



20. Mai 2026

**17. Bechtle
IT-Forum
Thüringen**

Steigerwald Stadion Erfurt

**20
26**

Einfaches mobiles Arbeiten mit Staatsgeheimnissen

2026-05-20: bechtle IT-Forum – Arnold Krille (genua GmbH)



01

Verschlusssachen und andere Staatsgeheimnisse

VSA §2 Abs. 1: Was sind Verschlusssachen?



Verschlusssachen sind im öffentlichen Interesse, insbesondere **zum Schutz des Wohles des Bundes oder eines Landes**, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform [...].

Geheimhaltungsbedürftig im öffentlichen Interesse können auch Geschäfts-, Betriebs-, Erfindungs-, Steuer- oder sonstige private Geheimnisse oder Umstände des persönlichen Lebensbereichs sein.

VSA §2 Abs. 3: Warum geheim halten?

STRENG GEHEIM

wenn die Kenntnisnahme durch Unbefugte **den Bestand oder lebenswichtige Interessen** der Bundesrepublik Deutschland oder eines ihrer Länder **gefährden kann**

GEHEIM

wenn die Kenntnisnahme durch Unbefugte **die Sicherheit** der Bundesrepublik Deutschland oder eines ihrer Länder **gefährden oder ihren Interessen schweren Schaden zufügen kann**

VS-Vertraulich

wenn die Kenntnisnahme durch Unbefugte **für die Interessen** der Bundesrepublik Deutschland oder eines ihrer Länder **schädlich sein kann**

VS-nur für den Dienstgebrauch (VS-NfD)

wenn die Kenntnisnahme durch Unbefugte **für die Interessen** der Bundesrepublik Deutschland oder eines ihrer Länder **nachteilig sein kann**

VS bearbeiten in der Praxis?

- Mobil?
- Bequem?
- Digital?
- Sicher?

BSI sagt: ja. ;-)



02

Wie arbeitet man sicher Mobil?

Mobiles Arbeiten

Wer unterwegs mit vertraulichen Informationen arbeitet, muss sich auf den zuverlässigen Schutz von Mobilgeräten und Daten verlassen können.



genua bietet ein umfassendes Portfolio von Remote-Working-Produkten, die zu individuellen Lösungen kombiniert werden können.

Ihre Vorteile

- Vertrauenswürdiges VPN-Ökosystem made in Germany
- Höchste Sicherheitsstandards, für den öffentlichen Sektor, geheimhaltungsbetonte Organisationen und Unternehmen
- Zulassung bis VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED

03

Lösungs-Bundle für den VS-NfD- konformen Arbeitsplatz genusecure Suite

Lösungs-Bundle für den VS-NfD-konformen Arbeitsplatz genusecure Suite

Lösungs-Bundle

Lösungsprofil

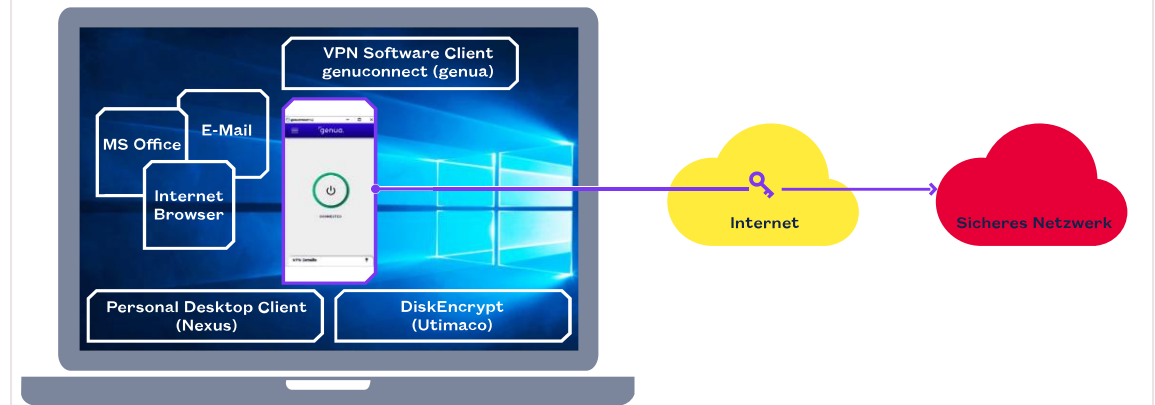
- All-in-One Security: genusecure Suite ist ausgelegt auf alle Organisationen mit VS-NfD-Bedarf
- Schützt Verbindungen, Anwendungen und Daten von mobilen Devices mit Windows 11
- Teil eines vollständigen VPN-Ökosystems für höchste Sicherheit

Ihre Vorteile

- Einfach & komfortabel: Anwender arbeiten über gewohnte Windows-Oberfläche ohne zusätzliche Layer
- Zukunftssicher & mobil: Die vollständig softwarebasierte Suite bietet Rundum-Security für New-Work-Konzepte
- VPN Software Client und Festplattenverschlüsselung sind für VS-NfD, NATO RESTRICTED und RESTREINT UE/ EU RESTRICTED zugelassen

genusecure Suite umfasst

- Den VPN Software Client genuconnect,
- die Festplattenverschlüsselung Utimaco DiskEncrypt und
- die Smartcard Middleware Nexus Personal Desktop Client



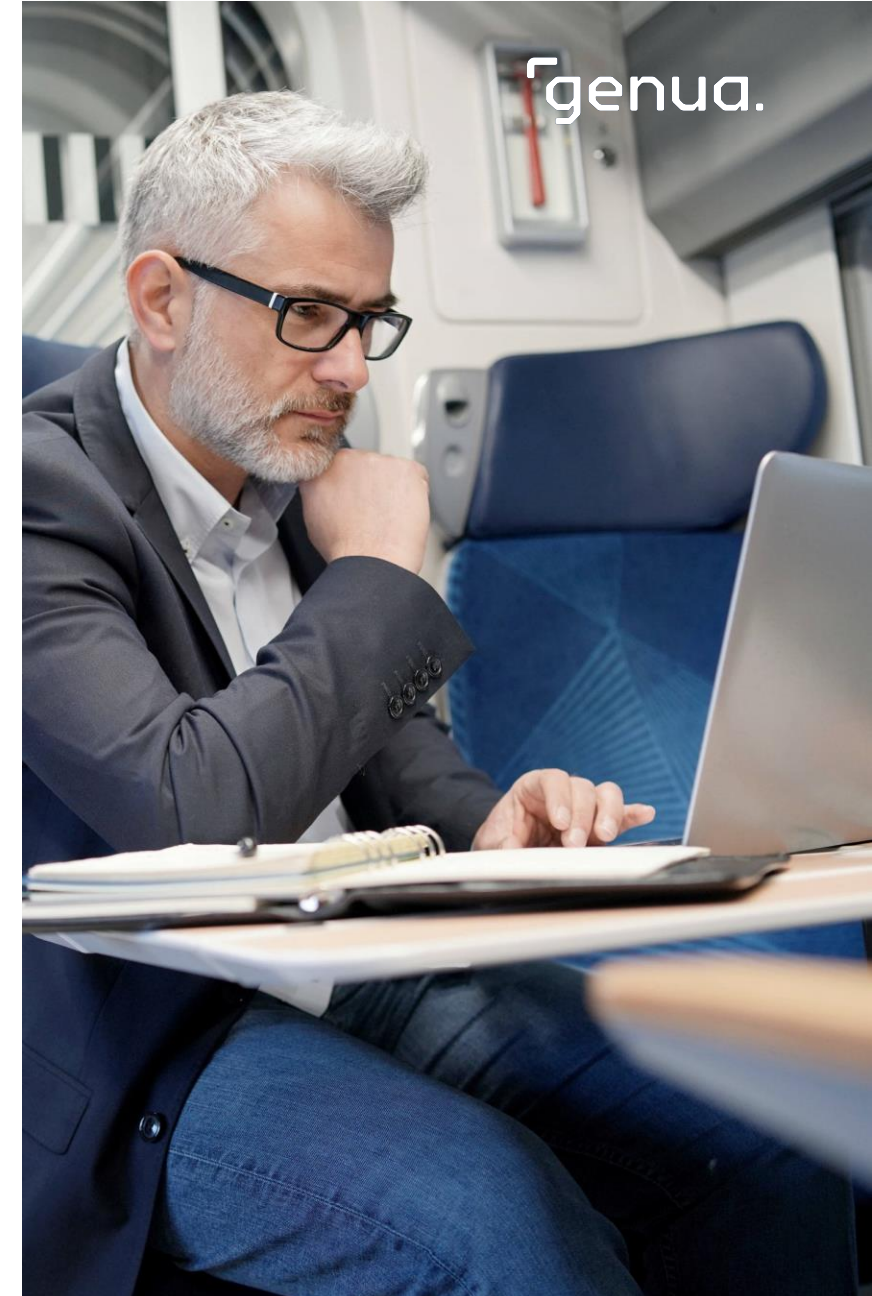
Lösungs-Bundle für den VS-NfD-konformen Arbeitsplatz genusecure Suite

Wesentliche Anwendungen

- Sichere, reibungslose Telearbeit bei voller Performance von hochentwickelten IT Tools
- Einrichtung New-Work-konformer VS-NfD-Arbeitsplätze

Typische Einsatzbereiche

genusecure Suite ermöglicht Organisationen mit VS-NfD-Bedarf, unabhängig von Ort und Zeit einen idealen Arbeitsplatz bereitzustellen, bei dem State-of-the-Art-Technologien Arbeitsabläufe vereinfachen und absichern sowie das Risiko von Datenverlusten auf allen Endgeräten minimieren.



