Zugriff nach Bedarf statt Vollzugang.
Secure Access mit ZTNA, SASE und modernem VPN.

Secure Access ermöglicht sicheren Zugriff auf Unternehmensressourcen auf Basis von SASE, Zero Trust Network Access und modernem VPN. Argos Security plant und betreibt die Lösung – mit kontextbasierter Zugriffskontrolle und durchgesetzten Richtlinien.

>600	<15 Min	≤30 Min	seit 1999	ISO 27001	100 %
Kunden	Erkennung (MTTD)	Rückmeldung (SLA)	Managed Security	TÜV-SÜD-zertifiziert	souveränes CDC ab Q1/2027

Das leistet der Service für Sie.

ZTNA & Least Privilege

Zugriff nur auf tatsächlich benötigte Ressourcen statt Netzwerk-Vollzugang: Nutzer erhalten genau die Rechte, die sie brauchen – das reduziert die Angriffsfläche deutlich.

SASE-Architektur

Netzwerk und Sicherheit als Service aus der Cloud: sicherer Zugriff auf Cloud-Anwendungen und interne Ressourcen – unabhängig vom Standort der Nutzer.

Kontextprüfung

Jede Zugriffsanfrage wird im Kontext bewertet – abhängig von Nutzer, Gerät und Standort. Wo VPN sinnvoll bleibt, kommt eine moderne, verschlüsselte Variante zum Einsatz.

Managed Betrieb

Argos Security betreibt und überwacht die Lösung inklusive Richtlinienpflege und Support – mit nachvollziehbarer Sicht auf Zugriffe für Betrieb, Sicherheit und Audits.

Für wen: Für Unternehmen mit mobilen Teams und Cloud-Ressourcen, die klassische VPNs durch Zero-Trust-Zugriff ablösen wollen – ebenso NIS-2- und KRITIS-Organisationen mit Anforderungen an kontrollierten, nachweisbaren Zugriff.

Ein offenes VPN ist eine Tür, die immer offensteht – oft mit Zugang zum gesamten Netzwerk. Secure Access wendet das Gegenprinzip an: kontextgeprüfter Zugriff nur auf benötigte Ressourcen, verschlüsselt. KI-Agenten unterstützen die Analysten bei der Erkennung ungewöhnlicher Zugriffsmuster.

Auf Seite 2: der direkte Vergleich mit dem klassischen Ansatz →

Ihr direkter Draht: +49 89 45 24 24-100 · kontakt@argos.security

Bildmotiv: KI-generiertes Symbolbild

Argos ZTNA (Zero Trust Network Access) vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos ZTNA (Zero Trust Network Access)
Zugriff	VPN gewährt oft Netzwerk-Vollzugang	**Nur tatsächlich benötigte Ressourcen** Least Privilege reduziert die Angriffsfläche
Prüfung	Vertrauen einmalig beim Login	**Jede Anfrage im Kontext bewertet** Nach Nutzer, Gerät und Standort
Cloud	Fernzugang nur für das lokale Netz gedacht	**SASE: Sicherheit als Cloud-Service** Standortunabhängiger Ressourcenzugriff
Umstieg	Harte Ablösung mit hohem Betriebsrisiko	**Schrittweise Migration** Kritische Zugänge zuerst auf ZTNA
Betrieb	Richtlinienpflege bleibt beim eigenen Team	**Managed Betrieb durch Argos** Monitoring, Richtlinienpflege und Support

Ihr Leistungsumfang im Überblick

- Zero Trust Network Access mit Least-Privilege-Zugriff
- SASE-Architektur für Cloud- und Ressourcenzugriff
- Modernes, verschlüsseltes VPN, wo es sinnvoll bleibt
- Kontextbasierte Kontrolle nach Nutzer, Gerät und Standort
- Managed Betrieb inklusive Monitoring und Richtlinienpflege
- Transparenz und Reporting für Betrieb, Sicherheit und Audits

> **Für Ihre Geschäftsleitung:** Auswahlsorgfalt belegbar (ISO/IEC 27001 TÜV SÜD, seit 1999, >600 Kunden) · Überwachung erfüllbar (Reporting & Reviews) · SLAs vertraglich statt Best Effort.
>
> **Ihr Part:** Ansprechpartner & Zugänge im Onboarding – Rollen, Freigaben und Eingriffstiefe werden gemeinsam festgelegt. Details (RACI, SLA-Matrix, AVV/TOM) im Erstgespräch.

Souverän. Deutsch. Nachweisbar.

- SOC-Betrieb aus München – nach deutschem Recht
- Datenhaltung auf Wunsch vollständig in Deutschland
- ISO/IEC 27001 zertifiziert (TÜV SÜD)
- Unterstützt NIS-2-, DORA- und ISO-27001-Nachweise
- DSGVO-konforme Verarbeitung – AVV (Art. 28), TOM & Unterauftragsverarbeiter-Übersicht auf Anfrage
- Ab Q1/2027: 100 % souveränes Cyber Defense Center

So starten Sie mit dem Service

01
Analyse & Design

Nutzergruppen, Ressourcen und Zugriffsanforderungen werden erfasst; darauf entstehen Zero-Trust-Zugriffskonzept und passende Richtlinien.

02
Implementierung

SASE und ZTNA werden eingerichtet und in Ihre Umgebung integriert – schrittweise, kritische Zugänge werden zuerst auf ZTNA umgestellt.

03
Betrieb & Optimierung

Argos betreibt und überwacht die Lösung, pflegt die Richtlinien und verfeinert Zugriffe und Regeln laufend im Regelbetrieb weiter.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie ZTNA (Zero Trust Network Access) auf Ihre Infrastruktur und Bedrohungslage zugeschnitten wird.



Dr. Nils Kaufmann
Chief Sales Officer

+49 89 45 24 24-100
kontakt@argos.security · www.argos.security

Mehr zur Leistung: argos.security/leistungen/ztna →

Termin buchen

Bildmotiv: KI-generiertes Symbolbild

07-2026