Zero Trust Application Access (ZTAA)

mit genusphere

Paul Schulz

Agenda

Einleitung

- Vorstellung

Zero Trust

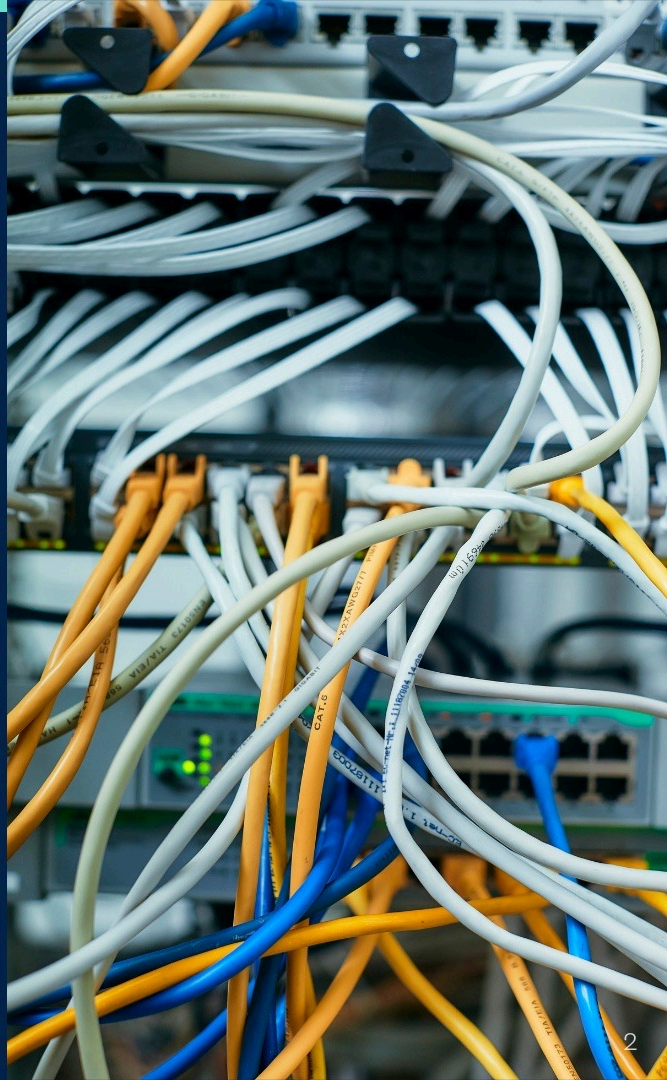
- Zero Trust: Kernprinzipien
- Sicherer Anwendungszugriff

genusphere

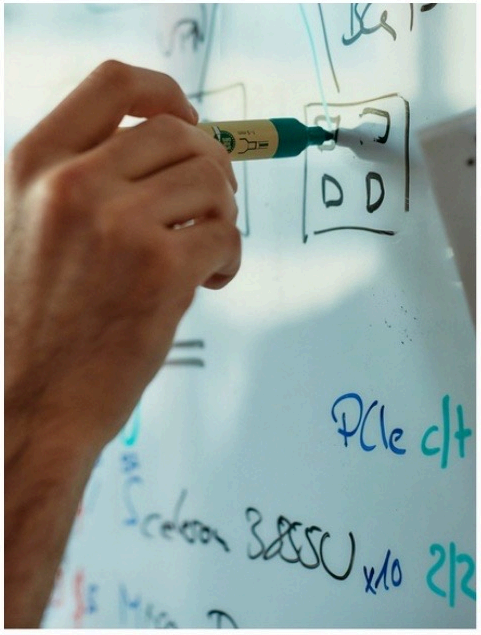
- Vorteile
- Use Cases
- Vergleich Fernzugriff und VPN

Fragen

- Zeit für Fragen mit FAQ



genua.



genua.

Wer sind wir?

genua.