04

VPN Software Client genuconnect

✓ Zugelassen

VPN Software Client genuconnect

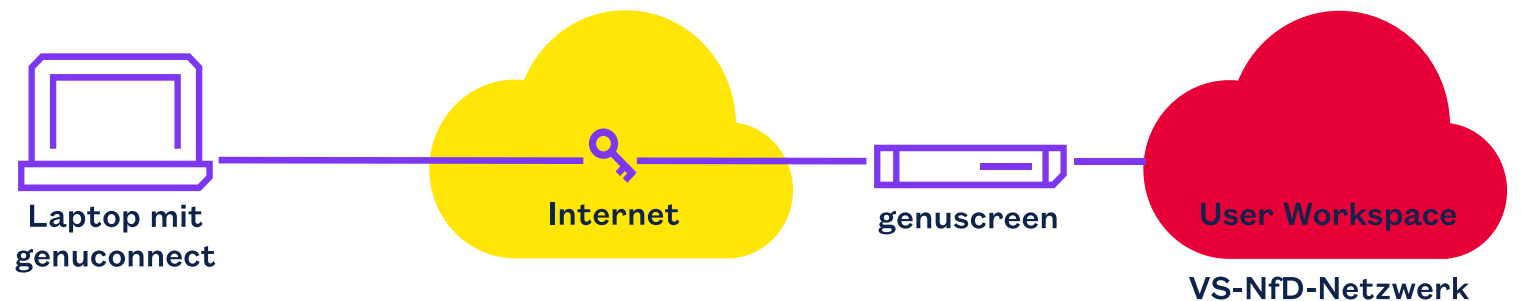
Lösungsprofil

- VPN Software Client für sicheren Zugriff auf eingestufte Daten
- Leistungsfähig, flexibel und skalierbar für Infrastrukturen mit mehr als 100.000 VPN-Clients
- Komplette Integration in Microsoft Windows

Ihre Vorteile

- Sichere VPN-Technologie made in Germany für Datenkommunikation über nicht vertrauenswürdige Netze
- Die verpflichtende Verwendung von Smartcards sorgt dabei für zusätzliche Sicherheit
- Zugelassen für VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED

Hochsichere Anbindung von Windows Devices mit dem VPN Software Client genuconnect



VPN Software Client genuconnect

Wesentliche Anwendungen

- Schutz sensibler Daten bei der Kommunikation aus dem Home Office oder von unterwegs
- Einrichtung New-Work-konformer VS-NfD-Arbeitsplätze

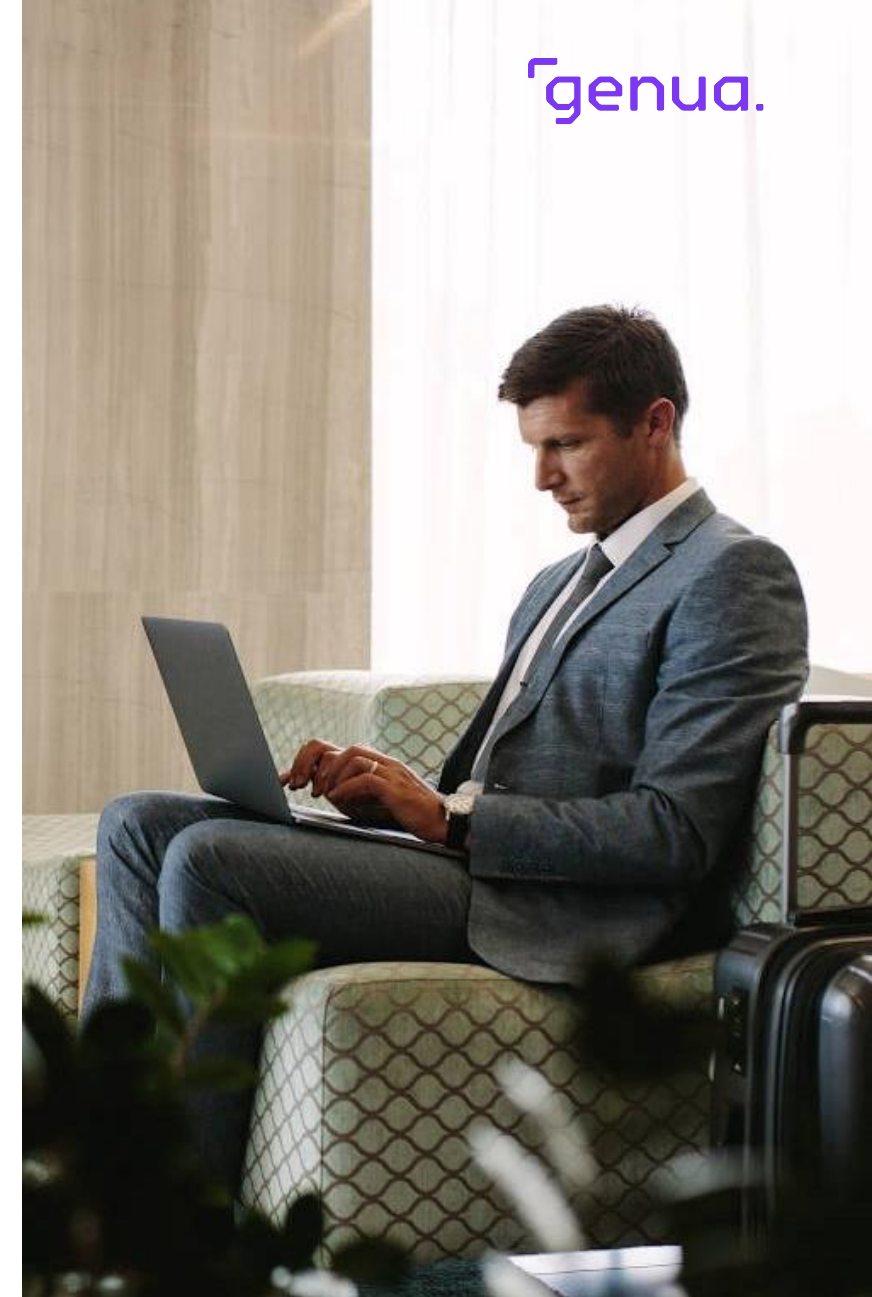
Typische Einsatzbereiche

Der VPN Software Client genuconnect sorgt beim Einsatz von Laptops und Tablets mit Microsoft Windows 10 oder 11 in

- staatlichen Organisationen und
- geheimschutzbetreuten Unternehmen

für höchste Sicherheit und Funktionalität. Die Lösung zeichnet sich durch geringe Komplexität, hohe Skalierbarkeit und überzeugende Benutzerfreundlichkeit aus.

 genua.de/genuconnect



05

Firewall & VPN-Appliance genuscreen

✔ Zertifiziert

✔ Zugelassen

Firewall & VPN-Appliance genuscreen

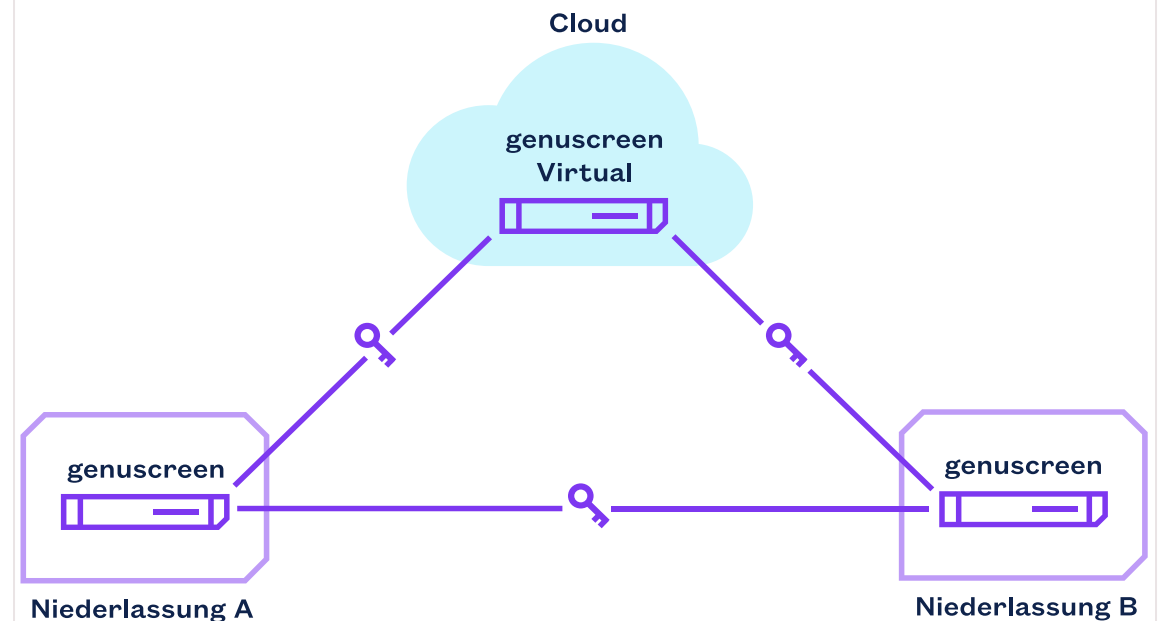
Lösungsprofil

- “2-in-1-Lösung”: Hochsichere Firewall und VPN-Appliance
- VPN-Komponente für stark verschlüsselte Virtual Private Networks (VPN) ermöglicht Datenkommunikation über öffentliche Netze
- Firewall-Komponente filtert Datenverkehr an Schnittstellen (z. B. Perimeter, interne Sicherheitszonen) und erlaubt nur ausdrücklich erwünschte Verbindungen

Ihre Vorteile

- Die VPN-Komponente inkl. quantenresistentem Schlüsselaustausch für IPsec/IKEv2 sowie die Firewall-Komponente sind zugelassen für VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED
- Zertifiziert nach Common Criteria (CC) EAL 4+
- Hochsicheres VPN in der VM: genuscreen Virtual für Einsatz auf Hypervisoren – mit BSI-Zulassung

Sicherer Transfer vertraulicher Daten zwischen verschiedenen Standorten und einer Cloud



Firewall & VPN-Appliance genuscreen

Wesentliche Anwendungen

- Bewährte Einwahlösung im Hochsicherheitsbereich durch VS-NfD-Zulassung
- Bridging Firewall zur Einrichtung von Schutz-zonen für besonders sensible Systeme, wie z. B. Server von R&D- oder HR-Abteilungen, innerhalb bestehender IT-Infrastrukturen

Typische Einsatzbereiche

- Die Firewall & VPN-Appliance genuscreen ermöglicht z. B.
- Bundes- und Landesbehörden,
 - Bundeswehr-Einheiten und
 - geheimschutzbetreuten Unternehmen
- einen sicheren Austausch von VS-NfD-Informationen. Die Zulassung umfasst gemäß der Verschlusssachenanweisung (VSA) neben der VPN- auch die Firewall-Komponente.

 genua.de/genuscreen



06

Warum genua?

Das Portfolio von genua

Lösungen von genua werden seit über 30 Jahren in Deutschland nach anerkannten Sicherheitsstandards hergestellt.



Mit eigener Forschung und Entwicklung unter einem Dach verfolgen wir konsequent das Security-by-Design-Prinzip, sichern sensible IT-Infrastrukturen und fördern so die digitale Souveränität Europas.

Ihre Vorteile

- IT Security made in Germany mit BSI-Zulassung für höchste Sicherheit
- Für Behörden, Geheimschutz, KRITIS und Industrie
- Bedarfsgerecht erhältlich als Software, Appliance oder virtualisierte Lösung
- Flexibles, kundennahes Service-Angebot



Trust Seal
www.teletrust.de/itsmig

made
in
Germany

Das Portfolio von genua

Unter dem Leitmotiv **"Excellence in Digital Security"** stellen wir ein integriertes Lösungsportfolio nach höchsten Sicherheits- und Qualitätsstandards zur Verfügung, das alle relevanten Segmente der IT-Sicherheit abdeckt.

