Nur konforme Geräte kommen ins Netz.
Network Access Control als Managed Service.

NAC kontrolliert, welche Geräte sich mit Ihrem Netzwerk verbinden dürfen: Nur bekannte, richtlinienkonforme Geräte erhalten Zugang. Argos betreibt NAC als Managed Service – mit automatischer Geräteerkennung, Richtliniendurchsetzung und voller Sichtbarkeit.

>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.

Geräteerkennung

Jedes Gerät im Netz wird automatisch erkannt und klassifiziert – Sie erhalten Echtzeit-Sichtbarkeit über alle Endpunkte, ohne blinde Flecken.

Zugangskontrolle

Richtlinienbasierte Kontrolle nach Nutzer, Gerät und Zustand entscheidet, wer ins Netz darf – non-konforme Geräte werden automatisch isoliert.

Gäste & BYOD

Gäste- und mitgebrachte Geräte werden sicher eingebunden – mit passenden, eingeschränkten Rechten und einheitlichen Regeln über alle Standorte.

Betrieb & Reporting

Argos übernimmt Betrieb und Monitoring als Managed Service, setzt Compliance-Vorgaben durch und liefert nachvollziehbares Reporting.

Für wen: NAC eignet sich für den Mittelstand mit wachsender Gerätezahl, Organisationen mit NIS-2- und KRITIS-Anforderungen an dokumentierten Netzzugang sowie Unternehmen mit vielen BYOD- und Gästegeräten oder verteilten Standorten.

Jedes unbekannte Gerät im Netz ist ein potenzielles Einfallstor – und man kann nicht schützen, was man nicht sieht. Argos schafft Sichtbarkeit und Kontrolle: Nur konforme Geräte erhalten Zugang, alle anderen werden erkannt und isoliert – betrieben als Managed Service, ohne Betriebsaufwand in Ihrem Team.

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

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

07-2026

Bildmotive: KI-generierte Symbolbilder

Argos Network Access Control (NAC) vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Network Access Control (NAC)
Sichtbarkeit	Unbekannte Geräte bleiben unentdeckt	**Jedes Gerät erkannt und klassifiziert** Echtzeit-Sichtbarkeit über alle Endpunkte
Zugang	Wer im Netz ist, bleibt weitgehend unkontrolliert	**Zugang nur für konforme Geräte** nach Nutzer, Gerät und Zustand
Abweichungen	Non-konforme Geräte bleiben im Netz	**Automatische Isolierung** unautorisierte Zugriffe werden verhindert
Gäste & BYOD	Ad-hoc-Freigaben ohne einheitliche Regeln	**Sicheres Onboarding mit klaren Rechten** einheitlich über verteilte Standorte
Betrieb	Pflege und Monitoring binden das eigene Team	**Managed Service durch Argos** inklusive Reporting und Compliance-Nachweis

Ihr Leistungsumfang im Überblick

- Automatische Geräteerkennung und -klassifizierung
- Richtlinienbasierte Zugangskontrolle nach Nutzer und Gerät
- Isolierung non-konformer Geräte
- Sicheres Gäste- und BYOD-Onboarding
- Echtzeit-Sichtbarkeit über alle Endpunkte
- Betrieb, Monitoring und nachvollziehbares Reporting

> **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
Erstgespräch & Aufnahme

Sie klären mit Argos Netzstruktur, Standorte und Anforderungen – von BYOD und Gästen bis zu dokumentiertem Netzzugang nach NIS-2 und ISO 27001.

02
Richtlinien & Rollout

Argos definiert Zugangsrichtlinien nach Nutzer, Gerät und Zustand, richtet die Geräteerkennung ein und bindet Gäste- und BYOD-Geräte sicher an.

03
Regelbetrieb

Argos betreibt und überwacht NAC als Managed Service, isoliert non-konforme Geräte automatisch und liefert nachvollziehbares Reporting.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Network Access Control (NAC) 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/network-access-control-nac →

Termin buchen

Bildmotive: KI-generierte Symbolbilder

07-2026