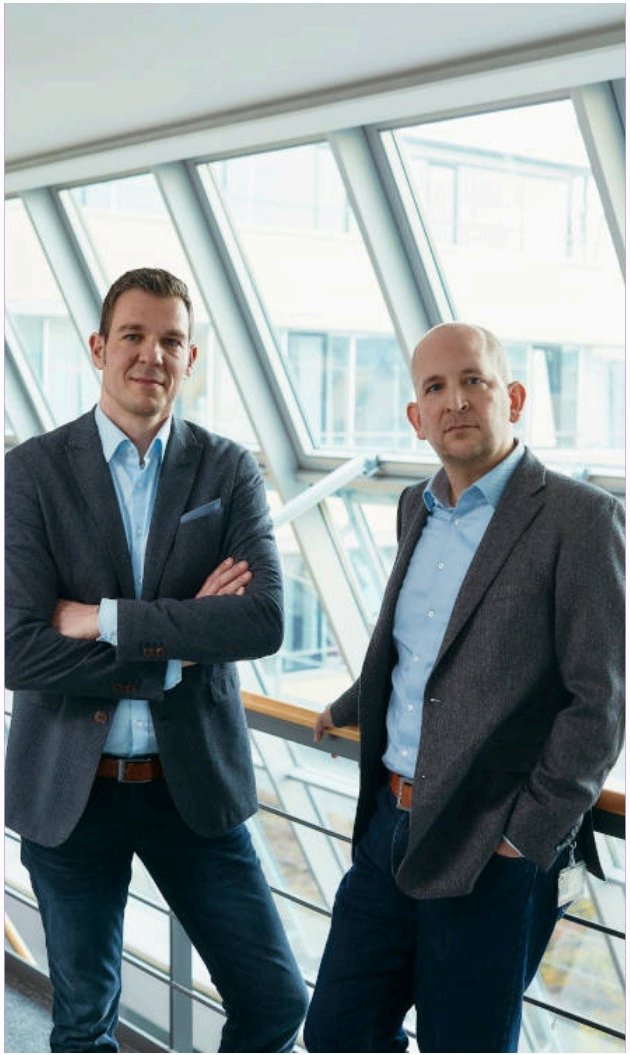
Seit 30 Jahren IT-Sicherheit

– made in Germany

WIR SIND IHR EXPERTE FÜR HOCHWERTIGE IT-SICHERHEIT MIT HAUPTSITZ IN KIRCHHEIM BEI MÜNCHEN, SOWIE STANDORTEN IN BERLIN, KÖLN, LEIPZIG UND STUTTGART.

Teil der Bundesdruckerei-Gruppe

bdr.



- Gegründet 1992
- Hauptsitz in Kirchheim bei München
- Produkte und Lösungen für Netzwerksicherheit
- Entwicklung und Kundenservice unter einem Dach
- Qualitätssicherung durch Zertifizierungen und Zulassungen vom BSI

Zero Trust: Kernprinzipien

Never Trust, Always Verify

- Zero Trust basiert auf dem Prinzip, dass kein Benutzer, Gerät oder keine Anwendung, unabhängig vom Netzwerkstandort, automatisch vertraut wird.
- Jede Zugriffsanfrage erfordert Authentifizierung und Autorisierung.
- Kontinuierliche Überprüfung ist essenziell; Vertrauen ist niemals dauerhaft.

Least Privilege Access

- Benutzer erhalten nur den minimal notwendigen Zugriff für ihre spezifischen Aufgaben.
- Dies begrenzt den Schaden durch kompromittierte Konten, da der Zugriff nur auf notwendige Ressourcen beschränkt ist.
- Ressourcen werden in kleine Einheiten mit fein abgestimmten Berechtigungen aufgeteilt.

Fokus auf Ressourcen

- Die Sicherheit richtet sich auf individuelle Ressourcen (Daten, Anwendungen) statt auf das gesamte Netzwerk.
- Dadurch wird eine Mikro-Perimeter-Sicherheit geschaffen, die engere Sicherheitskontrollen nahe an den Ressourcen ermöglicht.
- Dieser Ansatz unterscheidet sich von traditioneller perimeterbasierter Sicherheit.

Dynamische Richtlinien

- Zugriffsentscheidungen basieren auf Kontext in Echtzeit.
- Faktoren umfassen Benutzeridentität, Gerätegesundheit, Standort, Zeit und Datensensibilität.
- Dieser dynamische Ansatz ermöglicht fein abgestimmte Kontrolle und verhindert unbefugten Zugriff.

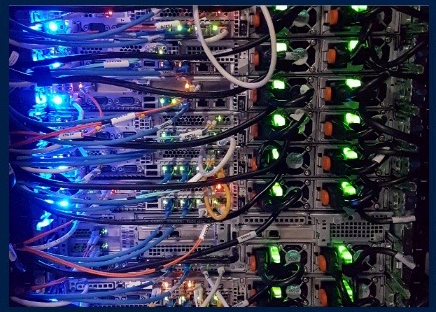
genua.

