

# Security als Enabler für KI – und nicht als Gegenspieler

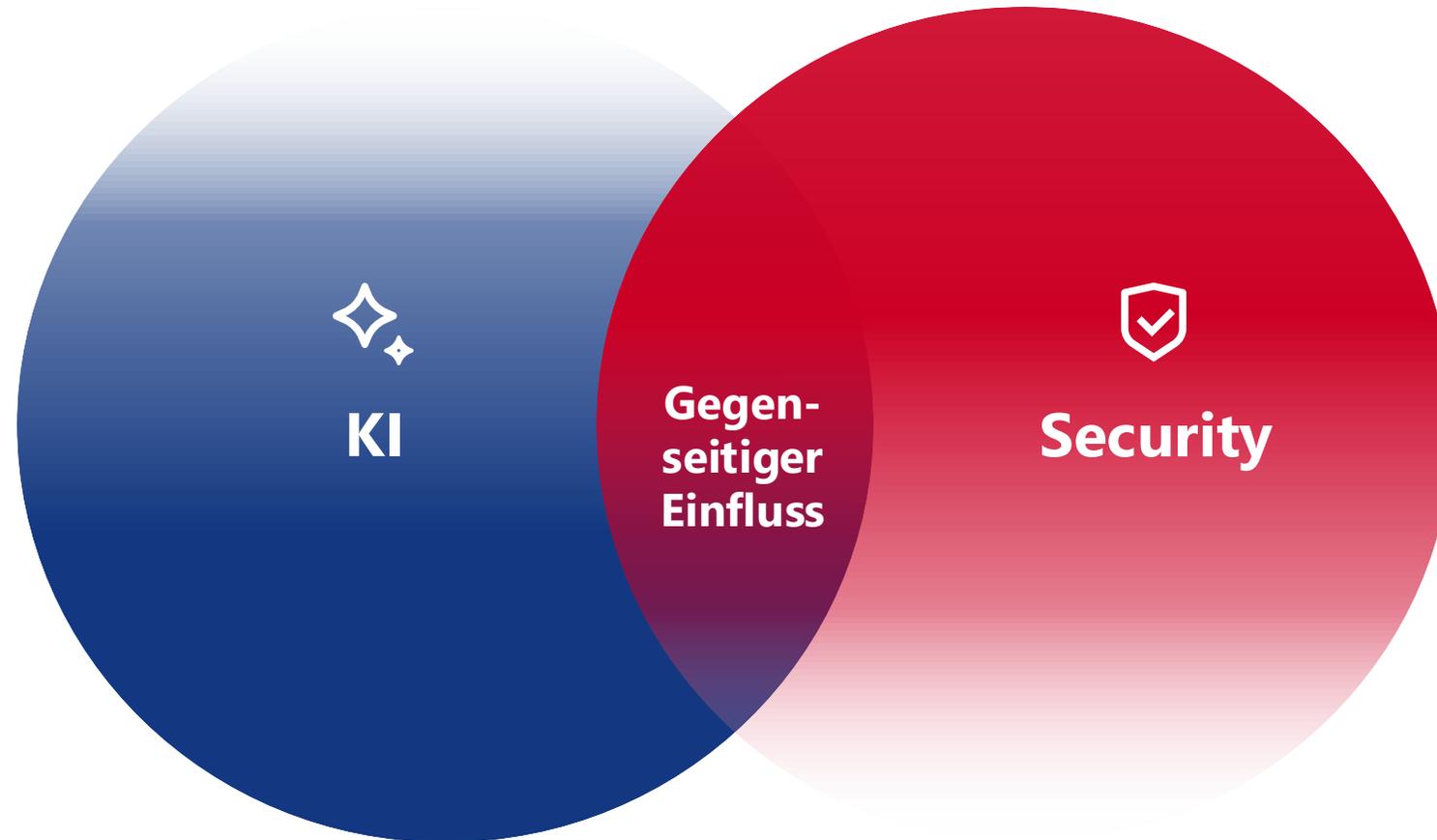
# Hi, ich bin Sebastian

Head of Cloud Security  
& Infrastructure

@novaCapta



# Security & KI im Zusammenspiel



## Unsere