Unser Qualitätsversprechen





Wir schaffen Vertrauen.

- ✔ **Vertrauen durch Sicherheit.**
Für die digitale Gesellschaft.
- ✔ **Dank Misstrauen aus Berufung.**
Unsere Skepsis für Ihre Sicherheit.



Eine starke Familie



- genua ist eine hundertprozentige Tochter der **Bundesdruckerei-Gruppe GmbH**.
- Als **Technologieunternehmen** des Bundes schafft die Bundesdruckerei-Gruppe **Vertrauen** in der Gesellschaft.
- Mit **Identifikationssystemen, Cybersicherheit und Digitalisierungslösungen** legen wir gemeinsam die Grundlage für eine moderne und resiliente Gesellschaft.
- Gemeinsam leisten wir einen relevanten Beitrag für die **digitale Souveränität** Deutschlands und Europas.



Made in Germany – für digitale Souveränität

Wir ermöglichen es **Behörden**, der **geheimhaltungsbetreuten Industrie** und **KRITIS-Unternehmen** von den Vorteilen der Digitalisierung zu profitieren und gleichzeitig ihr Know-how sowie ihre Daten zu schützen.

- Digitale Sicherheit – seit 1992
- Deutscher Hersteller und Dienstleister mit Hauptsitz in Kirchheim und 4 weiteren Standorten
- Höchste Standards – Zertifizierungen und Zulassungen durch das BSI
- Entwicklung und Kundenservice unter einem Dach
- Unternehmen der Bundesdruckerei-Gruppe




Forschung und Innovation: Zur Sicherung des Erfolgs

Wir kooperieren mit führenden Forschungseinrichtungen, Hochschulen und Unternehmen, verknüpfen unterschiedliche Kompetenzen und machen die daraus entstehenden Innovationen unseren Kunden zugänglich.



Aktuelle Themenfelder

-  Zero Trust, Cloud, Virtual Network Functions
-  Künstliche Intelligenz
-  Post-Quanten-Kryptografie



Forschungsprojekte – ein Auszug

| | | |
|-----------------------|---|-----------|
| SGLB | Secure Smart Grid Load Balancer | 2013-2016 |
| INDI | Intelligente Intrusion-Detection-Systeme für Industrienetze | 2014-2018 |
| SarDiNe | Netzsicherheit in Unternehmen und Behörden basierend auf Software Defined Networking | 2015-2018 |
| SENDATE | SEcure Networking for a DATa Center Cloud in Europe | 2016-2019 |
| QuaSiModO | Quantenresistente Verschlüsselungs- und Schlüsselaustauschverfahren für IPsec/IKEv2 | 2019-2023 |
| WINTERMUTE | KI-gestützte Lagebeurteilung, Policy Definition und Durchsetzung von Sicherheit in komplexen Netzen | 2020-2023 |
| AI-NET-PROTECT | Unterstützung agiler Geschäftsprozesse und Compliance-orientierter Zugriffskontrolle | 2021-2024 |
| VerSeCloud | Entwicklung einer formal verifizierten Virtualisierung für sicherheitskritische Anwendungen | 2021-2024 |
| AmiQuaSy | Praxisnahe Konzepte zur Migration auf Post-Quanten-Kryptografie in heterogenen Netzen | 2023-2026 |
| QUDIS | Post-Quanten-Kryptografie & Kryptoagilität in der digitalen Infrastruktur des Schienenverkehrs | 2024-2027 |

Stand: Juli 2024

Auswahl unserer Forschungsprojekte – kein Anspruch auf Vollständigkeit

Mit Sicherheit starke Partner

Wir arbeiten seit vielen Jahren vertrauensvoll und erfolgreich mit Vertriebs- und Kooperationspartnern aus **unterschiedlichen Branchen und Marktsegmenten** zusammen

- **Starkes Partnernetzwerk** in DACH für ein flächendeckendes Beratungs-, Service- und Support-Angebot
- Mit einem **umfassenden Partnerprogramm** sowie **exklusiven Partnerangeboten** investieren wir in die Zusammenarbeit und Kooperation mit exzellent ausgebildeten und gut vernetzten Partnern
- Gemeinsam erkennen wir Trends am Markt und lassen so **neue Angebote für unsere gemeinsamen Kunden entstehen**

➤ **Kooperation ist der entscheidende Faktor für den Erfolg digitaler Geschäftsmodelle.**



Diese Kunden vertrauen uns. Und noch mehr.

Öffentlicher Bereich

Behörden und Organisationen mit Sicherheitsaufgaben

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bundesministerium für Arbeit und Soziales

Bundeswehr

Deutscher Bundestag

Informationsverbund Berlin-Bonn (IVBB)

Landeshauptstadt München

Statistisches Bundesamt

THW



Privatwirtschaftlicher Bereich

BMW

ESG Elektroniksysteme und Logistik

EUROGATE

KASTO Maschinenbau

Klüber Lubrication

MAN

MTU Aero Engines

Hitachi Energy

Stuttgarter Lebensversicherung

WMF

Bosch



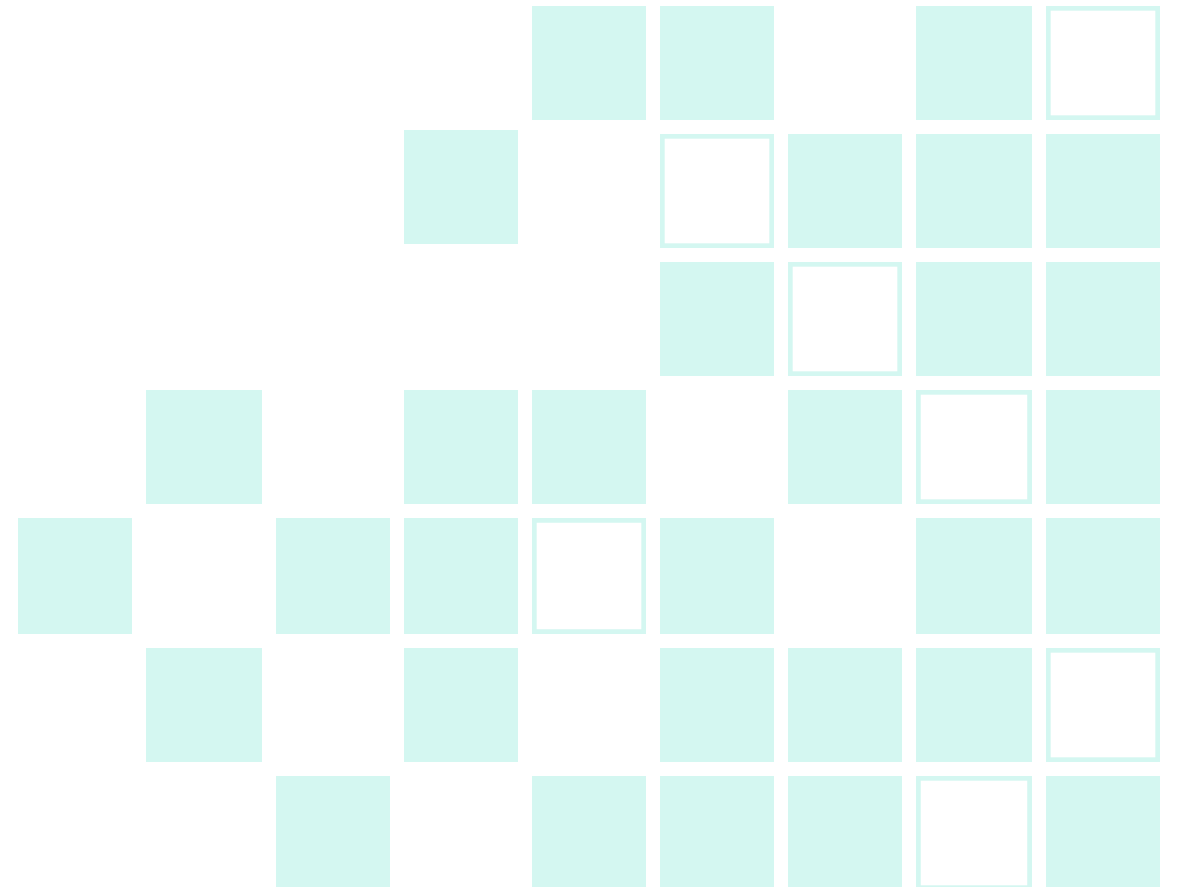


Fragen und Anmerkungen
sind herzlich willkommen.

Zögern Sie nicht, uns anzusprechen

Excellence in Digital Security

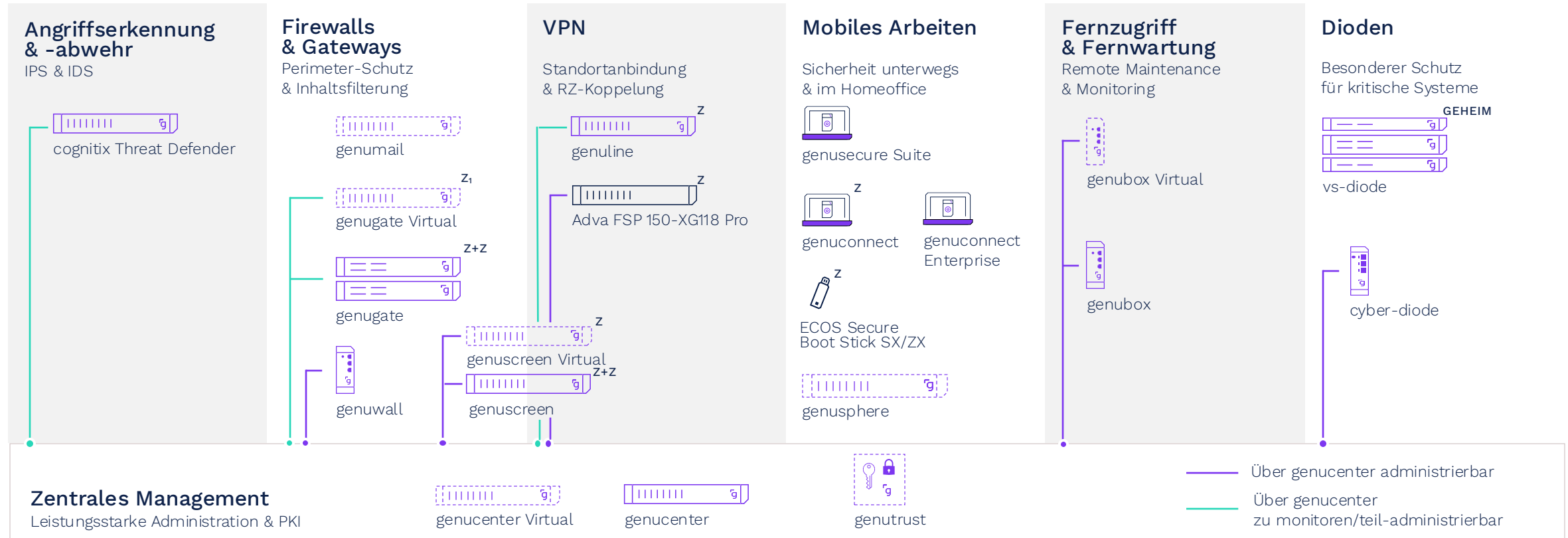
genua GmbH
Domagkstraße 7
85551 Kirchheim bei München
+49 89 991950-0
info@genua.de
www.genua.de