Sicherer Anwendungszugriff

Direkt-geroutete Architektur

genusphere verfolgt einen "direkt-gerouteten" Ansatz, bei dem eine direkte Verbindung vom Benutzer zu einem Zugriffspunkt innerhalb Ihres Netzwerks hergestellt wird.

Von dort aus wird die Verbindung direkt zu den Konnektoren und Anwendungen weitergeleitet.



On-Premises-Daten- und Steuerungsebene

Die Daten- und Steuerungsebene wird lokal innerhalb des Netzwerks Ihrer Organisation betrieben.

Dieser Ansatz unterscheidet sich von cloudbasierten Lösungen, die oft auf mehrere Zugriffspunkte und Drittanbieter-Infrastrukturen angewiesen sind.

Ein einziger Zugriffspunkt vor Ort

Im Gegensatz zu cloudbasierten Alternativen bietet genusphere einen einzigen On-Premises-Zugriffspunkt, der die Netzwerkarchitektur vereinfacht.

Rendezvous-Verbindungskonzept

genusphere nutzt ein "Rendezvous-Konzept", bei dem Verbindungen aus dem internen Netzwerk initiiert werden.

Der Konnektor stellt eine sichere Verbindung zur genusphere-Datenebene her, anschließend verbindet sich der Benutzer mit derselben Datenebene.

genua.

Sicherer Anwendungszugriff

- **Client-loser Zugriff**

  Benutzer greifen über einen Standard-Webbrowser auf Anwendungen zu, ohne dass ein VPN-Client erforderlich ist.

  genusphere unterstützt HTTP/HTTPS und andere Protokolle direkt im Browser.

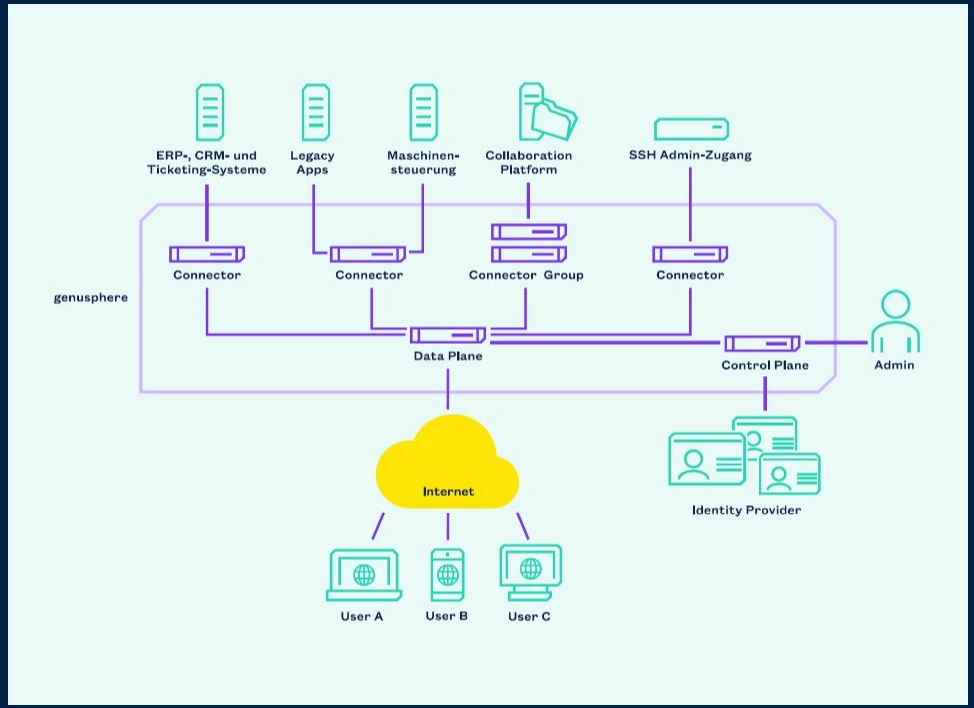
- **Mikro-Perimeter-Sicherheit**

  genusphere bietet fein abgestimmte, identitätsbasierte Zugriffskontrollen und schafft einen Mikro-Perimeter um jede Anwendung.

  Dies stellt sicher, dass Benutzer nur auf die Ressourcen zugreifen, die sie benötigen, und reduziert die Angriffsfläche.

