Sicherer Einsatz von Microsoft 365 Copilot

Schutz für Unternehmen durch Defender und Purview Services

Rashad Bakirov, Controlware GmbH, CC Cloud Modern Workplace
Robert Krauss, Controlware GmbH, CC Cloud Modern Workplace

16.09.2025, Congress Park Hanau

Überblick über die Agenda

1. Zero-Trust-Prinzipien und Microsoft 365 Copilot
2. Risikominderung
3. Datenschutz und Compliance
4. Sensibilisierung der Benutzer für Bedrohungen und Updates
5. Fazit

controlware

Die größte Chance und das größte Risiko für Ihre Daten?

Microsoft 365 Copilot ist ein Paradigmenwechsel für die Produktivität in Ihrem Unternehmen.

Gleichzeitig agiert die KI als Brandbeschleuniger: Sie deckt jede Schwachstelle in Ihrer Datenstruktur und Ihren Berechtigungen gnadenlos auf und macht sie nutzbar.

In den nächsten 40 Minuten erhalten Sie den strategischen Fahrplan, um die enormen Chancen von Copilot sicher zu nutzen – und die Risiken mit Defender und Purview gezielt zu beherrschen.

Übersicht über Microsoft 365 Copilot

controlware

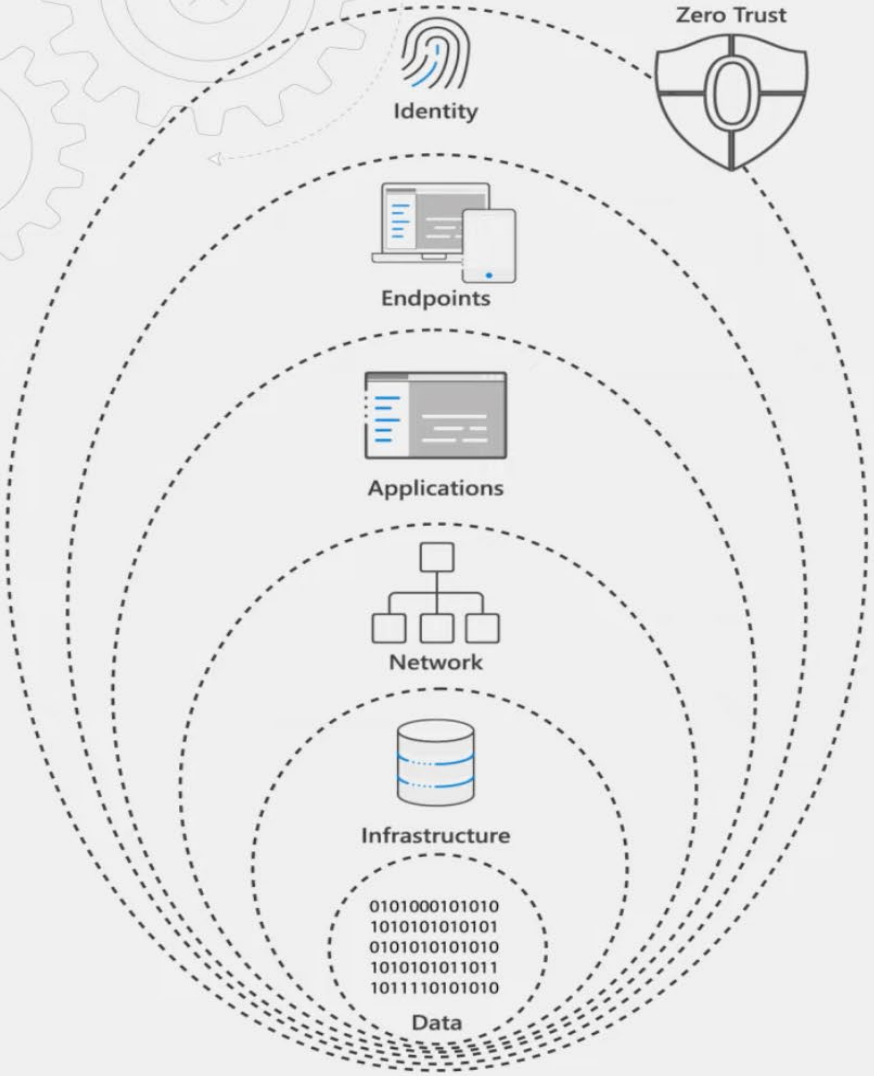
Übersicht über Microsoft 365 Copilot

● Included ▲ Included — Metered

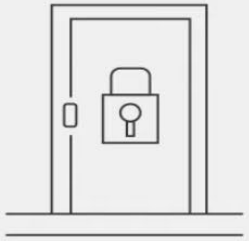
		Microsoft 365 Copilot Chat Free + Consumption	Microsoft 365 Copilot $30 pupm
Chat	Copilot Chat – Web grounded (powered by GPT-4o)	●	●
	Copilot Chat – Work grounded (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)		●
	Copilot Pages	●	●
	File upload[1]	●	●
	Code Interpreter[1]	●	●
	Image generation[1]	●	●
Agents[2]	Create agents using Copilot Studio[3], including SharePoint agents	●	●
	Discover and pin agents	●	●
	Use agents grounded in Web data	●	●
	Use agents grounded in work data (work data in your tenant's Microsoft Graph and 3rd party data via Graph connectors)	▲	●
	Use agents that act independently using autonomous actions	▲	▲
Personal assistant	Copilot reasons over personal work data (e.g., Outlook, OneDrive, Teams meeting transcripts and chats)		●
	Copilot in Teams		●
	Copilot in Outlook		●
	Copilot in Word		●
	Copilot in Excel		●
	Copilot in PowerPoint		●
	Copilot Actions		In preview
	Pre-built M365 agents (Interpreter, Facilitator, Project Manager, Employee Self-Service)		In preview
Copilot Control System	Enterprise Data Protection (EDP)	●	●
	IT management controls	●	●
	Agent management	●	●
	SharePoint Advanced Management		●
	Copilot Analytics to measure usage and adoption[4]		●
	Pre-built reports and advanced analytics to measure ROI		●

1. Limits apply. 2. Applies to employee-facing agents only. 3. Learn more about the full capabilities of Copilot Studio: aka.ms/CopilotStudioCapabilities 4. Basic reporting in Microsoft Admin Center available for Copilot Chat.

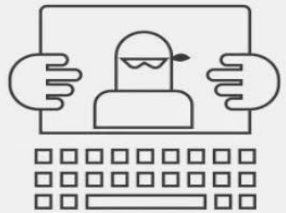
Zero Trust



Verify explicitly



Apply least privileged access



Assume breach

Sicherheitsrisiken bei der Verwendung von Copilot

Sicherer Einsatz von Microsoft 365 Copilot

Copilot als Brandbeschleuniger: Bestehende Risiken werden verstärkt

Grundprinzip

- Copilot findet und nutzt alle Daten, auf die ein Benutzer Zugriff hat – ohne Ausnahme.

Datenchaos als Hauptrisiko

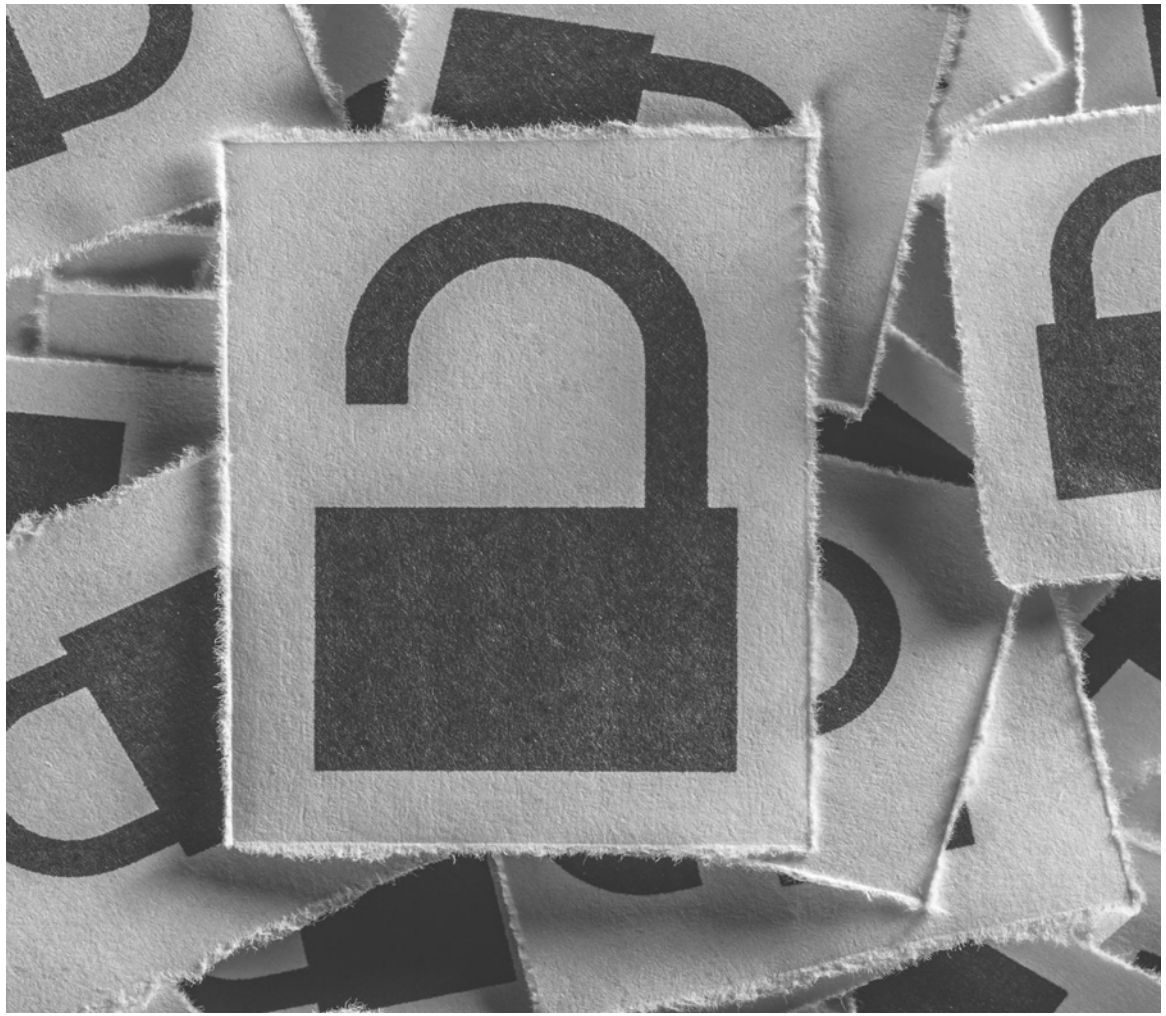
- Veraltete, falsche oder zu weitreichende Berechtigungen sind die größte Schwachstelle. Copilot macht dieses Problem sofort sichtbar.