Thesen: KI ist Enabler für Security – kein Gegenspieler



Identity



Data



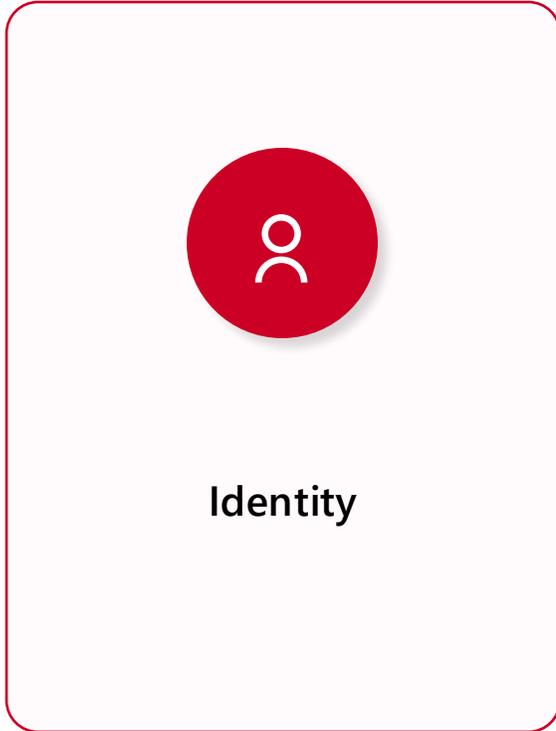
Environment



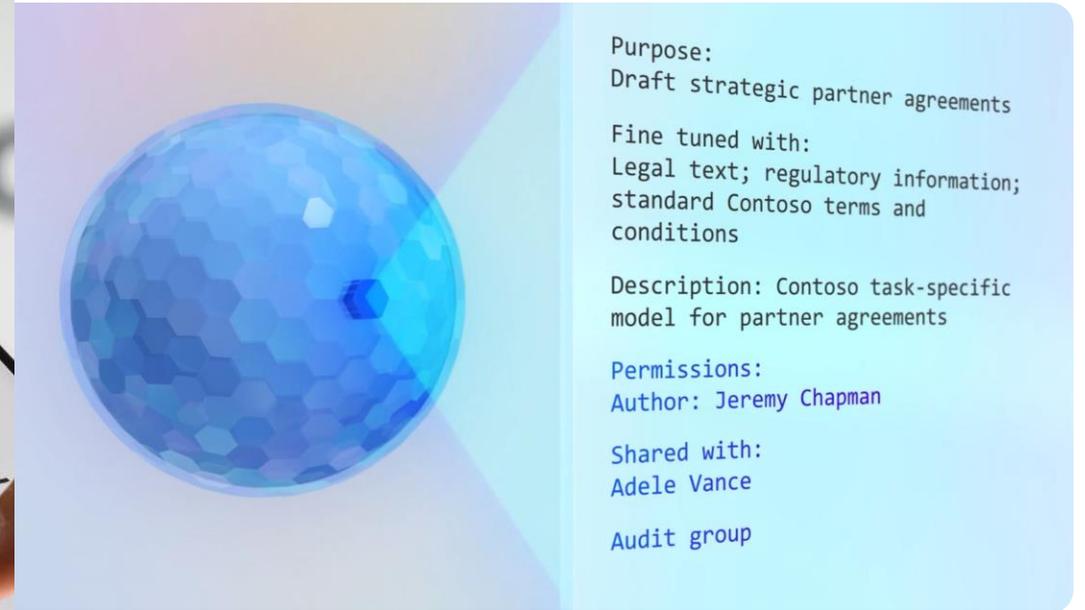
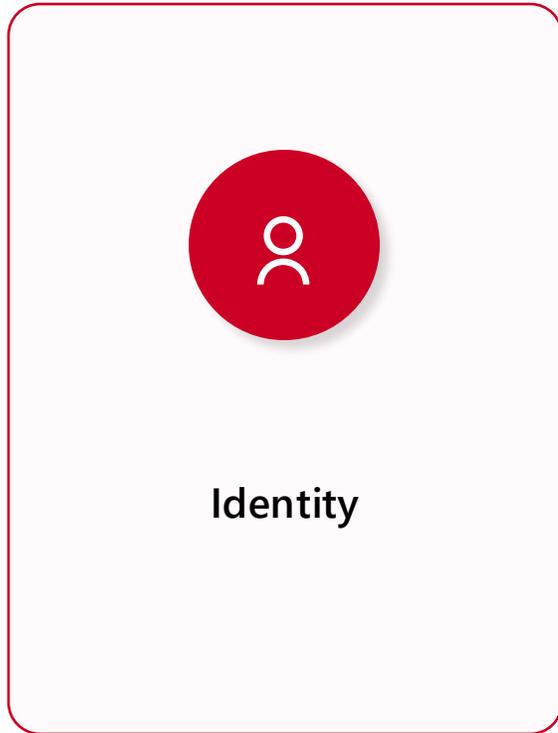
Monitoring

