Gestoppt, bevor es Ihre Mitarbeitenden erreicht. Email Security von Argos.

Neun von zehn Angriffen beginnen mit einer E-Mail. Email Security stoppt Phishing, Malware und Spam vor dem Posteingang – mit einer mehrstufigen Filterung, die Argos betreibt und laufend an neue Angriffsmuster anpasst.

>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.

Mehrstufige Filterung

Mehrstufige Phishing-, Malware- und Spam-Filter wehren Massen-Kampagnen ebenso ab wie gezielte Angriffe – mit adaptiver Bedrohungsabwehr und Anti-Ransomware am E-Mail-Eingang.

Echtzeit-Analyse

URLs und Anhänge werden in Echtzeit analysiert, verdächtige Inhalte kontrolliert detoniert. Schadinhalte werden gestoppt, bevor sie ein Endgerät erreichen können.

Schutz vor CEO-Fraud

Impersonation- und Spoofing-Schutz fängt gezielte Angriffe wie Spear-Phishing und Business E-Mail Compromise ab, die Basisfilter häufig durchlassen – gerade gegen Führungskräfte.

Integration & Reporting

Nahtlose Integration in Microsoft 365 und Google Workspace sowie nachvollziehbares Reporting – auch als dokumentierte Phishing-Abwehr für NIS-2 und regulierte Branchen.

Für wen: Für jede Organisation, die E-Mail nutzt – besonders für Unternehmen, deren Führungskräfte Ziel von CEO-Fraud und BEC sind, für Microsoft-365- und Google-Workspace-Nutzer sowie für NIS-2-verpflichtete und regulierte Branchen.

Integrierte Basisfilter fangen viel ab – gezielte Angriffe wie Spear-Phishing und BEC lassen sie häufig durch. Argos ergänzt eine spezialisierte, adaptive Schutzschicht. KI-Agenten helfen den Analysten, neue Kampagnen früh zu erkennen und Muster über viele Postfächer zu korrelieren – die Freigabe von Regeln 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 Email Security vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Email Security
Spear-Phishing	Basisfilter lassen gezielte Angriffe häufig durch	**Spezialisierte adaptive Schutzschicht** fängt Spear-Phishing und BEC ab
Analyse	Links und Anhänge werden kaum tiefgehend geprüft	**URL- und Anhang-Analyse in Echtzeit** mit Detonation verdächtiger Inhalte
Absender	Gefälschte Absender wirken täuschend echt	**Impersonation- und Spoofing-Schutz** gegen CEO-Fraud und BEC auf Führungsebene
Anpassung	Regeln veralten, Angreifer ändern Muster	**Adaptive Bedrohungsabwehr** passt sich laufend an neue Angriffsmuster an
Nachweis	Phishing-Abwehr kaum dokumentierbar	**Nachvollziehbares Reporting** dokumentiert für NIS-2 und regulierte Branchen

Ihr Leistungsumfang im Überblick

- Mehrstufige Phishing-, Malware- und Spam-Filter
- URL- und Anhang-Analyse in Echtzeit mit Detonation
- Impersonation- und Spoofing-Schutz gegen CEO-Fraud und BEC
- Anti-Ransomware und adaptive Abwehr am E-Mail-Eingang
- Nahtlose Integration in Microsoft 365 und Google Workspace
- Nachvollziehbares Reporting für NIS-2 und regulierte Branchen

> **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 & Anbindung

Im Erstgespräch klären wir Ihre Mail-Umgebung und Schutzanforderungen. Die Lösung integriert sich nahtlos in Microsoft 365 oder Google Workspace.

02
Feinjustierung

Die mehrstufige Filterung wird auf Ihre Organisation abgestimmt – inklusive Impersonation-Schutz für Führungskräfte und Prüfung ausgehender Mails.

03
Adaptiver Betrieb

Argos passt den Schutz laufend an neue Angriffsmuster an. KI-Agenten erkennen Kampagnen früh, die Regel-Freigabe bleibt in Expertenhand.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Email Security 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/email-security →

Termin buchen