

Logicalis Security Assessment

Data Security Assessment

Wissen, wo sensible Daten liegen, wer darauf zugreift und welche davon in KI-Anwendungen fließen – erste Ergebnisse in 48 Stunden.

Das Risiko: Blinde Flecken in der eigenen Datenlandschaft

Daten liegen verteilt über M365, Fileshares, Cloud-Speicher, SaaS-Dienste und Data Lakes. Eine vollständige Klassifizierung existiert in vielen Unternehmen nur teilweise oder gar nicht – regelbasierte Verfahren mit Pattern und Regex erzeugen zugleich viele False Positives und erreichen selten die gesamte Datenlandschaft.

Gleichzeitig steigen die Anforderungen durch DSGVO, NIS2 und Audits: „Wo liegen unsere regulierten Daten und wer kann darauf zugreifen?“ muss belegbar beantwortet werden – nicht geschätzt. Und mit Copilot, KI-Agenten und Shadow AI fließen genau diese Daten bereits in KI-Systeme.

Unser Ansatz: 3 Stufen zu voller Transparenz

1

Scoping & agentenlose Anbindung

Gemeinsame Auswahl einer aussagekräftigen Datenquelle, Ziele und Erfolgskriterien.
Anbindung read-only per API – kein Agent, kein Eingriff in Ihre Systeme.

2

KI-native Klassifizierung

Cyera erkennt und klassifiziert kontextbezogen: personenbezogene Daten, Finanz- und Gesundheitsdaten, geistiges Eigentum, Quellcode – inklusive kritischer Datenkombinationen.

3

Zugriffs- & Risikoanalyse

Wer kann auf sensible Daten zugreifen? Überprivilegierte und externe Zugriffe, offen geteilte Ablagen sowie Datenflüsse in KI-Dienste – priorisiert nach Risiko.

Ihr Nutzen: 3 konkrete Reports

- ✓ **Management-Report** – Ergebnisse und Risikolage verdichtet und aufbereitet für Geschäftsführung, Vorstand und Auditoren – inklusive Nachweisgrundlage für DSGVO- und NIS2-Anforderungen.
- ✓ **Gemeinsames Analyse-Dokument** – technische Befunde im Detail: Datenarten, Fundorte, Zugriffsrechte, exponierte Ablagen und riskante Datenkombinationen in Ihrer realen Umgebung – keine Demo-Daten.
- ✓ **Priorisierte Handlungsfelder & Roadmap** – bewertet nach Risiko und Aufwand – Ihre Basis für Quick Wins, für den sicheren Rollout von Copilot und KI-Agenten sowie für die Entscheidung über nächste Schritte.

Aufwand & Ablauf

Ca. 5 Personentage über 2–3 Wochen · erste Datentransparenz rund 48 Stunden nach Anbindung · agentenlos und read-only · bestehende Investitionen (z. B. Microsoft Purview) bleiben erhalten und werden ergänzt, nicht ersetzt.

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.

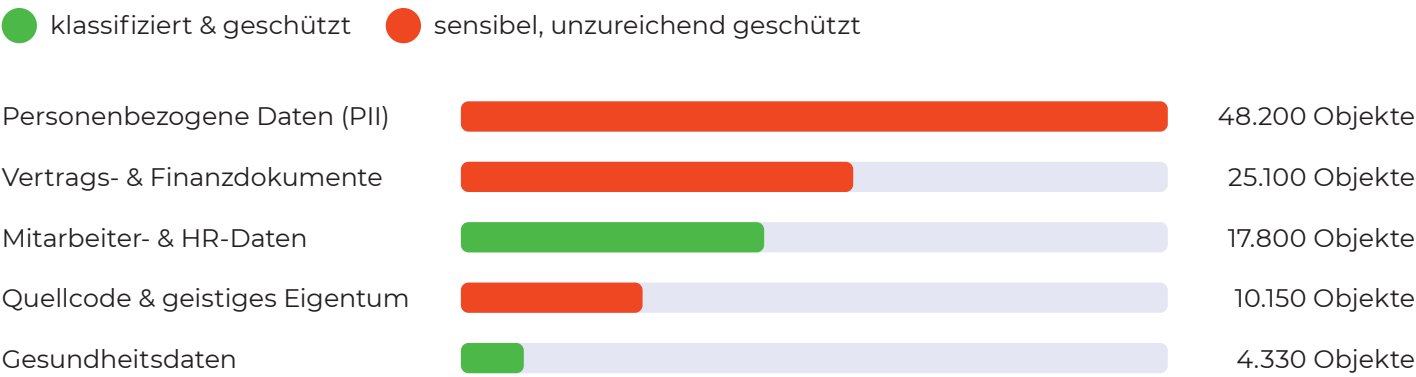
Arun Wadhawan · arun.wadhawan@logicalis.de · +49 1522 2516 526 · www.logicalis.de

So sieht Ihre Auswertung aus

Auszug aus dem Data Security Report – inkl. Klassifizierung, Zugriffsrisiken und KI-Datenflüssen

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 Zugriffs- & Exponierungsanalyse – Top-Funde (Beispiel)

BEFUND	FUNDORT	UMFANG	RISIKO
Öffentlich geteilte Links auf PII-Dateien	SharePoint Online	312 Dateien	HOCH
Überprivilegierte Zugriffsgruppe („Alle Mitarbeitenden“)	Fileshare Finanzen	9.400 Dateien	HOCH
Externe Gastzugriffe auf Vertragsordner	Microsoft Teams	47 Gäste	MITTEL
Klartext-Zugangsdaten in Dokumenten	OneDrive	86 Dateien	MITTEL
Veraltete Kopien regulierter Daten	Archiv-Fileshare	2.150 Dateien	NIEDRIG

3 Shadow AI & KI-Datenflüsse (Beispiel)

Sensible Daten in 6 nicht freigegebenen KI-Diensten nachweisbar

Neben M365 Copilot wurden weitere KI-Dienste mit Zugriff auf Unternehmensdaten identifiziert. Betroffen sind personenbezogene Daten, Quellcode und Finanzdaten. Zusätzlich: 3 selbst gebaute KI-Anwendungen (Copilot-Studio-Agenten) mit Anbindung an sensible Datenquellen ohne dokumentierte Freigabe

Ihr vollständiger Report schafft eine belastbare Entscheidungsgrundlage.

Am Ende erhalten Sie den vollständigen Report inkl. priorisierter Handlungsfelder und Roadmap-Empfehlung für Data Governance, DLP-Optimierung und eine sichere KI-Einführung. Alle Ergebnisse und Dokumente verbleiben bei Ihnen – unabhängig von Ihrer Entscheidung.

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