*In diesen elementaren Bereichen stärken sich KI und Security gegenseitig.*

# Unsere Thesen: KI ist Enabler für Security – kein Gegenspieler



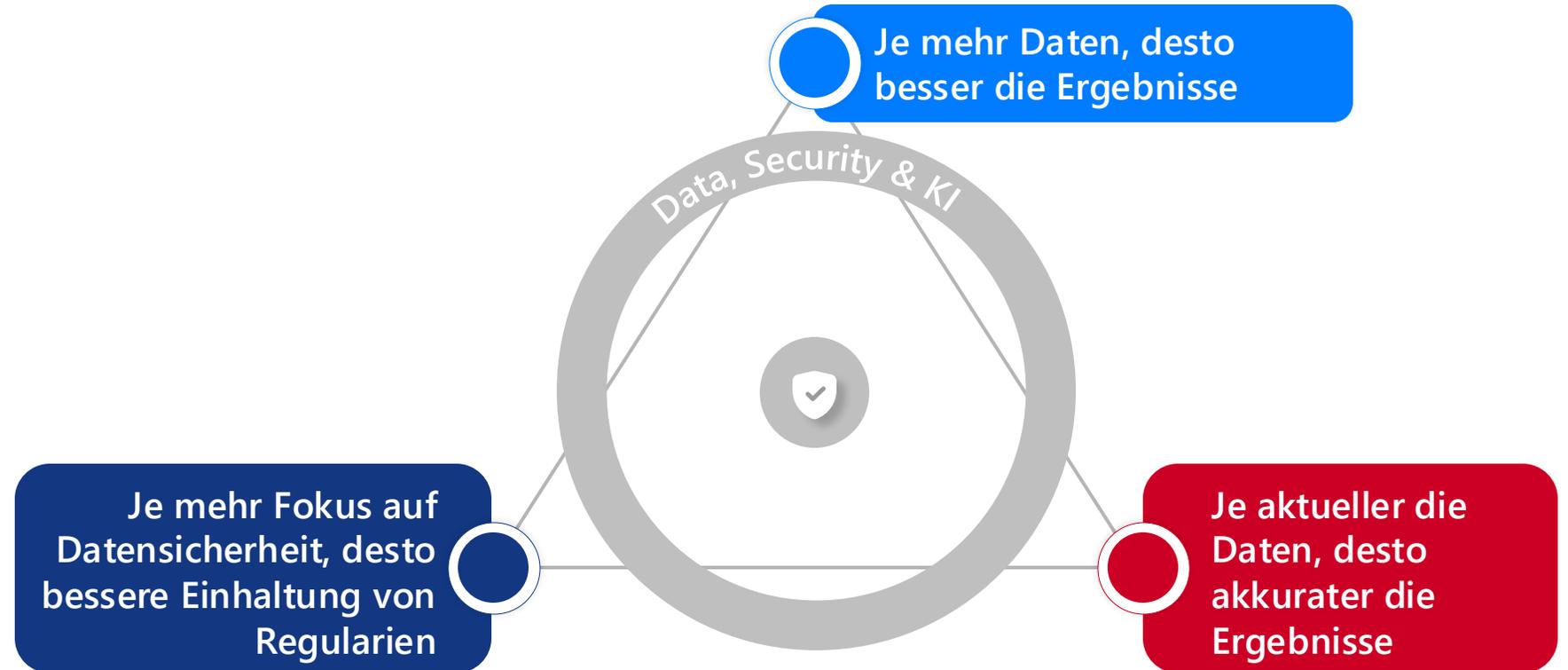
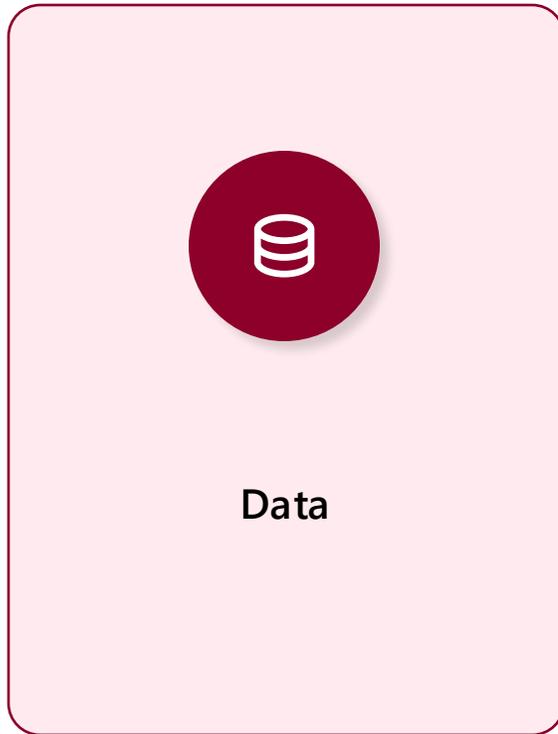
# Unsere Thesen: KI ist Enabler für Security – kein Gegenspieler