Unbeabsichtigter Datenabfluss

- Mitarbeiter können versehentlich sensible Informationen in Dokumenten oder Berichten zusammenfassen und teilen.

Gefahr durch Insider

- Ein unachtsamer oder böswilliger Mitarbeiter kann mit Copilot in Sekunden sensible Daten aus verschiedenen Quellen aggregieren, die sonst mühsam gesucht werden müssten.



Sicherer Einsatz von Microsoft 365 Copilot

Externe Angriffe: Ein kompromittiertes Konto wird zum Super-GAU

Angriffsziel Mitarbeiter-Konto

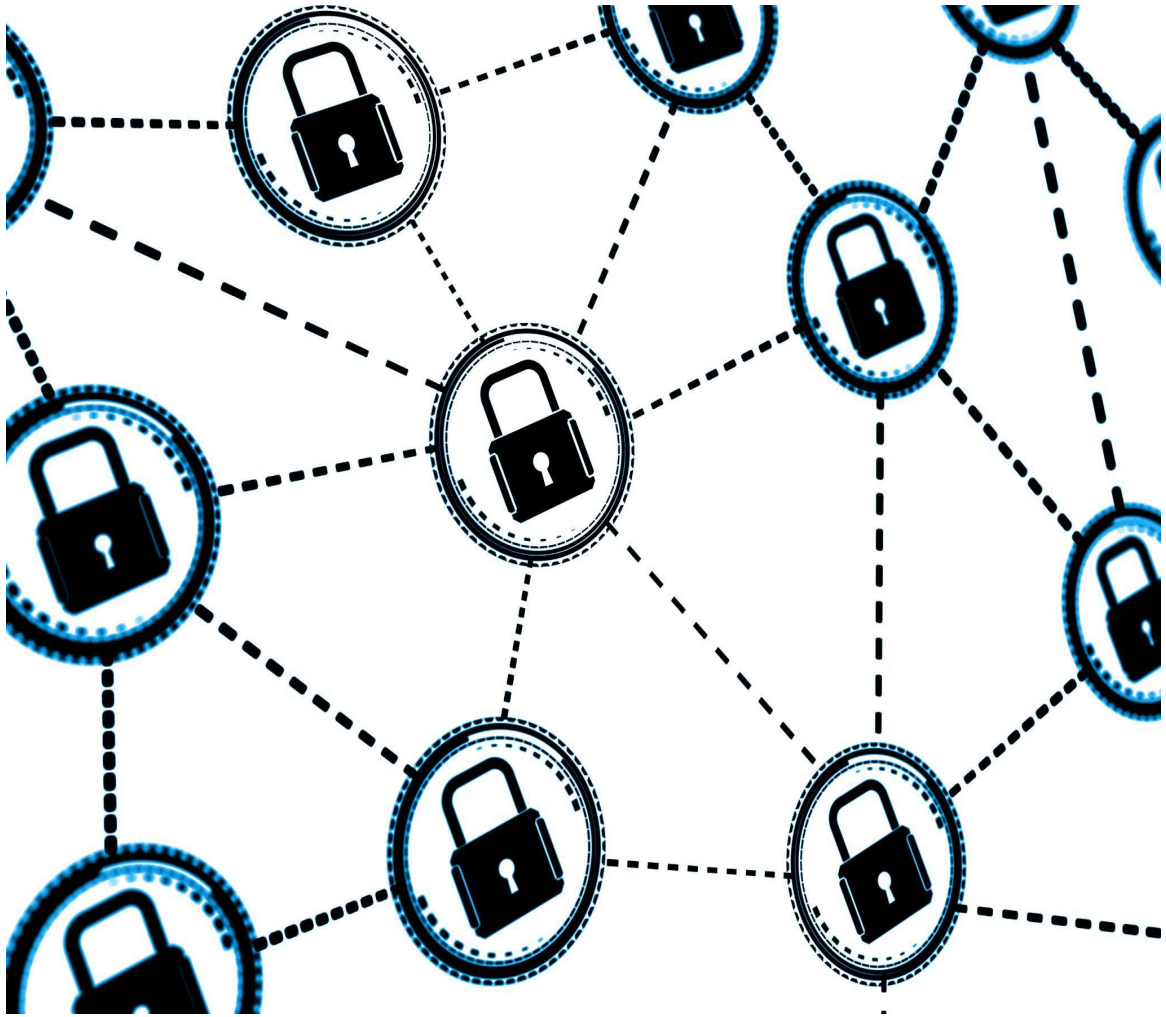
- Externe Angreifer benötigen nur einen erfolgreichen Phishing-Angriff, um vollen Zugriff zu erlangen.

Copilot als Werkzeug für Angreifer

- Nach der Übernahme eines Kontos kann ein Angreifer Copilot nutzen, um gezielt und extrem schnell nach wertvollen Informationen zu suchen (z.B. "Fasse alle Dokumente zu Finanzen und Passwörtern zusammen").

Das Gebot der Stunde

- Ohne flächendeckende Multi-Faktor-Authentifizierung (MFA) wird jedes Benutzerkonto zu einem unkalkulierbaren Risiko für das gesamte Unternehmen.



Strategien zur Risikominderung

Sicherer Einsatz von Microsoft 365 Copilot

controlware

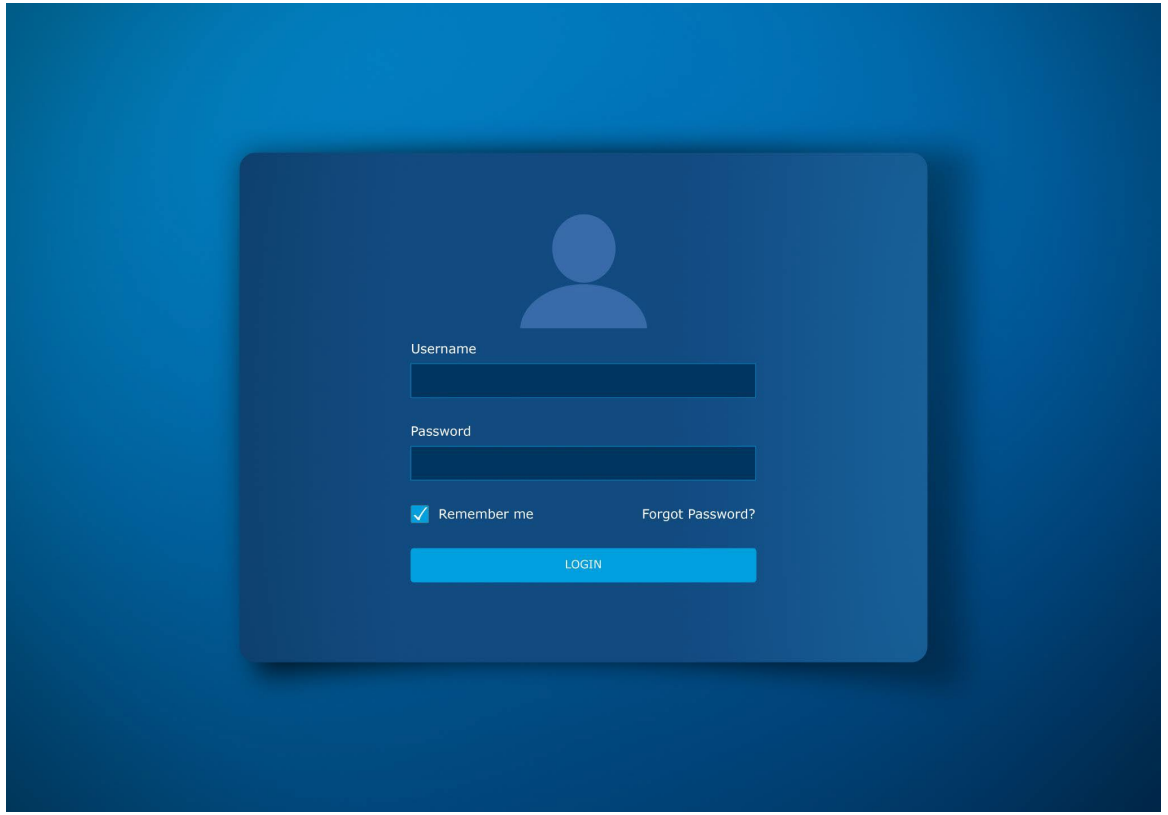
Fundament 1: Identität und Zugriffsrechte unter Kontrolle

Identität kompromisslos sichern (Wer ist der Benutzer?)

- Multi-Faktor-Authentifizierung (MFA): Die nicht verhandelbare Basissicherheit für jedes einzelne Konto.
- Bedingter Zugriff (Conditional Access): Zugriff auf Daten und Copilot nur von bekannten, sicheren Geräten und Standorten erlauben.

Zugriffe konsequent minimieren (Was darf der Benutzer?)

- Least-Privilege-Prinzip: Jeder erhält nur die Berechtigungen, die für seine aktuelle Rolle zwingend notwendig sind.
- Regelmäßige Access Reviews: Etablieren Sie einen "Daten-TÜV" für SharePoint und Teams, um veraltete Zugriffe systematisch zu entfernen.