- **Ende-zu-Ende-Verschlüsselung**

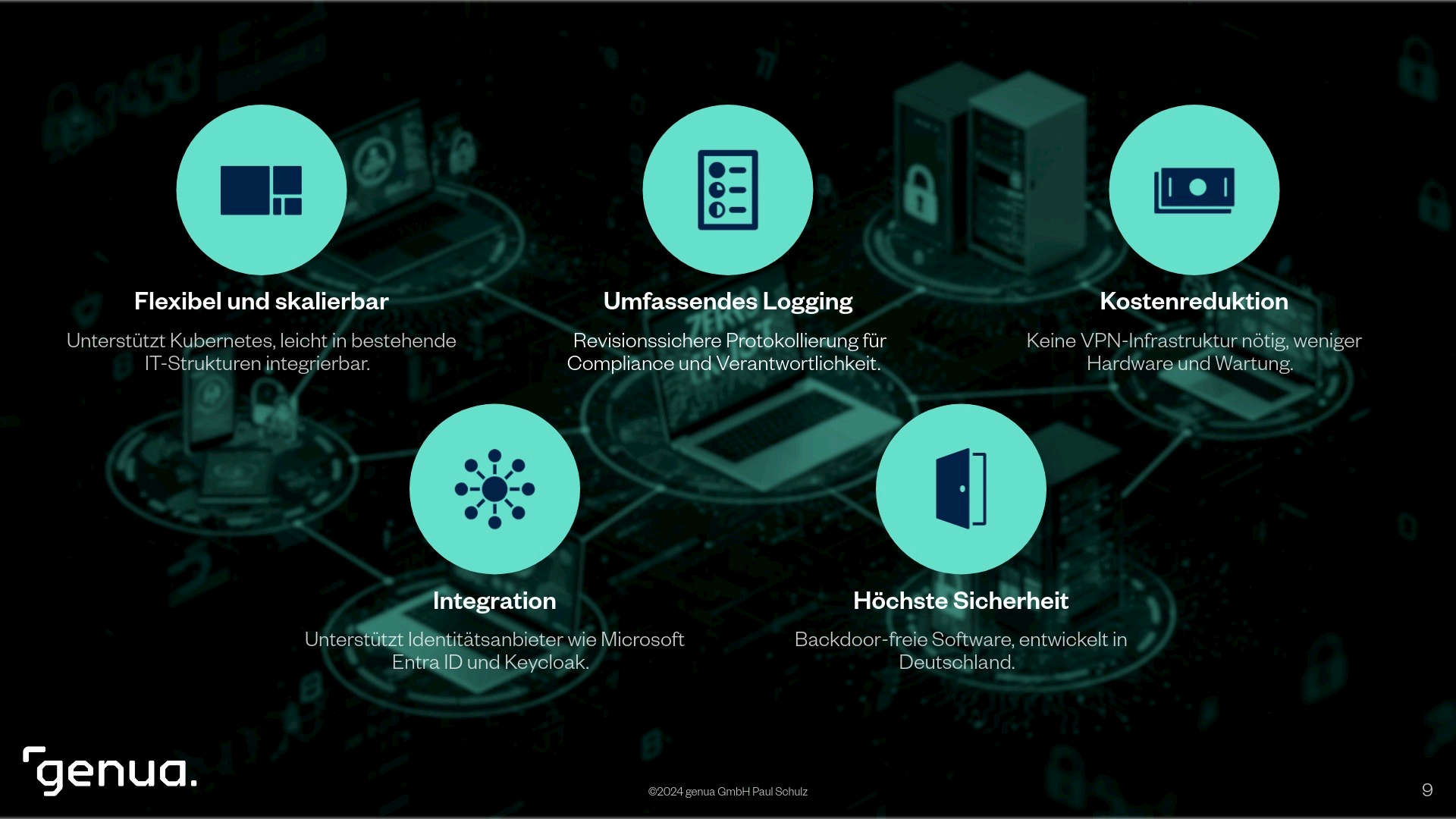
  Der gesamte Datenverkehr wird mit Ende-zu-Ende-Verschlüsselung gesichert, um sensible Informationen während der Übertragung zu schützen.