A

Anhang

Das genua Portfolio



+ — **Services** — **Trainings** — **Consulting** —

Updates/Hotline/
Auftragsentwicklung

IT Security Know-how
für Kunden & Partner

Beratungsangebot für
IT-Sicherheit & Compliance

Z BSI-Zulassung (VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED) Z₁ BSI-Zulassung VS-NfD Z+Z BSI-Zulassung (VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED) und Zertifizierung
GEHEIM BSI-Zulassung (GEHEIM, NATO SECRET und SECRET UE/EU SECRET)

A1

Firewalls & Gateways

Sichere Netzwerkgrenzen

Firewalls sind ein wichtiger Teil der Sicherheitsarchitektur. Sie verhindern, dass bösartiger Datenverkehr diese Grenze überschreitet.



genua bietet verschiedene spezialisierte Firewalls, darunter Systeme mit BSI-Zulassung und Zertifizierung nach Common Criteria (CC).

Ihre Vorteile

- Vertrauenswürdige Lösungen made in Germany – ohne Backdoors
- Minimierung von Angriffsflächen durch Security-by-Design-Ansatz
- Sichere Lösungen für den öffentlichen Sektor, geheimhaltungsbetonte Unternehmen, kritische Infrastrukturen und Industrie
- Zulassung bis VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED

A2

High Resistance Firewall genugate

✔ Zertifiziert

✔ Zugelassen

High Resistance Firewall genugate

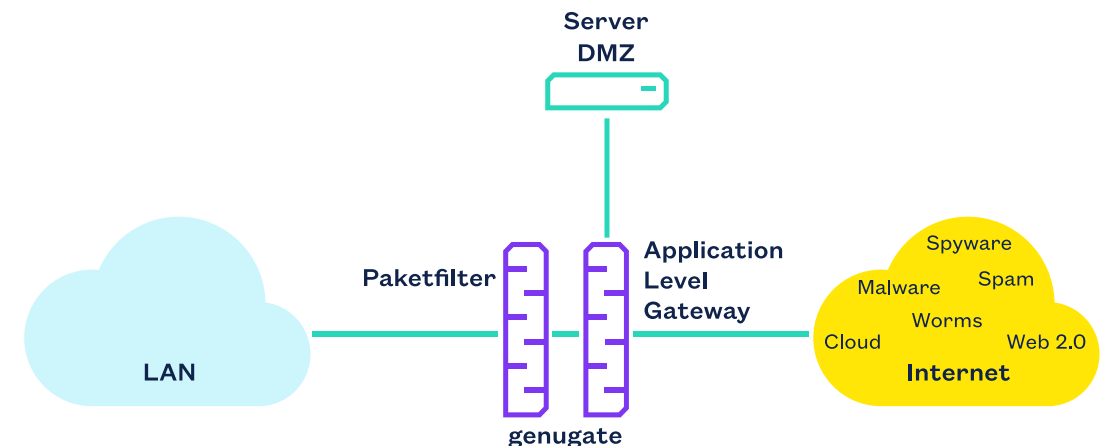
Lösungsprofil

- Zweistufige Firewall: Zwei Komponenten in zwei unabhängigen Rechnern
- Paketfilter (PFL) innen, mit individuell konfigurierbarem Regelwerk
- Application Level Gateway (ALG) außen, für gesamtheitliche, vollständige Inhaltsanalyse

Ihre Vorteile

- Bester Selbstschutz: Einzige vom BSI als „highly resistant“ eingestufte Firewall der Welt
- Zertifiziert nach Common Criteria (CC) EAL4+ mit AVA_VAN.5 (Advanced Methodical Vulnerability Analysis)
- Zugelassen für VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED

Hochsichere Schnittstellen durch
zweistufige Firewall genugate



High Resistance Firewall genugate

Wesentliche Anwendungen

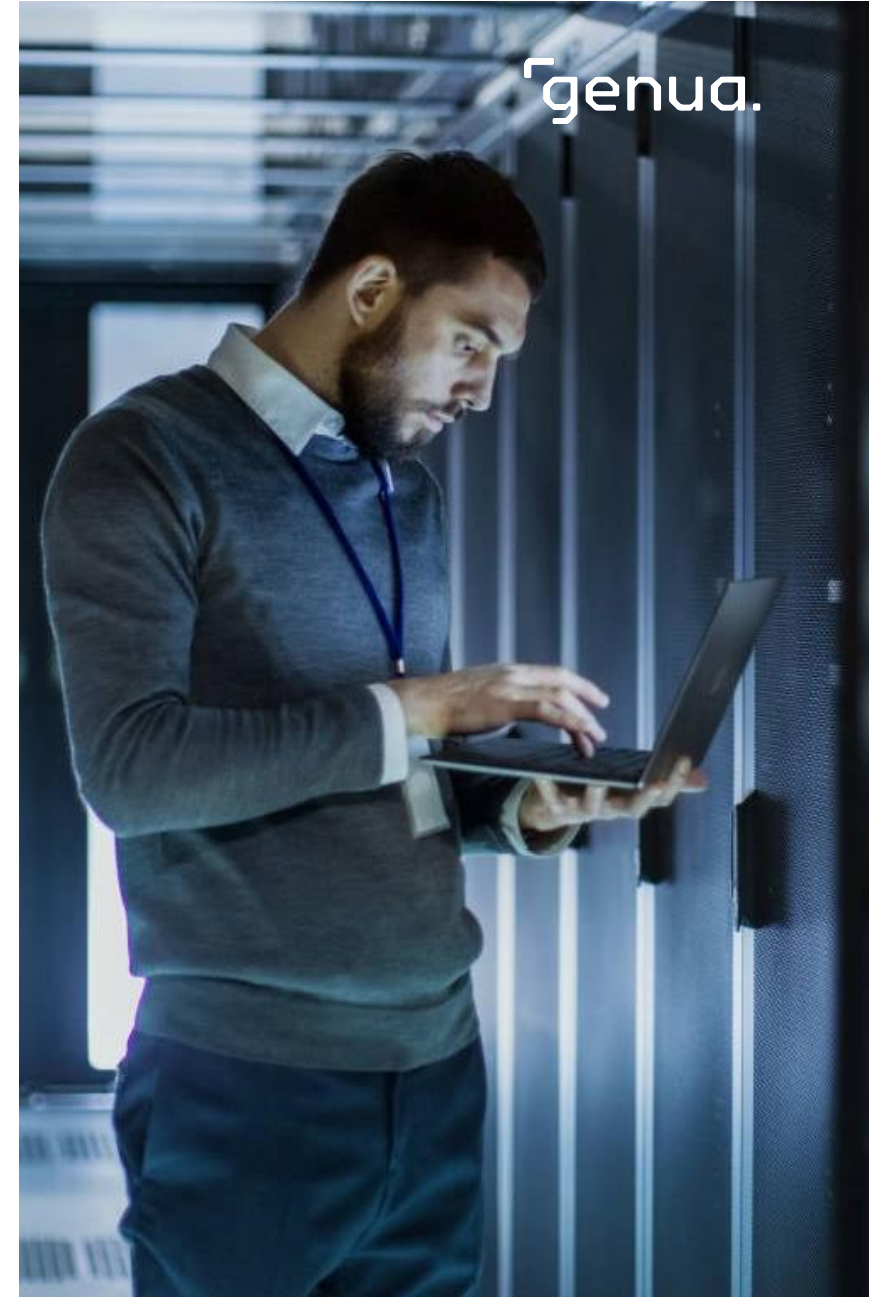
- Einsatz an der Netzwerkgrenze als hochsicheres, zweistufiges Firewall-System
- Einsatz als P-A-P-Lösung, ergänzt um einen weiteren Paketfilter nach Anforderungen gemäß VSA und IT-Grundschutz

Typische Einsatzbereiche

genugate ermöglicht es

- Bundesbehörden,
- bundesunmittelbare öffentlich-rechtliche Einrichtungen,
- Landesbehörden und
- Organisationen mit Zugang zu eingestuften Informationen, ihre Netze gemäß den einschlägigen gesetzlichen Vorgaben abzusichern.

 genua.de/genugate



A3

High Resistance Firewall genugate Virtual

✓ Zugelassen

High Resistance Firewall genugate Virtual

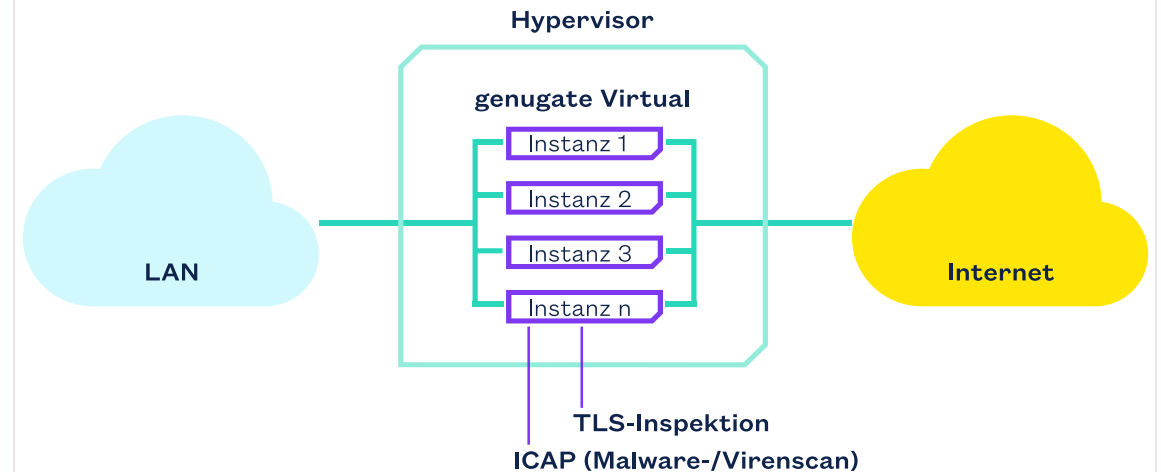
Lösungsprofil

- Das einzige virtuelle Application Level Gateway mit BSI-Zulassung und Zertifizierung nach Common Criteria (CC)
- Hohes Sicherheitsniveau durch umfassende Inhaltsanalyse
- Integrierte Web Application Firewall (WAF)