Sicherer Einsatz von Microsoft 365 Copilot

controlware

Fundament 2: Daten und Endgeräte aktiv schützen

Copilot den "Aktionsradius" klar definieren

- Gezielter Ausschluss: Sperren Sie sensible SharePoint-Bereiche (z.B. Finanzen, Personal, Geschäftsführung) proaktiv für die Indizierung durch Copilot.
- Datenklassifizierung (Purview): Nutzen Sie Vertraulichkeitsbezeichnungen (Sensitivity Labels), um den Zugriff von Copilot auf als "streng vertraulich" markierte Daten zu blockieren.

Endgeräte härten und verwalten

- Umfassender Endpunktschutz (Defender): Verhindern Sie die Kompromittierung von Konten durch robusten Schutz vor Phishing und Malware.
- Zentrales Geräte-Management (Intune): Stellen Sie sicher, dass nur sichere und konforme Geräte auf Unternehmensdaten zugreifen können – inklusive der Möglichkeit zur Remote-Löschung bei Verlust.

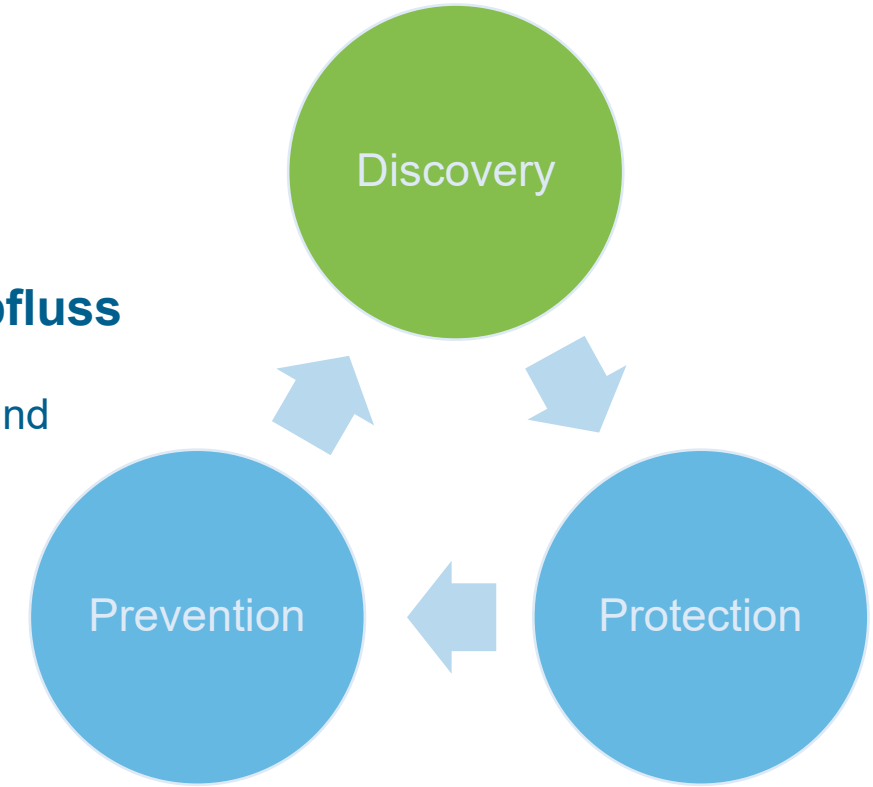
Microsoft 365 Defender Family

Technical Demo
Cloud Discovery

Zero Trust für Data Protection – Discovery, Protection & Prevention

controlware

🔍 **Was wird genutzt?**
Schatten-KI erkennen und Risiken verstehen



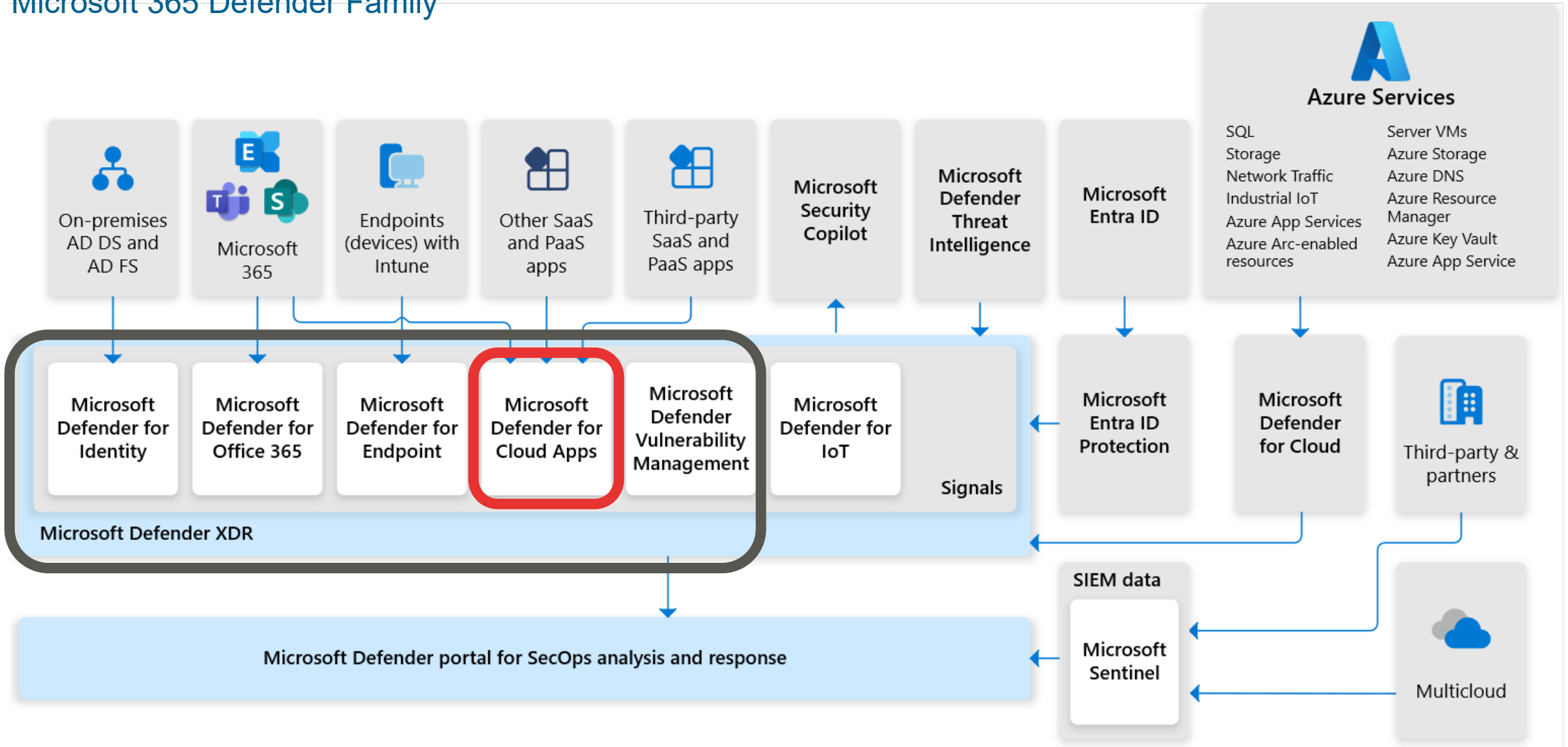
🚫 **Wie verhindern wir den Abfluss sensibler Daten?**
Aktionen am Endgerät überwachen und blockieren

🛡️ **Wie schützen wir sensible Daten?**
Daten klassifizieren, kennzeichnen und kontrollieren

