Zugriff nach Bedarf, nicht aufs ganze Netz. SASE und ZTNA als Managed Service.

SASE verbindet Netzwerk- und Sicherheitsfunktionen als Cloud-Service für standortunabhängigen Zugriff. Mit Zero Trust Network Access erhalten Nutzer genau die Zugriffsrechte, die sie benötigen – Argos plant, implementiert und betreibt die Lösung.

>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.

Zero Trust Network Access

ZTNA gewährt Zugriff nur auf einzelne, tatsächlich benötigte Ressourcen – mit Kontextprüfung nach Nutzer, Gerät und Standort statt pauschalem Netzzugang.

SASE-Architektur

Netzwerk- und Sicherheitsfunktionen kommen konvergent aus der Cloud – für sicheren, standortunabhängigen Zugriff auf Unternehmens- und Cloud-Ressourcen.

Modernes VPN

Wo VPN weiterhin sinnvoll ist, bleibt es – modern und verschlüsselt. Die Migration erfolgt schrittweise, kritische Zugänge werden zuerst umgestellt.

Betrieb & Richtlinien

Argos betreibt die Lösung als Managed Service – mit Monitoring, laufender Richtlinienpflege und Transparenz durch Reporting und Audit-Nachvollziehbarkeit.

Für wen: Für mobile und hybride Teams, Unternehmen mit Cloud-Ressourcen und Organisationen, die klassische VPNs ablösen möchten – ebenso für NIS-2- und KRITIS-Organisationen mit strikten Zugriffsanforderungen.

Klassische VPNs geben oft Zugang zum gesamten Netzwerk – ein Risiko, sobald ein Zugang kompromittiert wird. Argos invertiert dieses Prinzip: Zugriff wird kontextabhängig geprüft und auf die tatsächlich benötigten Ressourcen begrenzt – nach dem Least-Privilege-Prinzip, betrieben als Managed Service.

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

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

Bildmotive: KI-generierte Symbolbilder

Argos SASE (Secure Access Service Edge) vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos SASE (Secure Access Service Edge)
Zugriffsmodell	VPN öffnet oft das gesamte Netzwerk	**Zugriff nur auf benötigte Ressourcen** isoliert, nach dem Least-Privilege-Prinzip
Prüfung	Einmal eingewählt, dauerhaft drin	**Kontextprüfung bei jedem Zugriff** nach Nutzer, Gerät und Standort
Architektur	Getrennte Netzwerk- und Sicherheitslösungen	**Konvergent aus der Cloud** eine SASE-Architektur, standortunabhängig
Migration	VPN-Ablösung als riskanter Big Bang	**Schrittweiser Umstieg** kritische Zugriffe zuerst, VPN wo sinnvoll
Betrieb	Richtlinienpflege bindet das eigene Team	**Managed Service durch Argos** Monitoring, Richtlinienpflege, Reporting

Ihr Leistungsumfang im Überblick

- Zero Trust Network Access für benötigte Ressourcen
- SASE-Architektur mit Sicherheitsfunktionen aus der Cloud
- Modernes, verschlüsseltes VPN für geeignete Anwendungsfälle
- Kontextbasierte Zugriffskontrolle nach Nutzer und Gerät
- Betrieb, Monitoring und Richtlinienpflege als Managed Service
- Reporting und Audit-Nachvollziehbarkeit

> **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

Sie erfassen mit Argos Nutzergruppen, Ressourcen und Anforderungen. Daraus entsteht das Zero-Trust-Konzept für Ihre Zugriffsarchitektur.

02
Implementierung

Argos richtet die Lösung ein und integriert sie in Ihre Umgebung – die Migration vom klassischen VPN erfolgt schrittweise, kritische Zugriffe zuerst.

03
Betrieb & Optimierung

Argos betreibt die Lösung mit laufendem Monitoring und Richtlinienpflege und verfeinert die Zugriffsregeln kontinuierlich weiter.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie SASE (Secure Access Service Edge) 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/sase →

Termin buchen

Bildmotive: KI-generierte Symbolbilder