

Logicalis Security Assessment

Shadow-AI Assessment

Volle Transparenz über KI-Nutzung, Datenabflüsse und Schatten-IT – in 30 Tagen.

Das Risiko: Schatten-KI in Ihrem Unternehmen

Viele Unternehmen wissen heute nicht, welche Abteilungen generative AI nutzen, welche Daten dabei übertragen werden – oder ob sensible Informationen unbeabsichtigt an externe Modelle wie ChatGPT, Claude oder Gemini gesendet werden. Unkontrollierte Cloud-AI-Nutzung und Schatten-IT laufen häufig unbemerkt über DNS-Abfragen, Web-Zugriffe und verschlüsselte API-Calls.

Unser Ansatz: 3 Stufen zu voller Transparenz

1

DNS-Monitoring

Externe DNS-Anfragen werden an Cisco Secure Access weitergeleitet – sofortige Sichtbarkeit über AI-Domains & Shadow-IT.

2

Traffic-Forwarding

Ausgewählter Unternehmens-Traffic wird geroutet – umfassendere Analyse von Web- & Cloud-Zugriffen.

3

Deep Inspection & DLP

SSL-Entschlüsselung und AI-spezifisches Data-Loss-Prevention-Monitoring für maximale Detailtiefe.

Ihr Nutzen: 3 konkrete Reports

- ✓ **AI Visibility Report** – welche AI-Dienste, APIs und Modelle nutzen welche Abteilungen, wie oft und offiziell vs. inoffiziell.
- ✓ **Shadow-AI- & SaaS-Risikoanalyse** – nicht genehmigte AI-Tools, Browser-Erweiterungen und neu aufgetauchte Domains im AI-Kontext.
- ✓ **Deep-Inspection- & DLP-Analyse** – welche sensiblen Daten (PII, Kundendaten, Quellcode) tatsächlich an externe KI-Systeme übertragen werden..

Aufwand & Ablauf

Ca. 8 Personentage über 1-2 Wochen · 30-Tage-Testlizenz Cisco Secure Access inklusive · minimaler Aufwand für Ihr Team, kein Eingriff in den produktiven Betrieb.

Cisco Global Gold Partner · 7.500+ Architects of Change in über 30 Ländern · 10.000+ Kunden weltweit

Interesse? Lassen Sie uns sprechen.

Vereinbaren Sie einen unverbindlichen Termin für ein kostenfreies Erstgespräch.

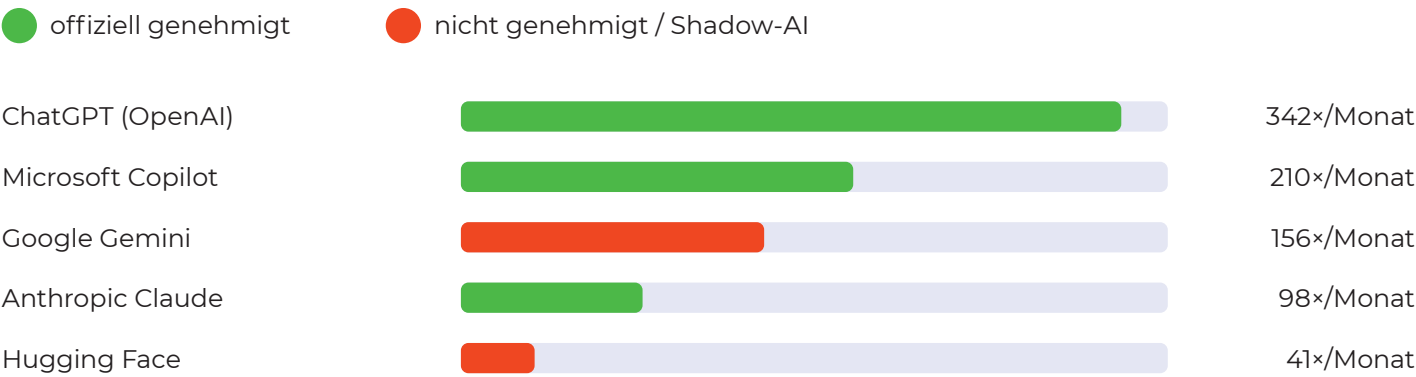
Arun Wadhawan · arun.wadhawan@logicalis.de · **+49 1522 2516 526** · www.logicalis.de

So sieht Ihre Auswertung aus

Auszug aus dem AI Visibility Report — inkl. Shadow-AI-Funde und DLP-Auffälligkeiten

Beispielhafte Darstellung mit fiktiven Werten zur Veranschaulichung. Ihre Auswertung basiert ausschließlich auf den tatsächlich in Ihrem Unternehmen erhobenen Daten.

1 Verteilung sensibler Daten nach Kategorie (Beispiel)



2 Shadow-AI- & SaaS-Risikoanalyse – Top-Funde (Beispiel)

BEFUND	ABTEILUNG	STATUS	RISIKO
QuillBot	Marketing	Nicht genehmigt	HOCH
Perplexity AI	Vertrieb	Nicht genehmigt	MITTEL
DeepL Write	HR	Nicht genehmigt	MITTEL
Notion AI	Produktentwicklung	Genehmigt	NIEDRIG

3 Deep-Inspection- & DLP-Analyse (Beispiel)

23 Datei-Uploads mit potenziell sensiblen Kundendaten an externe AI-Tools identifiziert (Kalenderwoche 34).

Betroffene Datentypen: Kundendaten (PII), interner Quellcode, Vertragsdokumente. Übertragungswege: Datei-Upload, Copy-&-Paste, Browser-Erweiterung.

Ihr vollständiger Report schafft eine belastbare Entscheidungsgrundlage.

Am Ende erhalten Sie den vollständigen Report inkl. Handlungsempfehlungen für Governance, DLP und eine sichere AI-Einführung in Ihrem Unternehmen.

Arun Wadhawan • arun.wadhawan@logicalis.de • +49 1522 2516 526 • www.logicalis.de