Wie Sie Ihre Daten in der KI-Welt schützen

controlware

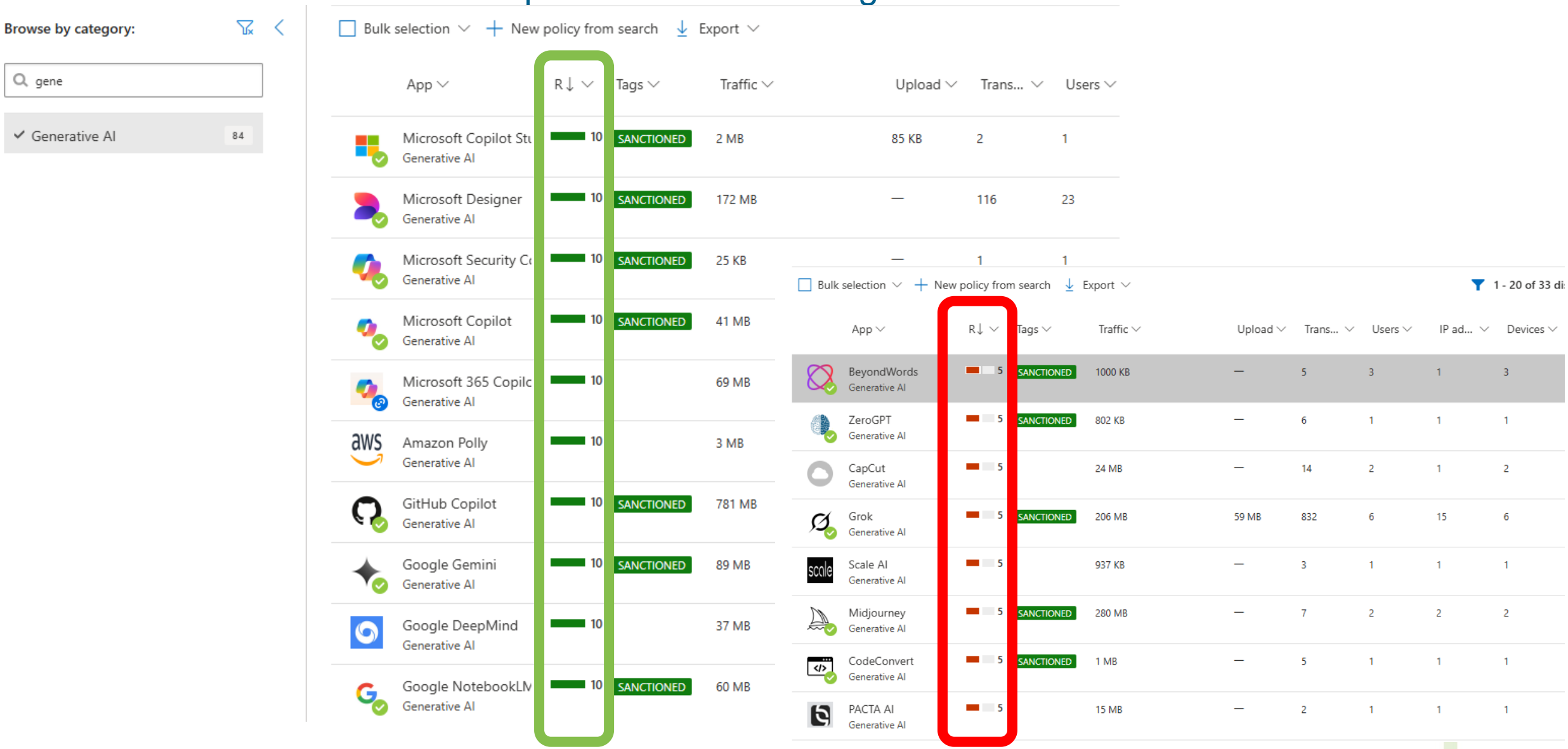
Microsoft 365 Defender Family



Schatten-KI sichtbar machen

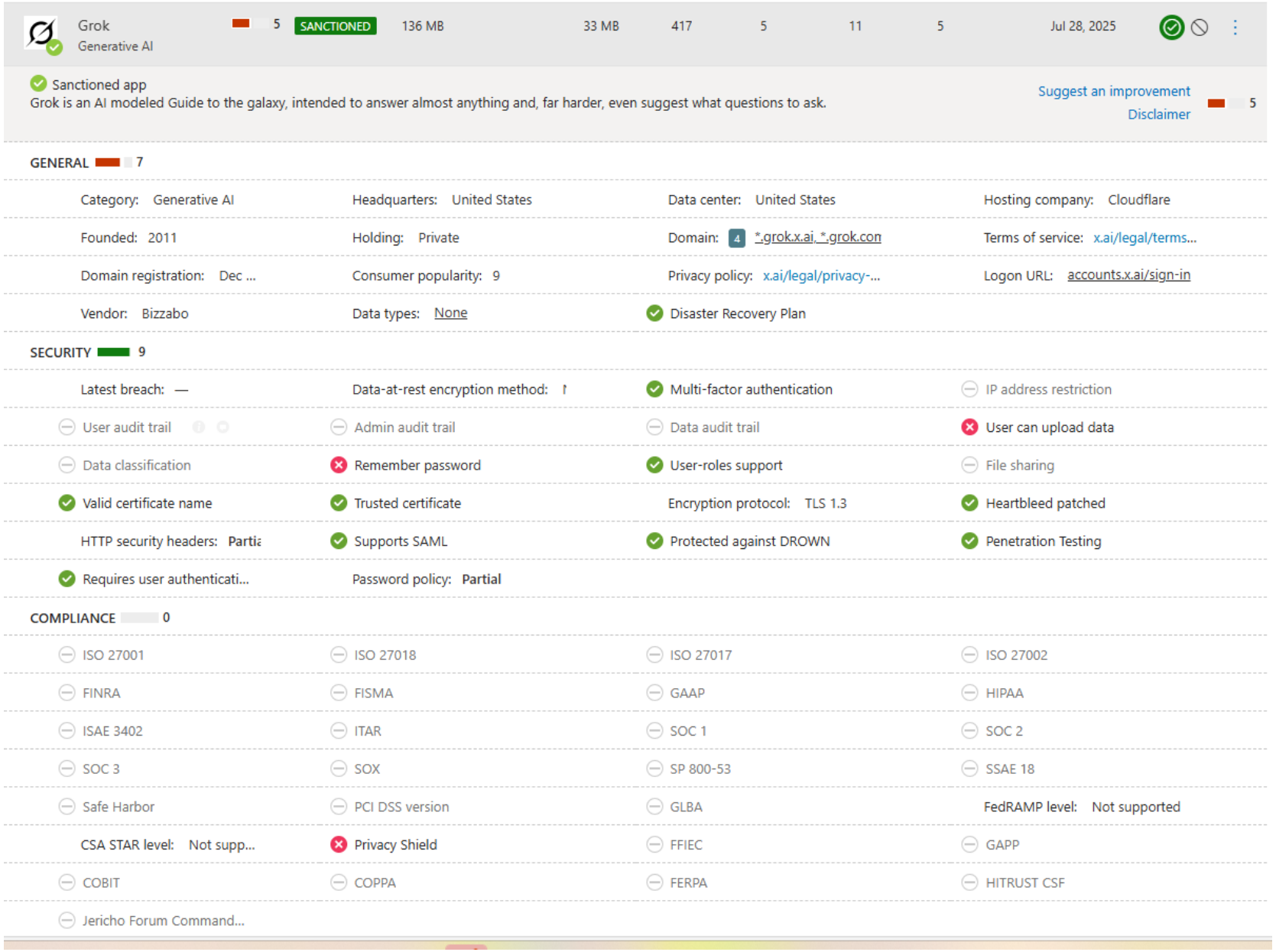
controlware

was passiert in meiner Organisation?



So werden Risikowerte berechnet

controlware



Grok
Generative AI
5 SANCTIONED 136 MB 33 MB 417 5 11 5 Jul 28, 2025

Sanctioned app
Grok is an AI modeled Guide to the galaxy, intended to answer almost anything and, far harder, even suggest what questions to ask.
Suggest an improvement
Disclaimer
5

GENERAL 7

Category: Generative AI	Headquarters: United States	Data center: United States	Hosting company: Cloudflare
Founded: 2011	Holding: Private	Domain: 4 *.grok.x.ai, *.grok.com	Terms of service: x.ai/legal/terms...
Domain registration: Dec ...	Consumer popularity: 9	Privacy policy: x.ai/legal/privacy-...	Logon URL: accounts.x.ai/sign-in
Vendor: Bizzabo	Data types: None	Disaster Recovery Plan	

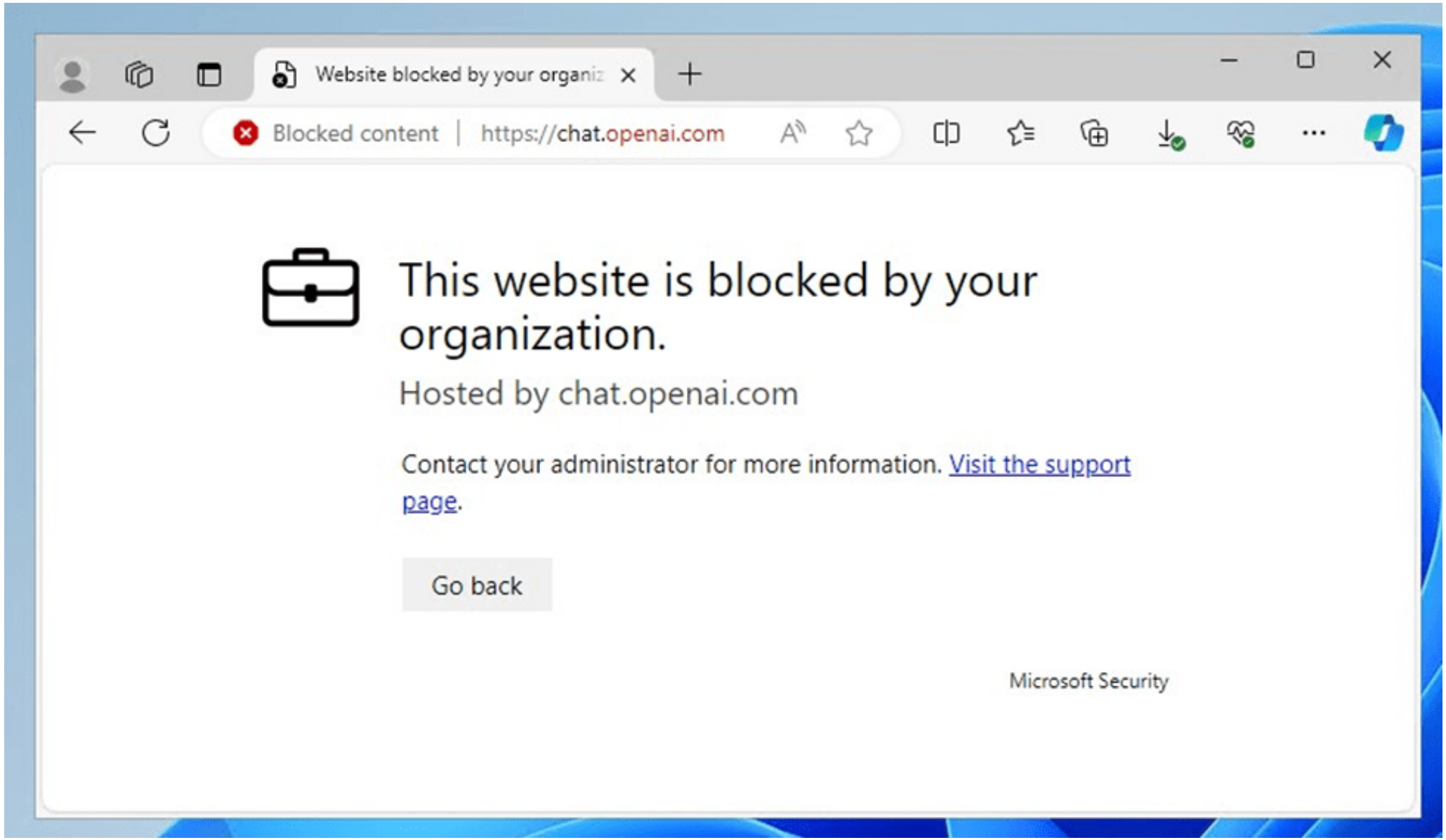
SECURITY 9

Latest breach: —	Data-at-rest encryption method:	Multi-factor authentication	IP address restriction
User audit trail	Admin audit trail	Data audit trail	User can upload data
Data classification	Remember password	User-roles support	File sharing
Valid certificate name	Trusted certificate	Encryption protocol: TLS 1.3	Heartbleed patched
HTTP security headers: Partia	Supports SAML	Protected against DROWN	Penetration Testing
Requires user authenticati...	Password policy: Partial		

COMPLIANCE 0

ISO 27001	ISO 27018	ISO 27017	ISO 27002
FINRA	FISMA	GAAP	HIPAA
ISAE 3402	ITAR	SOC 1	SOC 2
SOC 3	SOX	SP 800-53	SSAE 18
Safe Harbor	PCI DSS version	GLBA	FedRAMP level: Not supported
CSA STAR level: Not supp...	Privacy Shield	FFIEC	GAPP
COBIT	COPPA	FERPA	HITRUST CSF
Jericho Forum Command...			

