-256-GCM, an den Tenant gebunden.
- **Vier-Augen-Prinzip** für kritische Änderungen (Policy-Deploy, Restore, privilegierte Sessions).
- **Audit-Trail** für jede sicherheitsrelevante Aktion; auditorenfertige Evidence-Packs (NIS2/DORA/ISO).
- **DSGVO-Datenräume** je Mandant: EU ⇒ verpflichtende Log-Anonymisierung.