Vorteile genusphere

- **Zero Trust Security**
  - Minimiert Angriffsfläche durch Zugriffsbeschränkung auf notwendige Anwendungen.
- **Mikro-Perimeter**
  - Identitätsbasierte Kontrolle für gezielten Ressourcenzugriff.
- **Clientloser Zugriff:**
  - Direkter Anwendungszugriff per Browser, ohne VPN.
- **Datenhoheit**
  - Daten und Kontrolle bleiben vollständig On-Premises.
- **Verschlüsselte Kommunikation**
  - Sicherer Datentransfer jederzeit gewährleistet.

genua.



Flexibel und skalierbar

Unterstützt Kubernetes, leicht in bestehende IT-Strukturen integrierbar.

Umfassendes Logging

Revisionssichere Protokollierung für Compliance und Verantwortlichkeit.

Kostenreduktion

Keine VPN-Infrastruktur nötig, weniger Hardware und Wartung.

Integration

Unterstützt Identitätsanbieter wie Microsoft Entra ID und Keycloak.

Höchste Sicherheit

Backdoor-freie Software, entwickelt in Deutschland.

genua.

Vielfältige Anwendungsfälle

Sicherer Fernzugriff

Remote-Mitarbeiter können Anwendungen sicher erreichen, ohne vollen Netzwerkzugriff.

Externe Anbieter erhalten nur Zugriff auf spezifische Aufgaben.

Legacy- und Spezialanwendungen bleiben geschützt zugänglich.

Einfaches Management

Browserbasierter Zugang zu Admin-Schnittstellen (z. B. genua-Produkten).

Granulare Zugriffskontrolle für hohe Sicherheit.

Erweiterte Nutzungsszenarien

Kurzfristiger Zugriff

Temporäre Berechtigungen für externe Partner (z. B. Audits).

Flexible Unterstützung

Einheitlicher Zugang für Legacy- und moderne Anwendungen.

Mobiler Zugriff weltweit über Standardbrowser.

Einfachheit ohne Kompromisse

Kein Client oder VPN nötig.

Zielgruppenorientierte Lösungen

IT-Administratoren

Schneller, sicherer Zugang ohne VPN-Installationen.

CISOs

Verhindert laterale Angriffe durch eingeschränkte Rechte.

Mitarbeiter & Partner

Einfache, granulare Zugriffe – jederzeit und überall.

genusphere vs. genubox

Wesentliche Unterschiede zwischen sicherer Fernwartung und ZTAA

	genusphere	genubox
Positionierung	Zero Trust Application Access (ZTAA), Fokus auf Anwendungssicherheit und einfachen Zugriff.	Speziallösung für (OT-)Fernwartung in industriellen Umgebungen.
Anwendungsfall	Sicherer, browserbasierter Zugriff auf Anwendungen für verschiedene Nutzergruppen.	Sichere Fernwartung mit strikter Zugriffskontrolle.
Zielgruppe	Organisationen mit Bedarf an sicherem, unkompliziertem Fernzugriff.	Organisationen mit hohen Sicherheitsanforderungen, z. B. in kritischen Infrastrukturen.
Zugriff & Verbindung	"Treffpunkt-Konzept": Verbindungen von innen initiiert, Zugriff über Webbrowser.	"Rendezvous-Konzept": Verbindungen explizit intern, Zugriff über Client-App.
Kommunikationsschicht	Layer 7 (HTTP).	Layer 4 (TCP).
Protokolle	HTTP, HTTPS, RDP, VNC, SSH – browserbasiert.	RDP, VNC, SSH (via genuReSI-Client), industrielle Protokolle wie S7.
Mandantentrennung	Keine direkte Mandantenfähigkeit, Trennung über Kubernetes-Namespaces möglich.	Vollständig mandantenfähig, mit physischer Trennung durch dedizierte Appliance

genua.

genusphere vs. genubox

Erweiterte Funktionen und Skalierbarkeit

	genusphere	genubox
Wichtige Funktionen	Fein abgestufte Zugriffskontrolle, Benutzerportal und Dashboard.	Videoaufzeichnung von Zugriffen, Anti-Malware-Funktionen und hochgranulare Fernzugriffskonfiguration mit genuOS und genuSpan-Sensor.
Administration	Standalone-GUI für einfache Verwaltung.	Zentralisierte Verwaltung über genucenter, erfordert höheren Einrichtungsaufwand.
Client	Clientloser, browserbasierter Zugriff.	Erfordert genuReSI Windows-Client für den Zugriff, begrenzter Webzugriff über genuReSI Web.
Skalierbarkeit	Unterstützt Autoscaling über Kubernetes.	Mehrere Boxen ohne dynamisches Load Balancing; Cloud-Management für Lastverteilung bei VMs.
Sicherheit	TLS und mTLS für verschlüsselte Kommunikation.	SSH-Tunnel und starke Authentifizierungsmechanismen.
Primärer Fokus	Anwendungsbezogener Zugriff für moderne Cloud-Infrastrukturen.	Sicherer, netzwerkbezogener Zugriff auf OT- und IT-Infrastrukturen für Fernwartung.