Nicht genehmigte (unsanctioned) Apps



Datenschutz und Compliance

Sicherer Einsatz von Microsoft 365 Copilot

Leitplanken für Ihre Daten: Proaktiver Schutz mit Purview

Daten verstehen & klassifizieren

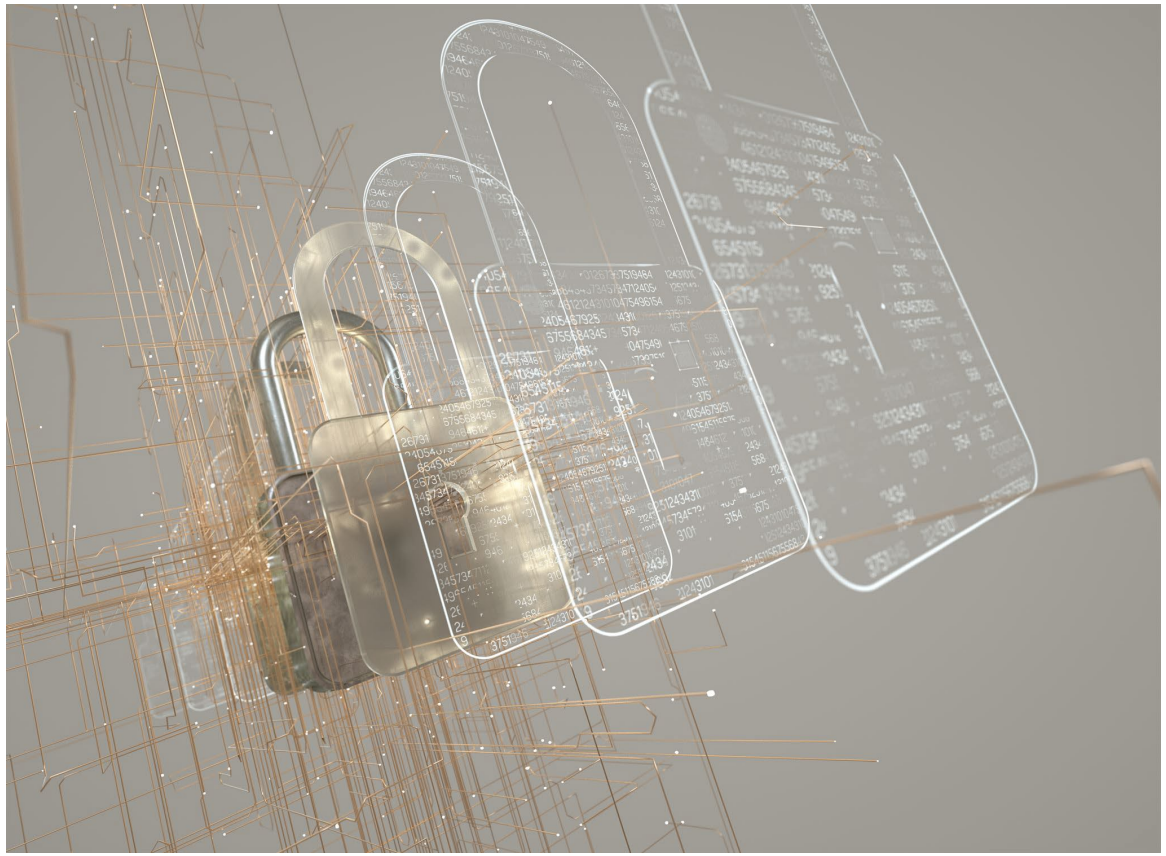
- Definieren Sie eine klare Struktur: Was ist "Öffentlich", "Intern" oder "Streng Vertraulich"? Dies ist die Grundlage für jeden Schutz.

Daten gezielt kennzeichnen (Sensitivity Labels)

- Diese "digitalen Etiketten" sind Ihr wichtigstes Werkzeug.
- Sie steuern den Zugriff, erzwingen automatisch Verschlüsselung und verhindern, dass Copilot als "streng vertraulich" markierte Inhalte überhaupt verarbeitet.

Datenabfluss aktiv verhindern (Data Loss Prevention - DLP)

- DLP ist Ihr "digitales Sicherheitsschloss" am Ausgang des Unternehmens.
- Es erkennt und blockiert basierend auf den Kennzeichnungen aktiv den Versand sensibler Daten – egal ob absichtlich oder versehentlich.



Sicherer Einsatz von Microsoft 365 Copilot

controlware

Sehen, was passiert: Überwachung und schnelle Reaktion

Lückenlose Protokollierung (Audit)

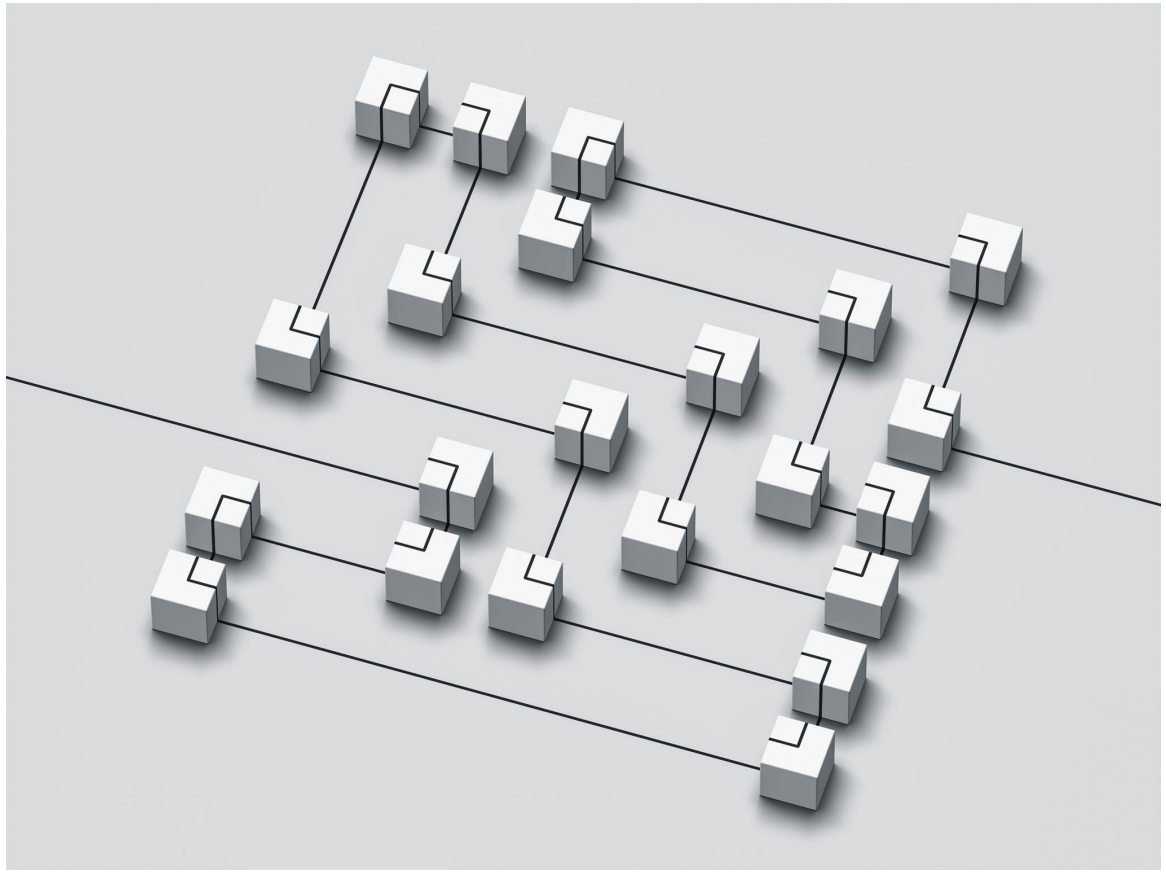
- Jede Copilot-Anfrage wird aufgezeichnet. Das schafft Transparenz und stellt die Nachvollziehbarkeit sicher ("Wer hat was wann gesucht?").

Automatische Alarmierung

- Lassen Sie sich proaktiv über verdächtige Aktivitäten informieren, z.B. wenn ein Benutzer ungewöhnlich viele sensible Daten abruft.

Klarer Notfallplan (Incident Response)

- Legen Sie fest, wer im Ernstfall informiert wird und wie Copilot für einzelne Benutzer oder das ganze Unternehmen schnell deaktiviert werden kann. Nur so bleiben Sie handlungsfähig.