Ihre Vorteile

- Zugelassen für die Geheimhaltungsstufe VS-NfD
- Zertifiziert nach Common Criteria (CC) EAL4+ mit AVA_VAN.5 (Advanced Methodical Vulnerability Analysis)
- Proxy-Dienste für diverse Protokolle (WWW, SMTP, SOAP, SSH, IMAP, usw.)
- Hohe Skalierbarkeit und Automatisierbarkeit

genugate Virtual bietet skalierbare Netzwerksicherheit für sensible Infrastrukturen



High Resistance Firewall genugate Virtual

Wesentliche Anwendungen

- Flexibler Einsatz zur Absicherung von Cloud- und Virtualisierungsumgebungen
- Skalierbarkeit für schnelle und effiziente Anpassung an wachsende Netzwerkkumgebungen

Typische Einsatzbereiche

genugate Virtual bietet umfassenden Schutz für Anwendungsfälle wie

- den sicheren Zugriff auf Cloud-Dienste,
- die Absicherung von Datenübertragungen und
- die Abwehr von unautorisierten Zugriffen

im öffentlichen Sektor, geheimschutzbetreuten Unternehmen und kritischen Infrastrukturen.

 genua.de/genugate-virtual



A4

High-Speed VPN Appliance genuline

✓ Zugelassen

High-Speed VPN Appliance genuine

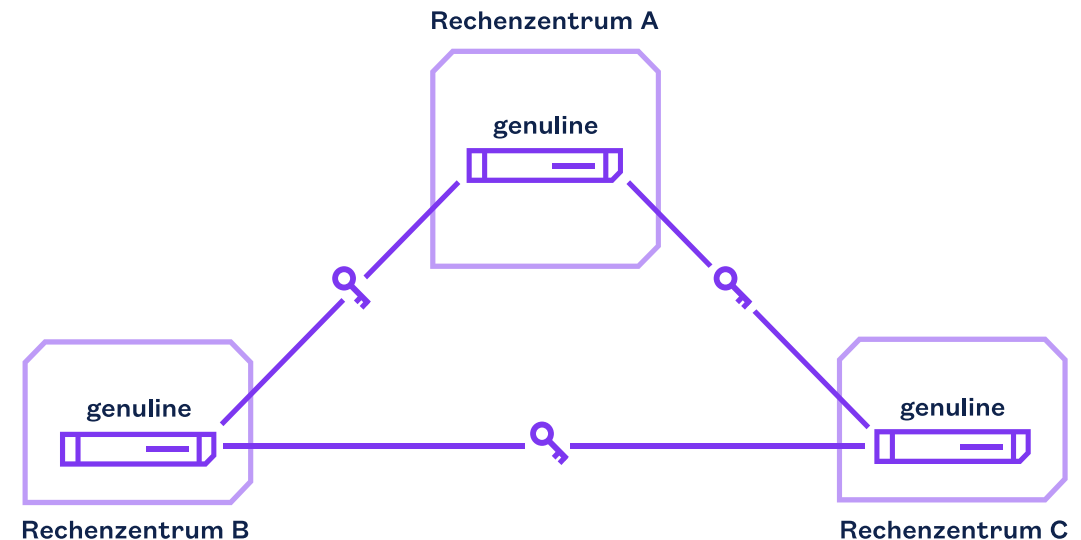
Lösungsprofil

- VPN-Gateway für verschlüsselte und besonders stark abgesicherte High-Speed-Transfers großer Datenmengen über das Internet
- Field Programmable Gate Arrays (FPGA) ermöglichen eine außergewöhnlich schnelle Signalverarbeitung

Ihre Vorteile

- Bandbreite bis zu 100 Gbit/s, Latenz unter 50 Mikrosekunden
- Bis zu 2.048 gleichzeitige Clients
- Zukunftssicheres VPN inkl. quantenresistentem Schlüsselaustausch für IPsec/IKEv2 ist zugelassen für VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED
- Einfache und schnelle Integration in bestehende Ökosysteme

Anwendungsbeispiel High-Speed-Kopplung von Rechenzentren



High-Speed VPN Appliance genuine

Wesentliche Anwendungen

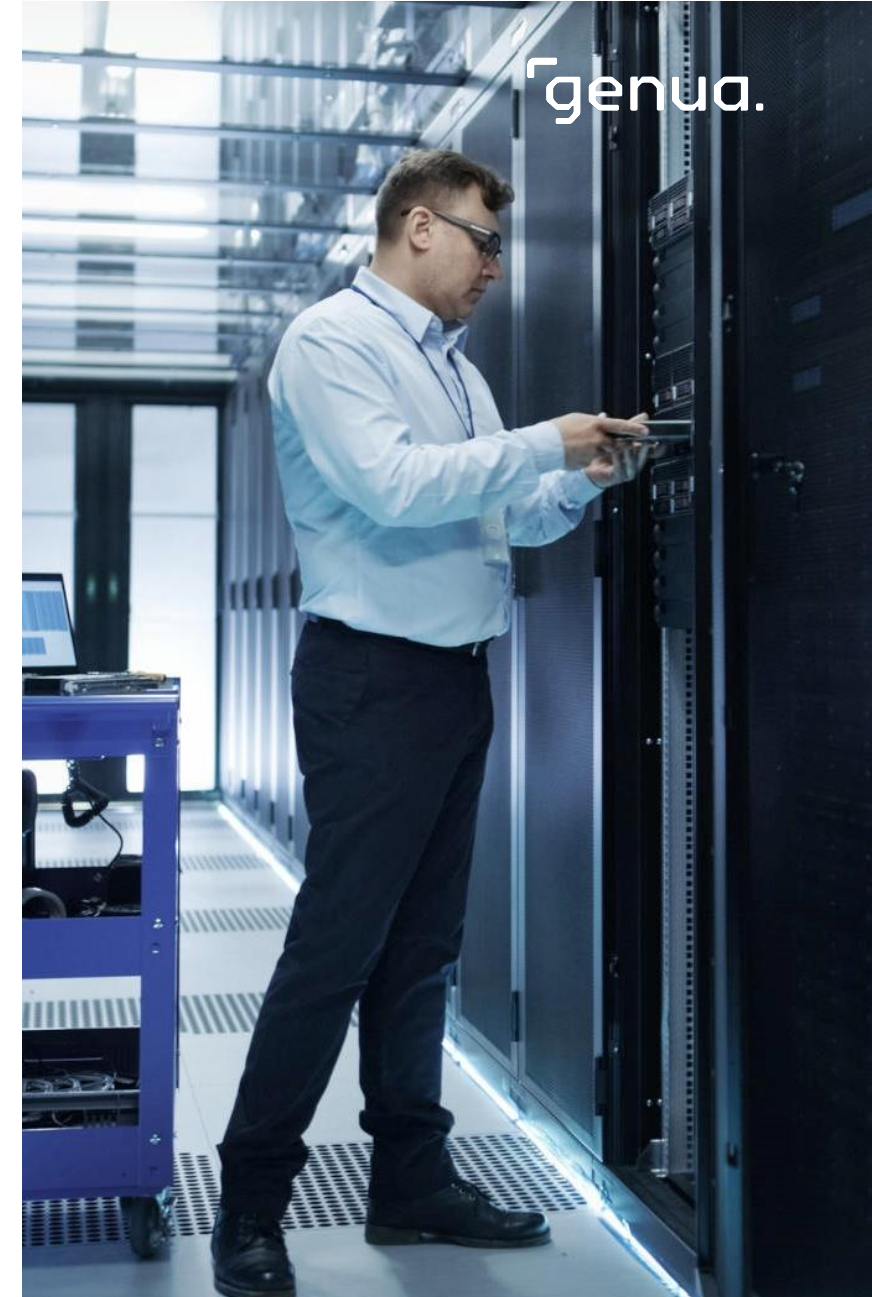
- Kopplung mehrerer Rechenzentren mit bis zu 100 Gbit pro Sekunde bei konstant niedriger Latenz
- Anbindung verteilter Standorte mit bis zu 100 Gbit pro Sekunde bei geringer Latenz, z. B. zur Absicherung anspruchsvoller Anwendungen wie VoIP- oder Videokonferenzen

Typische Einsatzbereiche

Die High-Speed VPN Appliance genuine ermöglicht es Organisationen wie

- Bundes- und Landesbehörden sowie
 - geheimschutzbetreuten Unternehmen,
- die Anforderung einer außergewöhnlich schnellen, hochsicheren Verarbeitung eingestufter Daten zu erfüllen.