## Copilot Tuning = Large-Language-Modelle anpassen

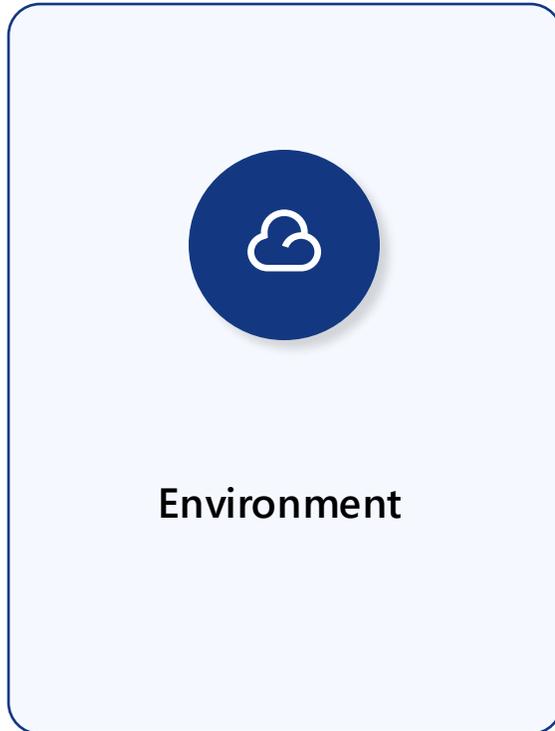
- Für Bestimmte Aufgaben (mit Agents)
- Mit spezifischen Unternehmenskontext
- Für eine bestimmte Gruppe an berechtigten Usern