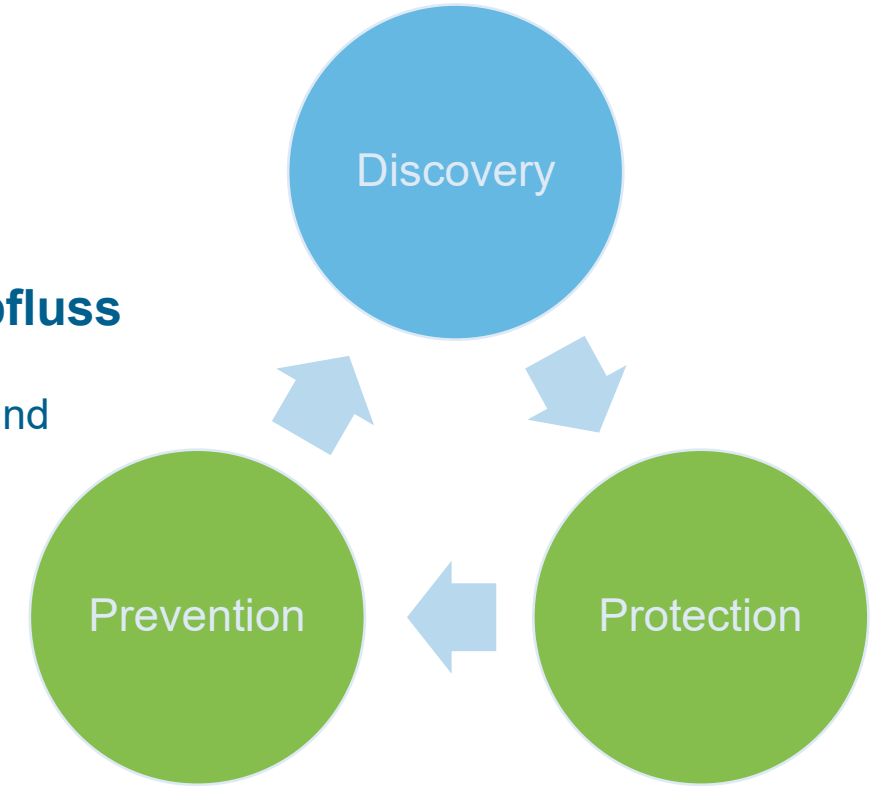


Technische Demo
Protection und Prevention

Zero Trust für Data Protection – Discovery, Protection & Prevention

controlware

🔍 Was wird genutzt?
Schatten-KI erkennen und Risiken verstehen



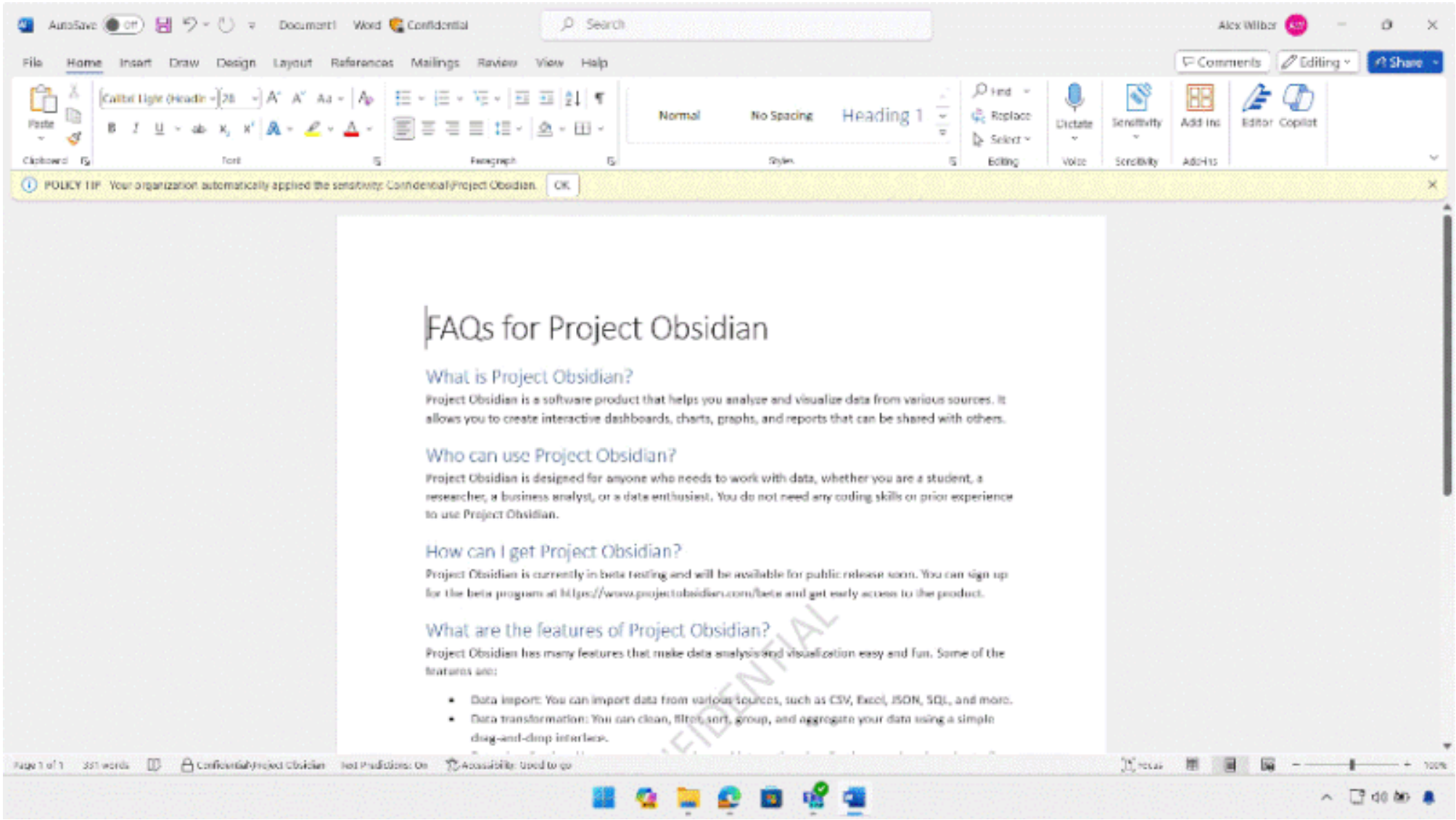
🚫 Wie verhindern wir den Abfluss sensibler Daten?
Aktionen am Endgerät überwachen und blockieren

🛡️ Wie schützen wir sensible Daten?
Daten klassifizieren, kennzeichnen und kontrollieren