genua.

genusphere vs. genuconnect

Unterschiede zur klassischen IPSec VPN

	genusphere	genuconnect
Architektur	Data Plane, Control Plane, Connectors.	Clientbasiert mit genuscreen als Konzentrator.
Zugriffsziel	Anwendungen (Apps).	Netzwerk via VPN.
Systemanforderungen	Browser (Chrome, Edge).	Windows 10/11, genuscreen.
Verbindungstyp	„Treffpunkt-Konzept“, über Data Plane.	IPsec-VPN zum Konzentrator.
Zugriffsmethode	Clientlos, HTTP/S, WebSockets.	Clientbasiert, IPsec-Software-Client.
Kommunikationsschicht	Layer 7 (HTTP).	Layer 3 (IPsec), Layer 4 (UDP).
Netzwerk	Internet.	VPN über Router/Firewalls.
Regulation	Keine VS-NfD-Zulassung.	IPsec für bestimmte Szenarien zugelassen.

genua.

genusphere vs. genuconnect

Unterschiede zur klassischen IPSec VPN

	genusphere	genuconnect
Unterstützte Protokolle	HTTP, HTTPS, RDP, VNC, SSH über Browser.	Alle IP-basierten Protokolle.
Autorisierung & Richtlinien	Feingranulare Regeln (Gruppe, Zeit, Ort).	Zugriffssteuerung über VPN & Konzentrator.
Administration	Standalone GUI.	genucenter & Windows-Tools.
Management	Zentrales Admin-Portal.	genucenter für Konzentrator.
Skalierbarkeit	Autoscaling via Kubernetes.	Keine dynamische Lastverteilung.
Sicherheit	TLS & mTLS für Kommunikation.	IPsec-Tunnel, Protokollabhängige Sicherheit.
Authentifizierung	OpenID Connect (z. B. Azure AD).	Zertifikate, Passwort, OTP.
Datenschutz	Verschlüsselte Verbindungen, nur für Kunden lesbar.	Unverschlüsselte Daten hinter VPN.
Plattform	K3S, Redhat OpenShift, Docker.	genuOS (OpenBSD) auf Intel-Hardware.

genua.

FAQ

Was ist Zero Trust?
„Vertraue niemandem, überprüfe alles.“ Keine Nutzer oder Geräte werden von Natur aus vertraut.

Warum ist Zero Trust notwendig?
Klassische Sicherheitsmodelle reichen nicht aus, um moderne Bedrohungen und Cloud-Umgebungen abzusichern.

Was sind die Ziele von Zero Trust?
Schutz der Datenintegrität, Einschränkung der Angreiferbewegung im Netzwerk.

Was unterscheidet Zero Trust von klassischen Ansätzen?
Kein vertrauenswürdiger Netzwerkbereich, jede Zugriffsanfrage wird geprüft.

Was sind die Kernkomponenten?
Policy Decision Point (PDP) und Policy Enforcement Point (PEP).

Was macht genusphere?
Bietet sicheren Zugriff auf Apps, ohne das gesamte Netzwerk freizugeben.

Wie setzt genusphere Zero Trust um?
Identitätsbasierte Regeln und Zugriff über den Browser, keine Clients nötig.

Welche Vorteile hat genusphere?
Micro-Perimeter-Sicherheit, hohe Skalierbarkeit, Integration mit Entra ID und Keycloak.

Welche Protokolle werden unterstützt?
HTTP, HTTPS, RDP, VNC, SSH.

Wie wird Sicherheit gewährleistet?
Verschlüsselte Verbindungen mit TLS und mTLS.

Zero-Trust-Einführung

Welche Schritte sind nötig?
Prozesse analysieren, beteiligte Parteien und Ressourcen identifizieren.

Welche Herausforderungen gibt es?
Komplexität, fehlende Standards, Bedarf an kontinuierlicher Überwachung.

Wie können diese gelöst werden?
Strukturiertes Vorgehen, Priorisierung und Infrastruktur-Analyse.