 genua.de/genuline



A5

**Adva
FSP 150-
XG118Pro**

 Zugelassen

Adva

FSP 150-XG118Pro

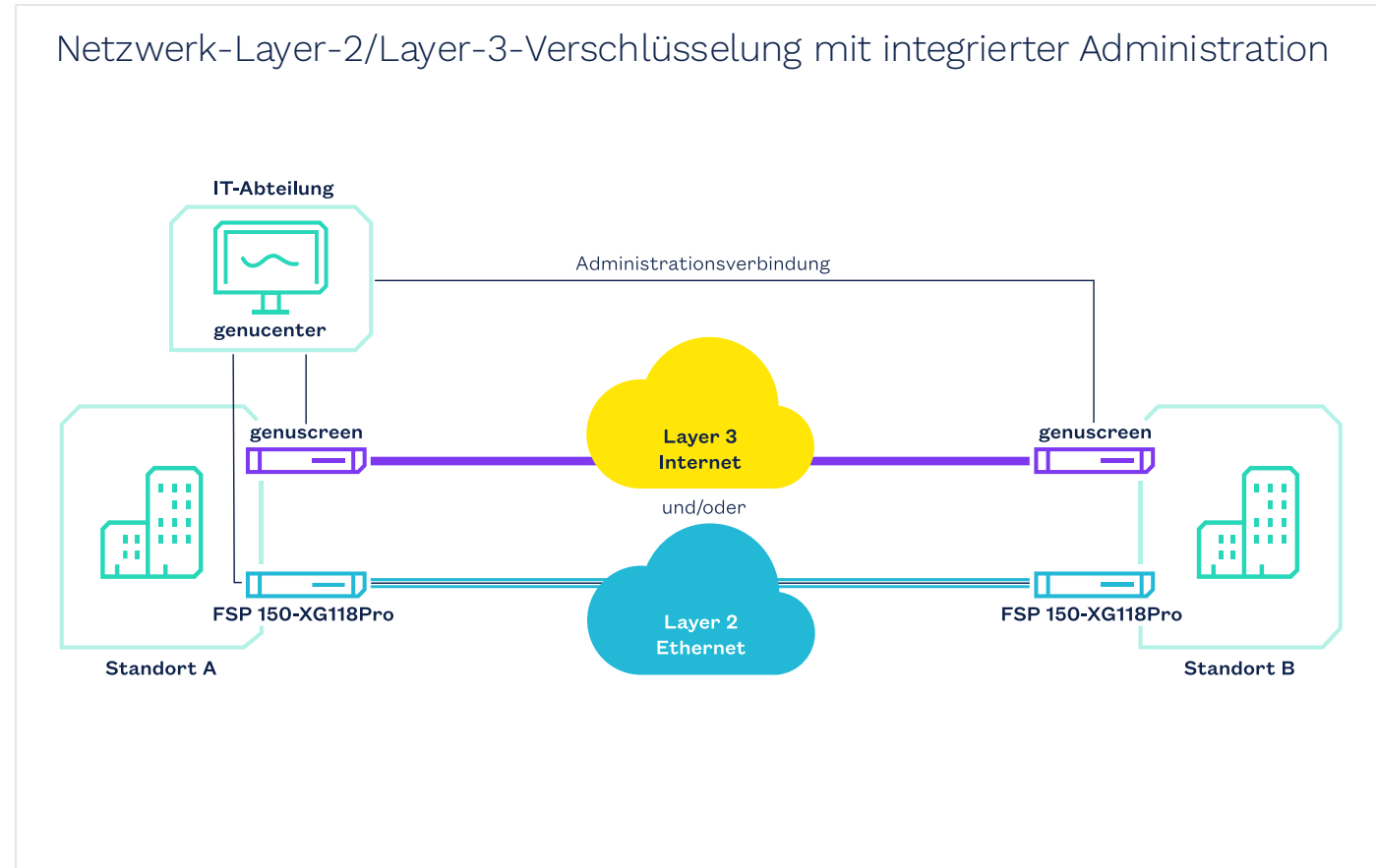
Partnerprodukt

Lösungsprofil

- Schnelle und sichere Transfers sensibler Daten
- Ende-zu-Ende Verschlüsselung von Ethernet-Verbindungen auf Netzwerk-Layer-2
- Verwaltung via Central Management Station genucenter

Ihre Vorteile

- Zulassung für VS-NfD und EU/NATO RESTRICTED
- Perfekte Ergänzung zur zugelassenen Layer-3-Lösung genuscreen in Multi-Layer-Netzen
- Optional nachrüstbares Server-Modul für virtualisierte Netzwerkfunktionen



Adva

FSP 150-XG118Pro

Wesentliche Anwendungen

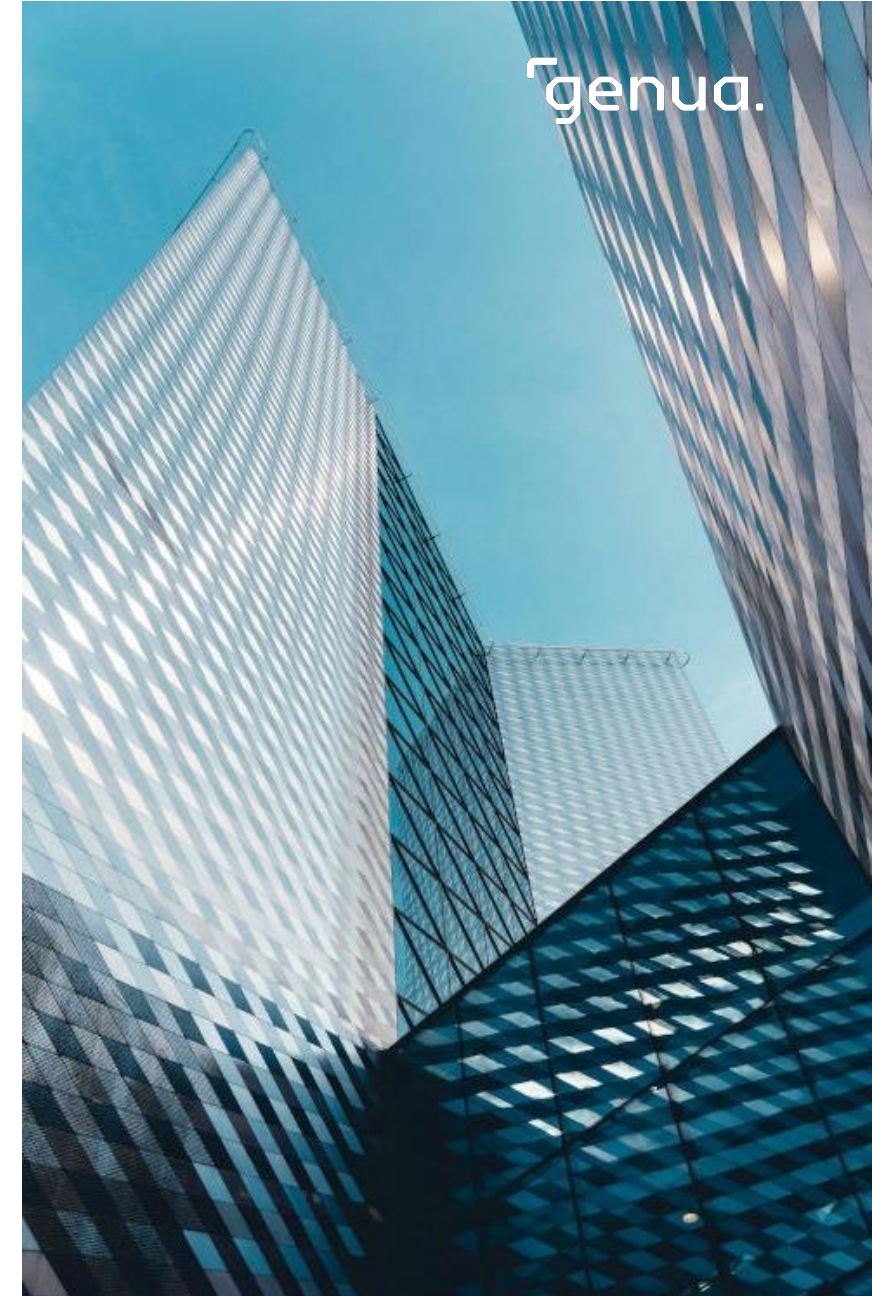
- Verschlüsselung und Übertragung klassifizierter Daten über nicht vertrauenswürdige Weitverkehrsnetze

Typische Einsatzbereiche

Das Netzzugangsgerät Adva FSP 150-XG118Pro ermöglicht z. B.

- Behörden,
- Versorgungsunternehmen und
- andere Anbieter unverzichtbarer Dienste

die Übertragung hochsensibler Daten über nicht vertrauenswürdige Netze in Cloud-Rechenzentren.



A6

Zertifikats- lösung genutrust

Zertifikatslösung genustrust

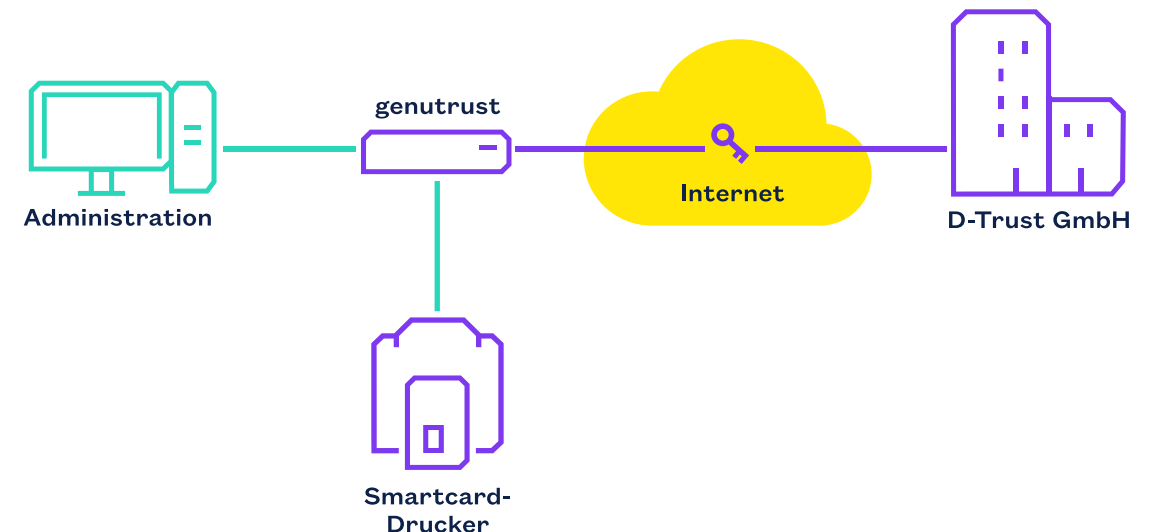
Lösungsprofil

- Bezug benötigter Mengen an VPN-Zertifikaten sowie Einrichtung von E-Mail-Zertifikaten auf Smartcards
- Optimierter Prägeprozess mit Automatismen für Smartcards
- Erfüllt alle BSI-Anforderungen an eine PKI

Ihre Vorteile

- Bezug von Zertifikaten gemäß den Richtlinien TR-03145-1.1 und TR-03145-VS-NfD
- Alle Vorteile einer PKI (D-Trust GmbH) ohne den Betrieb einer eigenen Infrastruktur
- Bundles mit verschiedenen Mengenstaffeln an Zertifikaten erhältlich
- Einfache Nutzung innerhalb bestehender Infrastrukturen

Bereitstellung von Smartcards mit der hochsicheren Zertifikatslösung genustrust



Zertifikatslösung genustrust

Wesentliche Anwendungen

- Möglichkeit, eine Public-Key-Infrastruktur (PKI) zum Bezug von VPN-Zertifikaten gemäß den Richtlinien TR-03145-1.1 und TR-03145-VS-NfD zu nutzen
- Einrichtung von E-Mail-Zertifikaten auf Smartcards

Typische Einsatzbereiche

Die Zertifikatslösung genustrust ermöglicht Organisationen

- aus dem öffentlichen Sektor und
- der Privatwirtschaft,

die nicht direkt auf die Verwaltungs-Public-Key-Infrastruktur (V-PKI) zugreifen können, den Bezug von Zertifikaten der D-Trust GmbH sowie die vollständig automatisierte Produktion gebrauchsfertiger Smartcards.