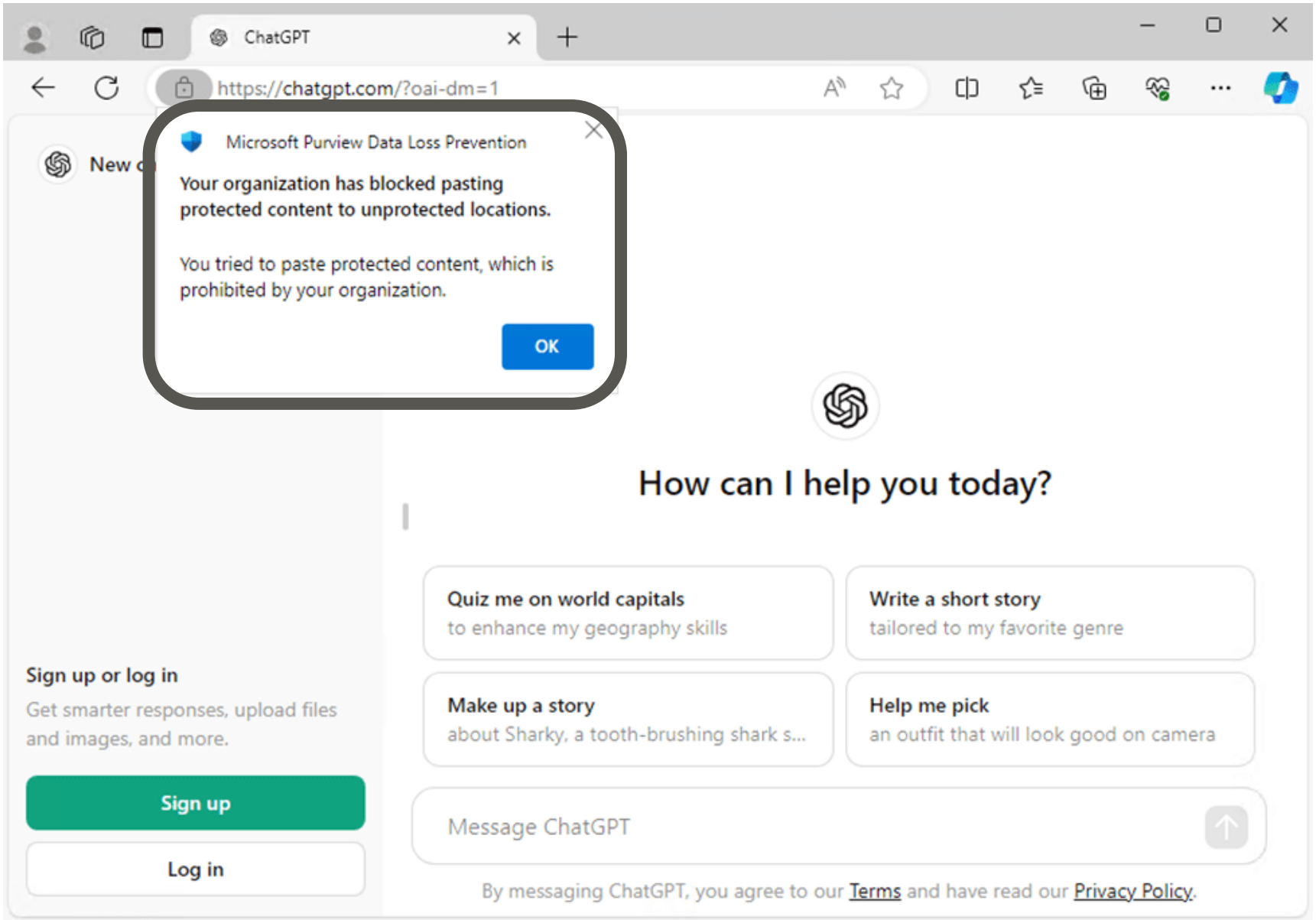
Daten klassifizieren und schützen

controlware

Blockierung von sensiblen Inhalten in KI-Anwendungen

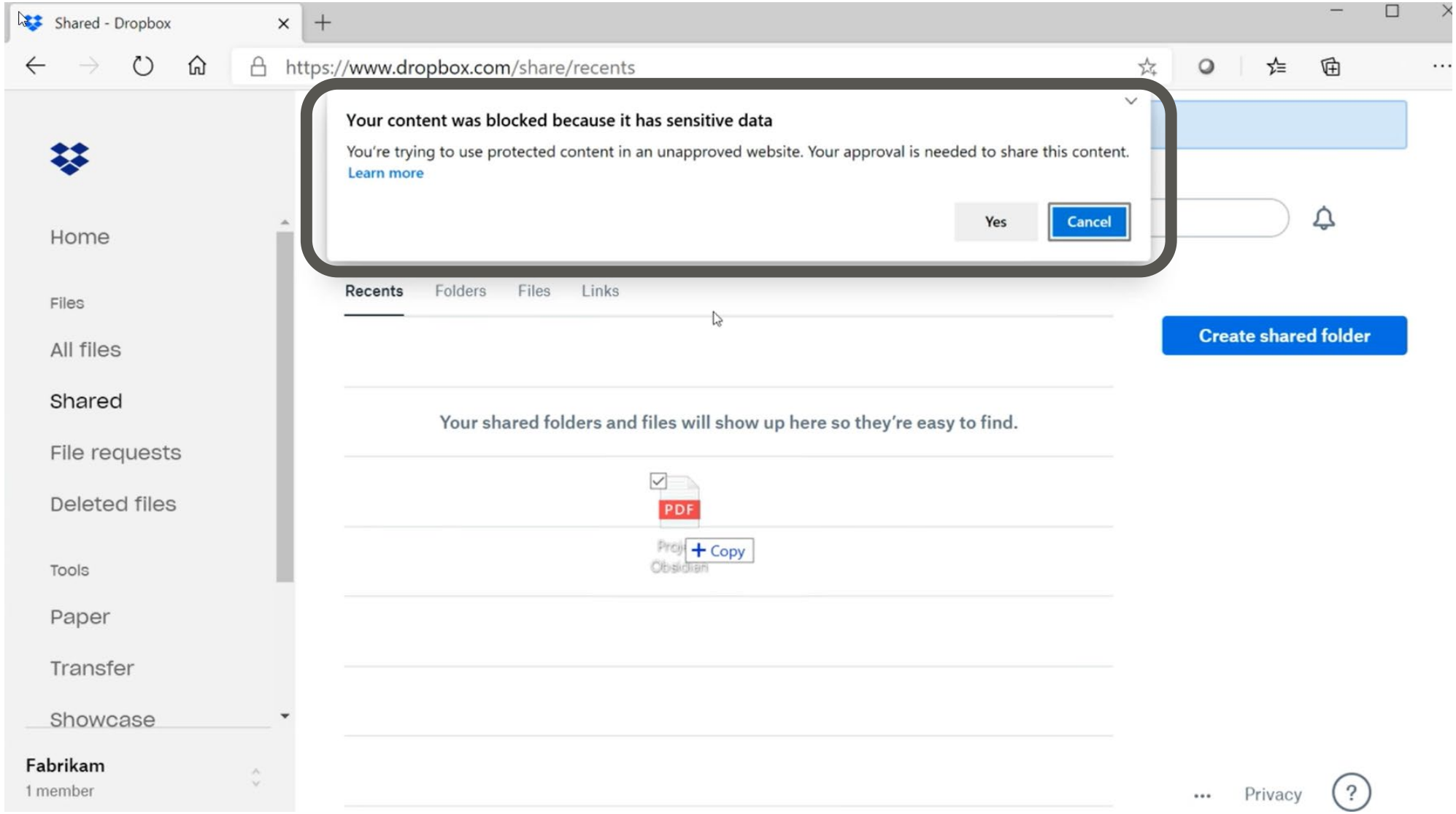


Sensible Daten-Uploads zu AI-Services verhindern



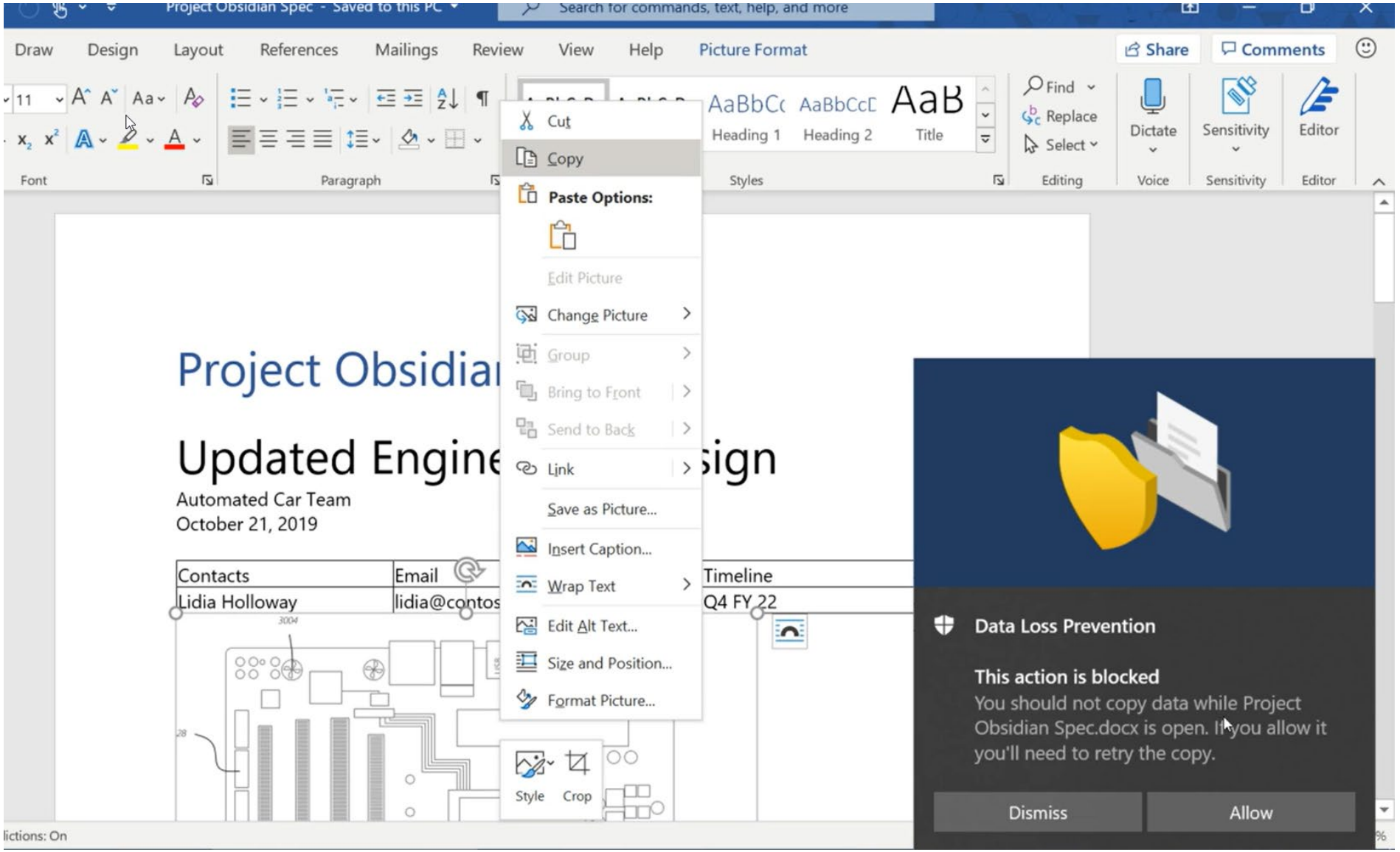
Datenabfluss verhindern

Endpoint DLP – Hochladen von Dateien in Cloudspeicher blockieren



Schutz vor Textkopien aus Projekt „Obsidian“ (Vertraulich)

controlware



Schulung und Sensibilisierung der Benutzer

Sicherer Einsatz von Microsoft 365 Copilot

Der Faktor Mensch: Ihre wichtigste Verteidigungslinie

Technik ist nur die halbe Miete

- Die besten Schutzmaßnahmen sind wirkungslos, wenn Mitarbeiter die Risiken nicht verstehen.

Schulung ist eine Investition, kein Kostenfaktor

- Trainieren Sie den verantwortungsvollen Umgang mit Copilot.
- Schärfen Sie das Bewusstsein für sensible Daten ("Was ist schützenswert?").
- Klären Sie über neue Angriffsvektoren wie "Prompt Injection" auf.

Etablieren Sie eine Sicherheitskultur

- Ein gut informierter Mitarbeiter ist Ihr effektivster Schutz vor unbeabsichtigtem Datenabfluss und der beste Sensor für verdächtige Aktivitäten.

Bleiben Sie über Bedrohungen und Updates auf dem Laufenden

Sicherer Einsatz von Microsoft 365 Copilot

controlware

Sicherheit ist kein Projekt, sondern ein kontinuierlicher Prozess

Die Bedrohungslandschaft entwickelt sich rasant

- Neue Angriffsmethoden auf KI-Systeme entstehen kontinuierlich. Ihre Abwehrstrategie muss anpassungsfähig bleiben.

Nutzen Sie den Microsoft Secure Score als Ihr Cockpit

- Messen Sie objektiv Ihr aktuelles Sicherheitslevel.
- Identifizieren Sie proaktiv Schwachstellen.
- Priorisieren Sie konkrete Handlungsempfehlungen.

Etablieren Sie einen Sicherheits-Zyklus

- Regelmäßige Risikoanalysen, das Einholen von Nutzerfeedback und die Anpassung Ihrer Richtlinien sind entscheidend für dauerhaften Schutz.

