Die letzte Verteidigungslinie hält.
Endpoint Protection als Managed Service.

Endpoint Protection schützt Laptops, Server und mobile Geräte vor Malware, Ransomware und verdächtigen Aktivitäten. Argos betreibt die Lösung als Managed Service – mit verhaltensbasierter Erkennung und 24/7-Überwachung aus dem eigenen SOC.

>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.

Verhaltensbasiert

Verhaltensbasierte Erkennung stoppt auch unbekannte und dateilose Bedrohungen, die klassische Signaturen übersehen – die entscheidende Ergänzung zum Virenschutz.

MDR aus dem SOC

Managed Detection & Response: Das SOC überwacht Ihre Endgeräte rund um die Uhr, bewertet verdächtige Aktivitäten und dämmt sie ein.

Schnelle Isolation

Kompromittierte Geräte werden schnell isoliert, bevor sich Angriffe ausbreiten – ergänzt um proaktives Threat Hunting durch die Analysten.

Zentrale Verwaltung

Zentrale Verwaltung und Richtliniendurchsetzung über alle Geräte hinweg – mit nachvollziehbarem Reporting je Gerät und Standort für Ihre Nachweispflichten.

Für wen: Geeignet ist die Leistung für Unternehmen mit hybriden, ortsunabhängigen Arbeitsumgebungen sowie für den Mittelstand ohne eigenes Security Operations Center, der Erkennung und Reaktion auslagern will.

Klassischer Virenschutz erkennt nur Bekanntes über Signaturen – unbekannte und dateilose Angriffe laufen durch. Argos ergänzt verhaltensbasierte Erkennung um Managed Detection & Response: Das SOC bewertet verdächtige Aktivitäten rund um die Uhr, KI-Agenten priorisieren Alarme – die Bewertung bleibt in Expertenhand.

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

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

Argos Endpoint Protection vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Endpoint Protection
Erkennung	Signaturbasiert, nur bekannte Malware	**Verhaltensbasierte Erkennung** auch unbekannte und dateilose Angriffe
Überwachung	Alarme laufen ins Leere	**24/7-Überwachung aus dem SOC** deutschsprachige Analysten, DACH-Fokus
Reaktion	Manuelle Reaktion, oft zu spät	**Schnelle Isolation betroffener Geräte** SOC-gestützte Eindämmung rund um die Uhr
Proaktivität	Warten auf den nächsten Alarm	**Proaktives Threat Hunting**
Nachweis	Kaum belastbare Dokumentation	**Reporting je Gerät und Standort** belastbar für NIS-2- und KRITIS-Anforderungen

Ihr Leistungsumfang im Überblick

- Malware- & Ransomware-Schutz mit verhaltensbasierter Erkennung
- Managed Detection & Response aus dem SOC
- 24/7-Überwachung und schnelle Isolation kompromittierter Geräte
- Proaktives Threat Hunting
- Zentrale Verwaltung und Richtliniendurchsetzung
- Nachvollziehbares Reporting je Gerät und Standort

> **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 & Scoping

Wir erfassen Geräte, Standorte und Anforderungen – von hybriden Arbeitsumgebungen bis zu NIS-2- und KRITIS-Vorgaben – und definieren Richtlinien.

02
Rollout & Anbindung

Argos rollt die Lösung über alle Endgeräte aus, setzt zentrale Richtlinien durch und bindet Ihre Umgebung an die 24/7-Überwachung des SOC an.

03
Regelbetrieb & Reaktion

Das SOC überwacht, bewertet und dämmt rund um die Uhr ein – inklusive Threat Hunting, schneller Isolation und laufendem Reporting.

> *„Dank der professionellen und schnellen Hilfe können wir Vorfälle jederzeit und schnell bereinigen. Die umfassende und kompetente Beratung inklusive rechtlicher Betreuung ist unbezahlbar.“*
>
> Sascha Prütz, Vorstand, WIIT AG

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Endpoint Protection 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/endpoint-protection →

Termin buchen