A7

Märkte & Kunden

Ihre Sicherheit im Blick

Branchenspezifische Lösungen



Öffentlicher Sektor



Geheimhaltungsbetreute Industrie



KRITIS



Industrie



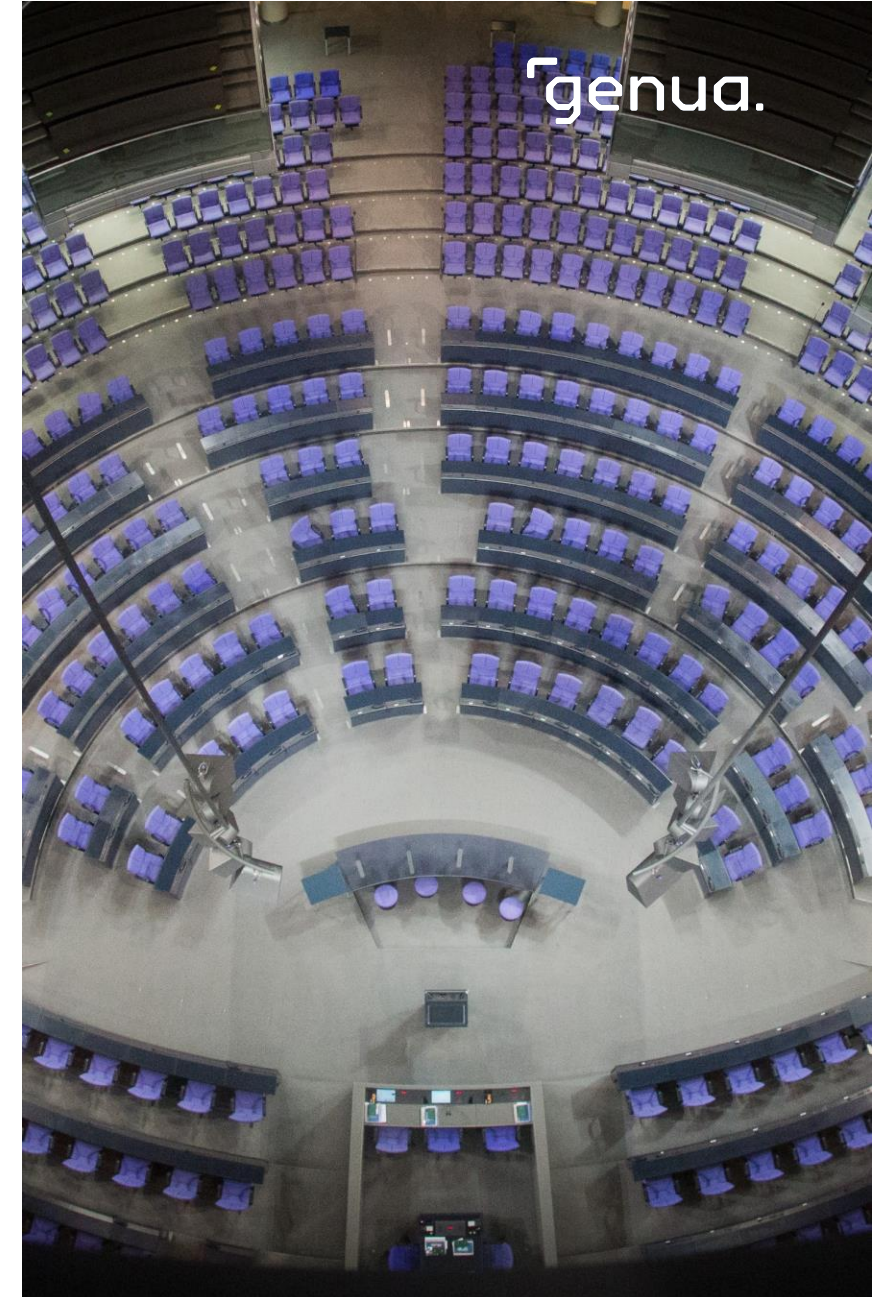


Agiler, schneller, mutiger, sicher

Eine sichere IT-Infrastruktur zählt zu den zentralen Leistungsanforderungen an zeitgemäß agierende Behörden und Unternehmen der öffentlichen Hand.

- Hochsicherheits-Portfolio für VS-konforme Infrastrukturen
- Zeitgemäße Arbeitsplätze – mobil, flexibel und VS-NfD-konform
- Zulassungen und Zertifizierungen vom BSI als anerkannte Sicherheitsnachweise

>> genua sorgt für die Sicherheit dieser Systeme und schützt die sensiblen Daten von Staat, Wirtschaft und Bürgern.





IT-Sicherheitslösungen für öffentliche Auftraggeber

Rechenzentrum



genuline

High-Speed-Datentransfers mit VS-NfD-Zulassung

genubox

Kontrollierte Remote Maintenance

vs-diode

Hochsicherer Einbahn-Datentransfer bis GEHEIM

genugate Virtual

Virtualisierte Firewall mit VS-NfD-Zulassung

Liegenschaften



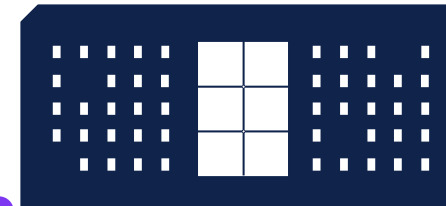
genuscreen

Sichere Vernetzung mit VS-NfD-Zulassung

Adva FSP 150-XG118Pro

Layer-2-Netzzugangsgerät mit genucenter-Verwaltbarkeit

Behörde



genugate

Robuster Netzwerkschutz mit VS-NfD-Zulassung

genuscreen

Sicherheitszonen im Netzwerk mit VS-NfD-Zulassung

Adva FSP 150-XG118Pro

Layer-2-Netzzugangsgerät mit genucenter-Verwaltbarkeit

cognitix Threat Defender

Anomalie-Erkennung und Reaktion auf Bedrohungen

genumail

Schutz vor E-Mail-basierten Angriffen

Mobile Mitarbeiter & Home Office



genusecure Suite

Lösungs-Bundle für den VS-NfD-konformen Arbeitsplatz

genuconnect

VPN Software Client mit VS-NfD-Zulassung

ECOS Secure Boot Stick SX/ZX

Sichere mobile Verwendung VS-NfD-eingestufter Informationen

genusphere

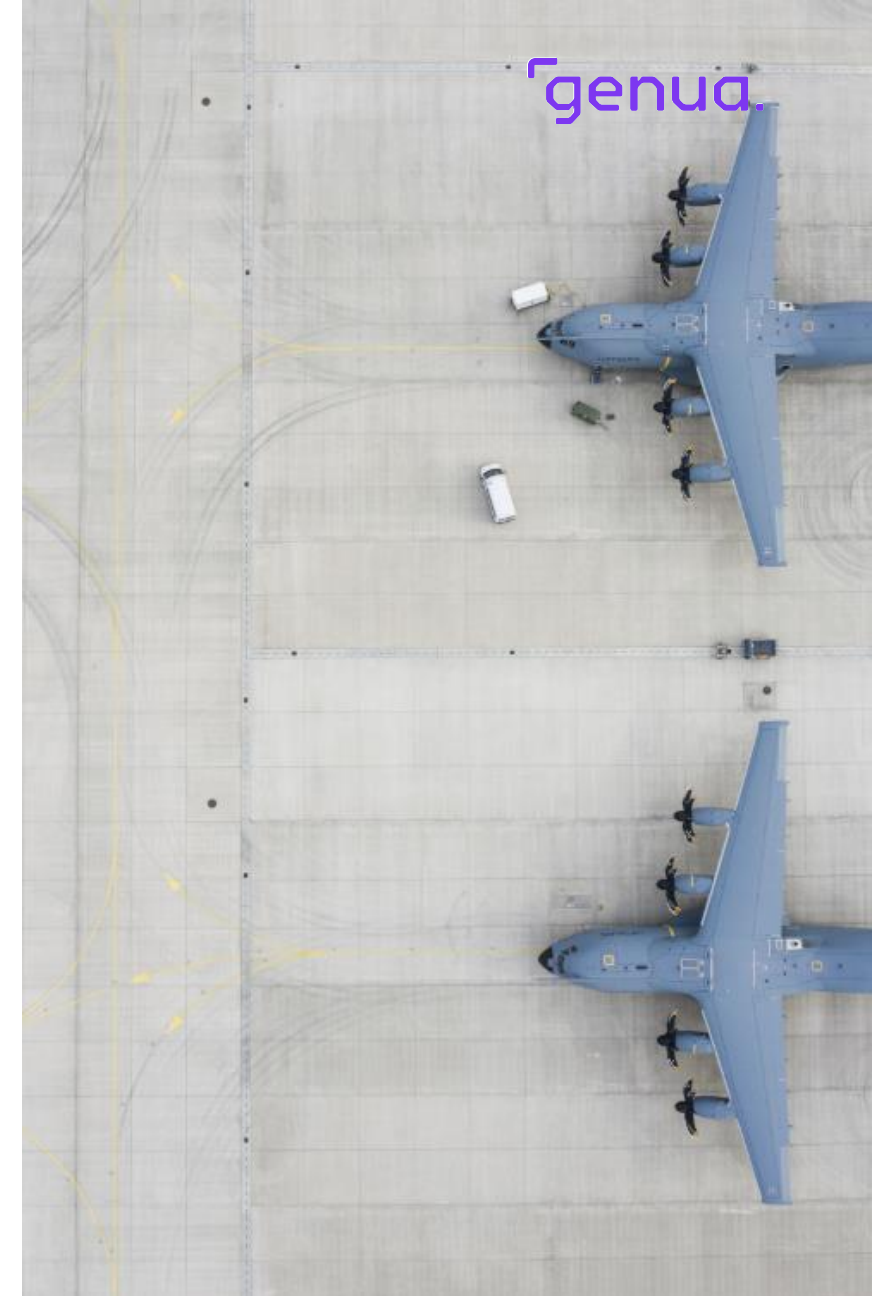
Zero-Trust-Lösung für sichere Remote-Zugriffe auf interne Applikationen

Schutz sensibler Daten bis Geheimhaltungsgrad VS-NfD

Ihr Unternehmen arbeitet mit Dokumenten und Daten,
die als "Verschlusssache" (VS) eingestuft sind?
Außenstandorte oder Mitarbeitende auf Reisen müssen
auf diese Dateien zugreifen können?

- Lösungen von genua sind vom BSI zertifiziert und zugelassen
- IT-Sicherheit made in Germany – für Ihre digitale Souveränität
- VS-konforme Infrastrukturen
- Sichere Anbindung von mobilen Arbeitsplätzen an VS-NfD-eingestufte Netze

 genua sorgt für absolute Vertraulichkeit.