Technische Demo
Secure Score

Sicherer Einsatz von Microsoft 365 Copilot

controlware

Microsoft Secure Score

Applied filters:

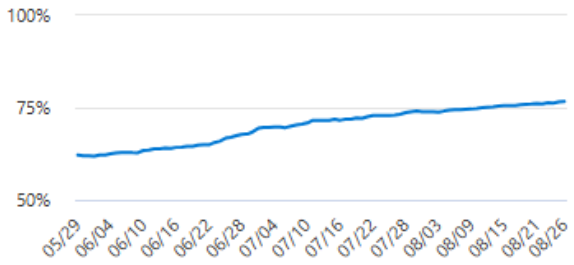
Filter

Your secure score

Include

Secure Score: 76.67%

1121.73/1463 points achieved



Breakdown points by: Category

Identity	83.08%
Data	71.11%
Device	78.16%
Apps	66.79%

Points achieved Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added
12	124	1	2	0

Recently updated: 0

Top recommended actions

Recommended action	Score impact	Status	Category
Block credential stealing from the Windows local security aut...	+0.62%	To address	Device
Secure Microsoft Defender Firewall domain profile	+0.62%	To address	Device
Enable impersonated domain protection	+0.55%	To address	Apps
Set the phishing email level threshold at 2 or higher	+0.55%	To address	Apps
Enable impersonated user protection	+0.55%	To address	Apps
Set User Account Control (UAC) to automatically deny elevati...	+0.55%	To address	Device
Disable the built-in Administrator account	+0.55%	To address	Device
Block process creations originating from PSExec and WMI co...	+0.62%	To address	Device

Comparison

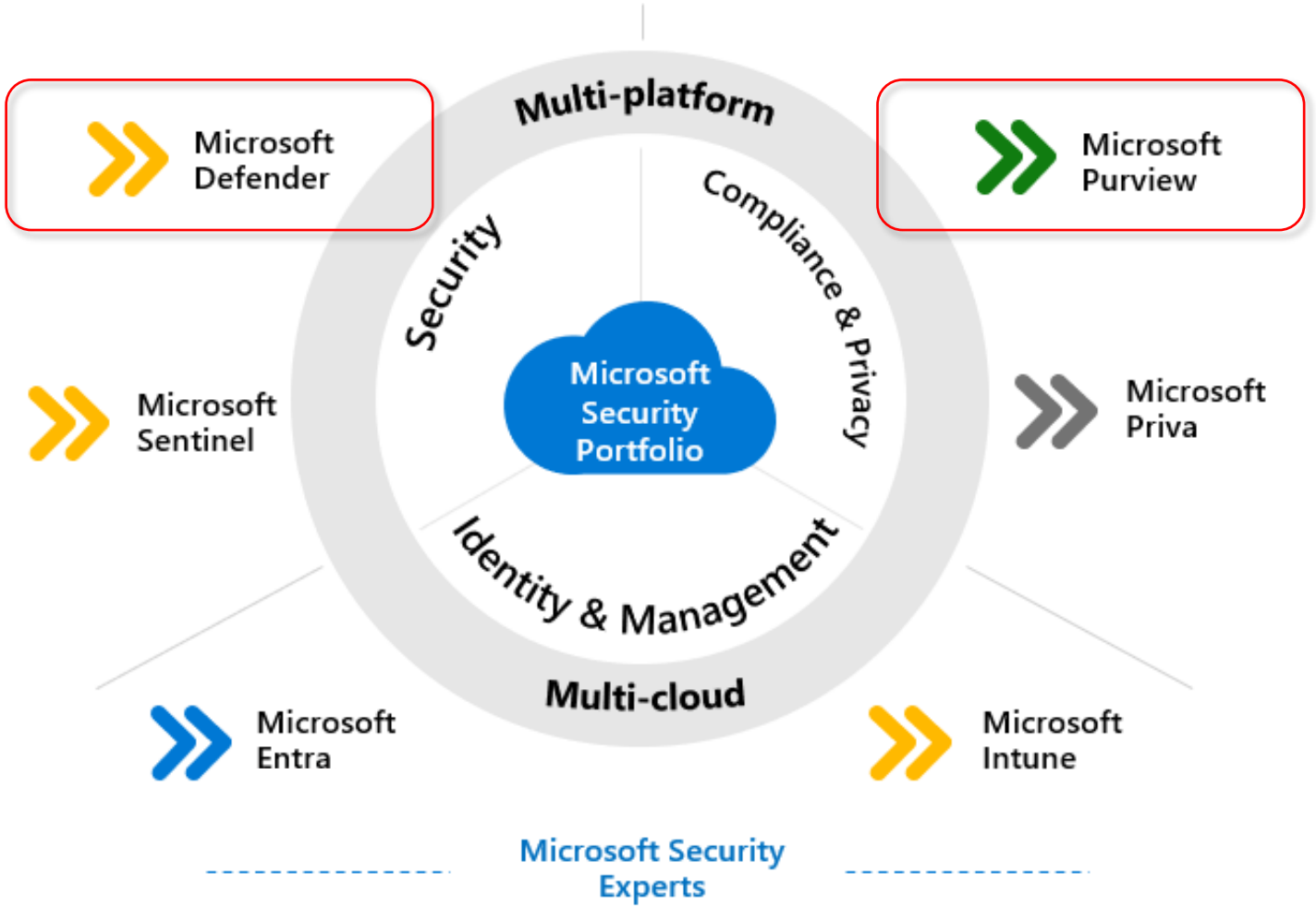
Your score	76.67 / 100
Organizations of a similar size	45.01 / 100

Wie Sie Ihre Daten in der KI-Welt schützen

controlware

Zero Trust layers of protection

1. Data protection
2. Identity and access
3. App protection
4. Device management and protection
5. Threat protection
6. Secure collaboration with Teams
7. User permissions to data



Fazit

Sicherer Einsatz von Microsoft 365 Copilot

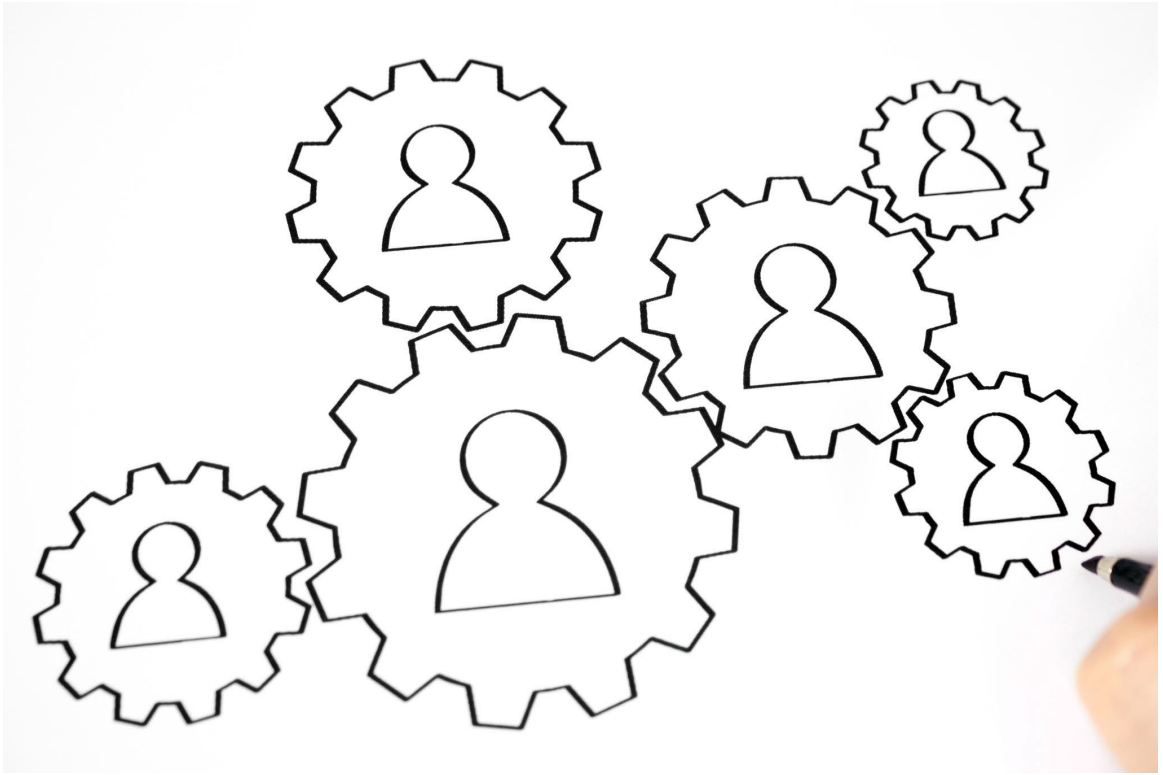
Ihre 4 wichtigsten Handlungsfelder

1. **Identität & Geräte härten**
   - Erzwingen Sie MFA und stellen Sie sicher, dass nur konforme Endgeräte zugelassen sind.

2. **Berechtigungen aufräumen**
   - Setzen Sie das Least-Privilege-Prinzip konsequent durch. Entfernen Sie alle unnötigen Zugriffsrechte.

3. **Daten klassifizieren & schützen**
   - Nutzen Sie die Werkzeuge von Purview (Sensitivity Labels & DLP), um Ihre sensiblen Informationen aktiv zu schützen.

4. **Mitarbeiter befähigen**
   - Machen Sie Ihre Benutzer durch Schulung und klare Richtlinien zu Ihrer stärksten Verteidigungslinie.



Sicherer Einsatz von Microsoft 365 Copilot

controlware

Ihr Fahrplan für einen sicheren Copilot-Einsatz

Copilot ist sicher, aber er nutzt, was er findet

- Die Sicherheit hängt direkt von der Qualität Ihres M365-Fundaments ab.

Ein mehrschichtiger Ansatz (Zero Trust) ist entscheidend

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.