IT-Sicherheitslösungen für die geheimhaltungsbetonte Industrie

Rechenzentrum



genuline

High-Speed-Datentransfers mit VS-NfD-Zulassung

genubox

Kontrollierte Remote Maintenance

vs-diode

Hochsichere Einbahn-Datentransfer bis GEHEIM

genugate Virtual

Virtualisierte Firewall mit VS-NfD-Zulassung

Filiale



genuscreen

Sichere Vernetzung mit VS-NfD-Zulassung

Adva FSP 150-XG118Pro

Layer-2-Netzzugangsgerät mit genucenter-Verwaltbarkeit

Zentrale



genugate

Robuster Netzwerkschutz mit VS-NfD-Zulassung

genuscreen

Sicherheitszonen im Netzwerk mit VS-NfD-Zulassung

Adva FSP 150-XG118Pro

Layer-2-Netzzugangsgerät mit genucenter-Verwaltbarkeit

cognitix Threat Defender

Anomalie-Erkennung und Reaktion auf Bedrohungen

genumail

Schutz vor E-Mail-basierten Angriffen

Mobile Mitarbeiter & Home Office



genusecure Suite

Lösungs-Bundle für den VS-NfD-konformen Arbeitsplatz

genuconnect

VPN Software Client mit VS-NfD-Zulassung

ECOS Secure Boot Stick SX/ZX

Sichere mobile Verwendung VS-NfD-eingestufter Informationen

genusphere

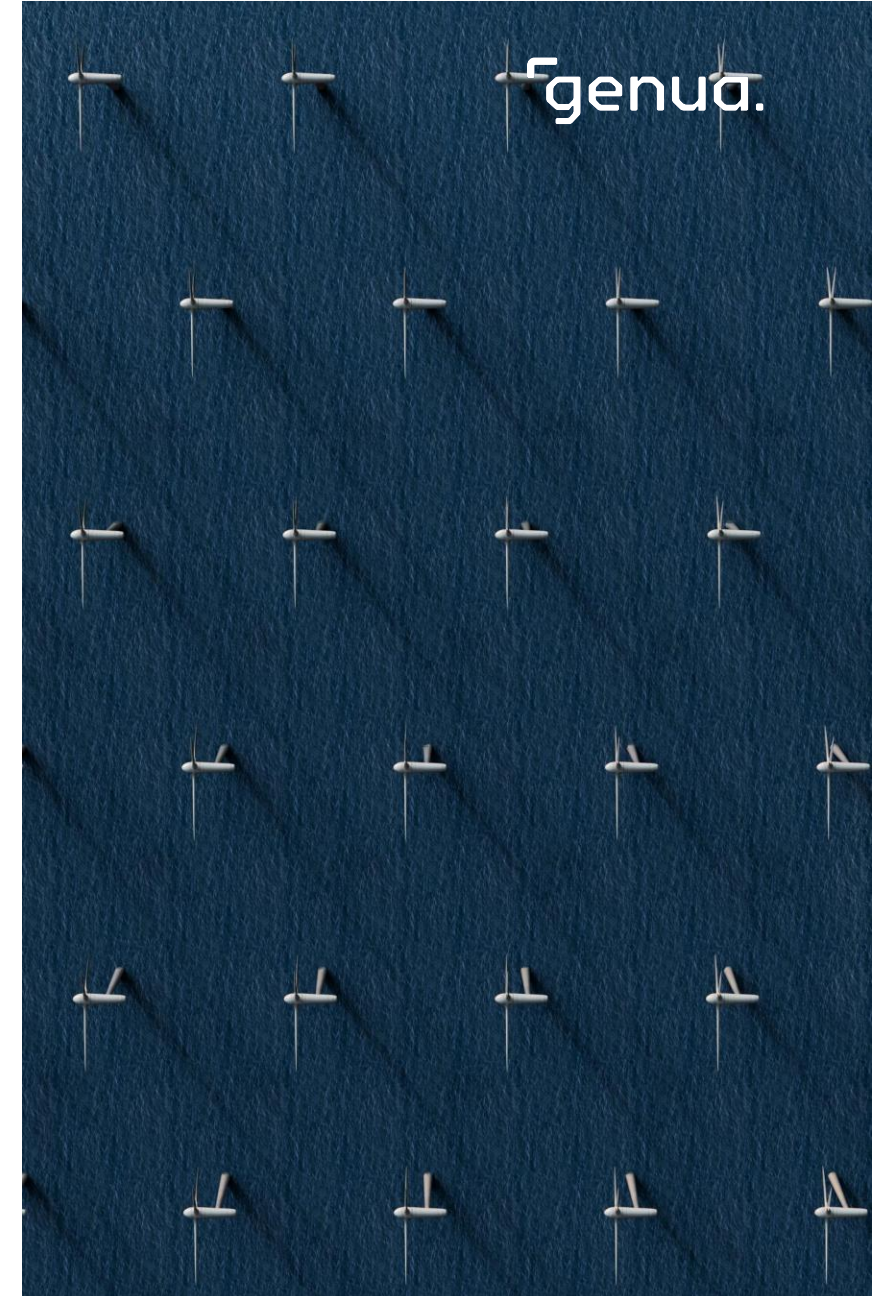
Zero-Trust-Lösung für sichere Remote-Zugriffe auf interne Applikationen

Schutz sensibler Anlagen

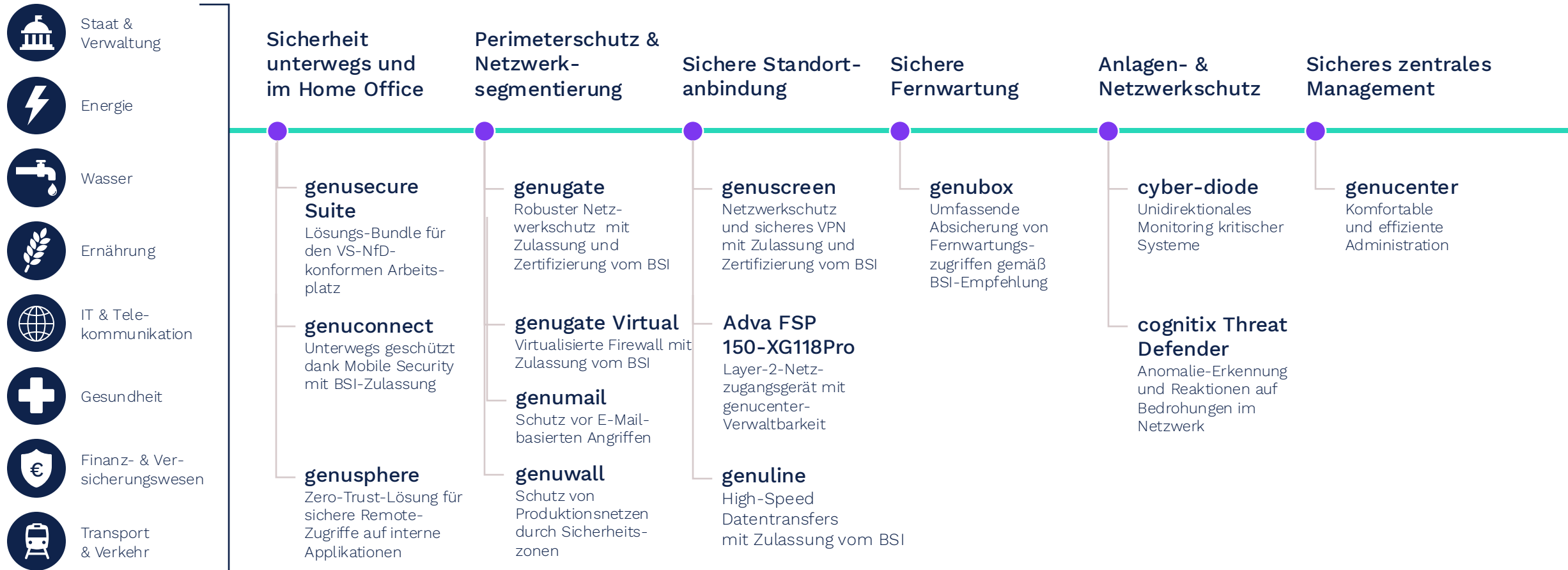
Von der Funktionsfähigkeit kritischer Infrastrukturen hängt der Schutz der Bevölkerung ab.

- Anlagen- und Netzwerkschutz durch hochsichere Zero-Trust-Fernwartung
- One-way-Datenübertragung für Predictive Maintenance
- Angriffserkennung
- Security by Design
- Sichere IT-Lieferketten

 genua sorgt für die Erfüllung höchster Sicherheitsanforderungen.



IT-Sicherheitslösungen für kritische Infrastrukturen



OT/IT-Sicherheit für die digitale Industrie 4.0

Schutz vernetzter Produktionsanlagen vor Cyberangriffen, um Verfügbarkeit, Safety und wertvolle Business Assets zu schützen.

- Umsetzung von Defense in Depth und Zero Trust
- Netzwerksegmentierung gemäß Zones & Conduits (sichere Zonenübergänge)
- Netzwerküberwachung mittels intelligenter Anomalieerkennung
- Sicherer Fernzugriff durch eine geeignete Fernwartungsarchitektur
- Hochsichere Datenausleitung mittels Datendiode

 **genua** sorgt für eine gesamtheitliche Cybersicherheitsstrategie und zuverlässige Lösungen.



IT-Sicherheitslösungen für Ihr Unternehmen

Filiale



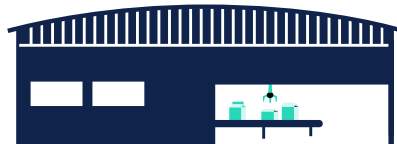
genuscreen

Sichere Vernetzung und Datensicherheit

genuline

High-Speed-Datentransfers und Datensicherheit

Produktionsstandort



cyber-diode

Monitoring kritischer Systeme

genubox

Sicher kontrollierte Fernwartung

genuwall

Für Sicherheitszonen im Produktionsnetz

Zentrale



genugate

Robuster Netzwerkschutz im Unternehmen

genuscreen

Sichere Vernetzung und Datensicherheit

cognitix Threat Defender

Anomalieerkennung und Reaktion auf Bedrohungen

genumail

Schutz vor E-Mail-basierten Angriffen

Mobile Mitarbeiter & Home Office



genusecure Suite

Lösungs-Bundle für den VS-NfD-konformen Arbeitsplatz

genuconnect Enterprise

Geschützte Verbindungen für Laptops und Tablets mit MS Windows

genusphere

Zero-Trust-Lösung für sichere Remote-Zugriffe auf interne Applikationen