# Unsere Thesen: KI ist Enabler für Security – kein Gegenspieler



Die "Dreifaltigkeit" von Daten im KI-Zeitalter

# Unsere Thesen: KI ist Enabler für Security – kein Gegenspieler



## Microsoft Entra Agent ID

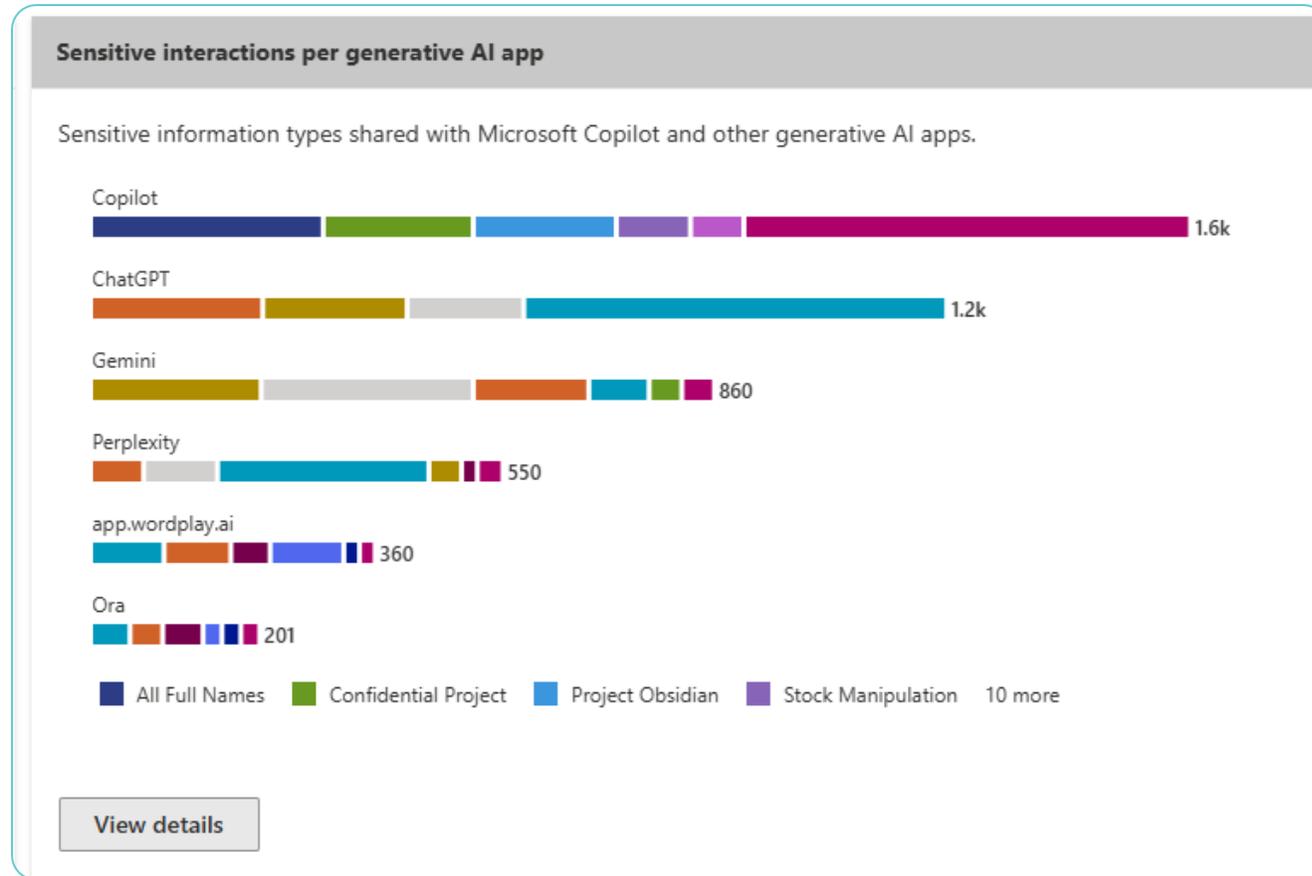
- KI-Agenten verwalten und absichern
- KI-Agenten so handhaben wie menschliche Team-Mitglieder



# Unsere Thesen: KI ist Enabler für Security – kein Gegenspieler

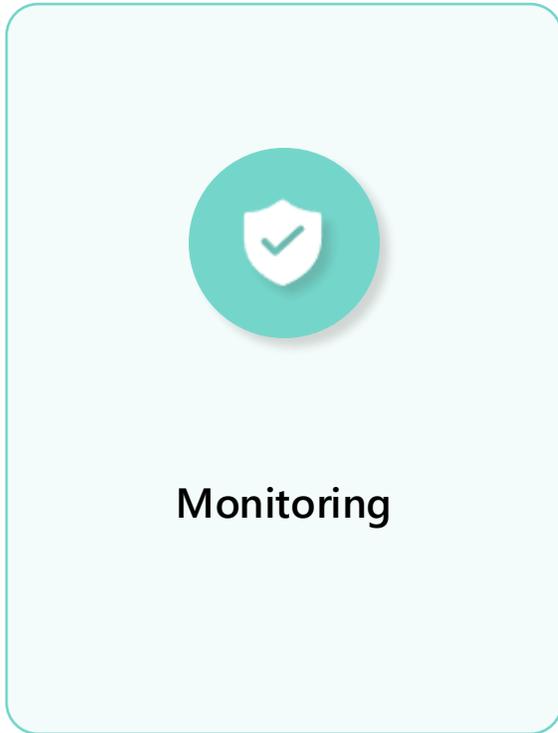


Monitoring



**Herausfinden, wie AI Apps auf Unternehmensdaten zugreifen**  
(Purview Data Security Posture Management)

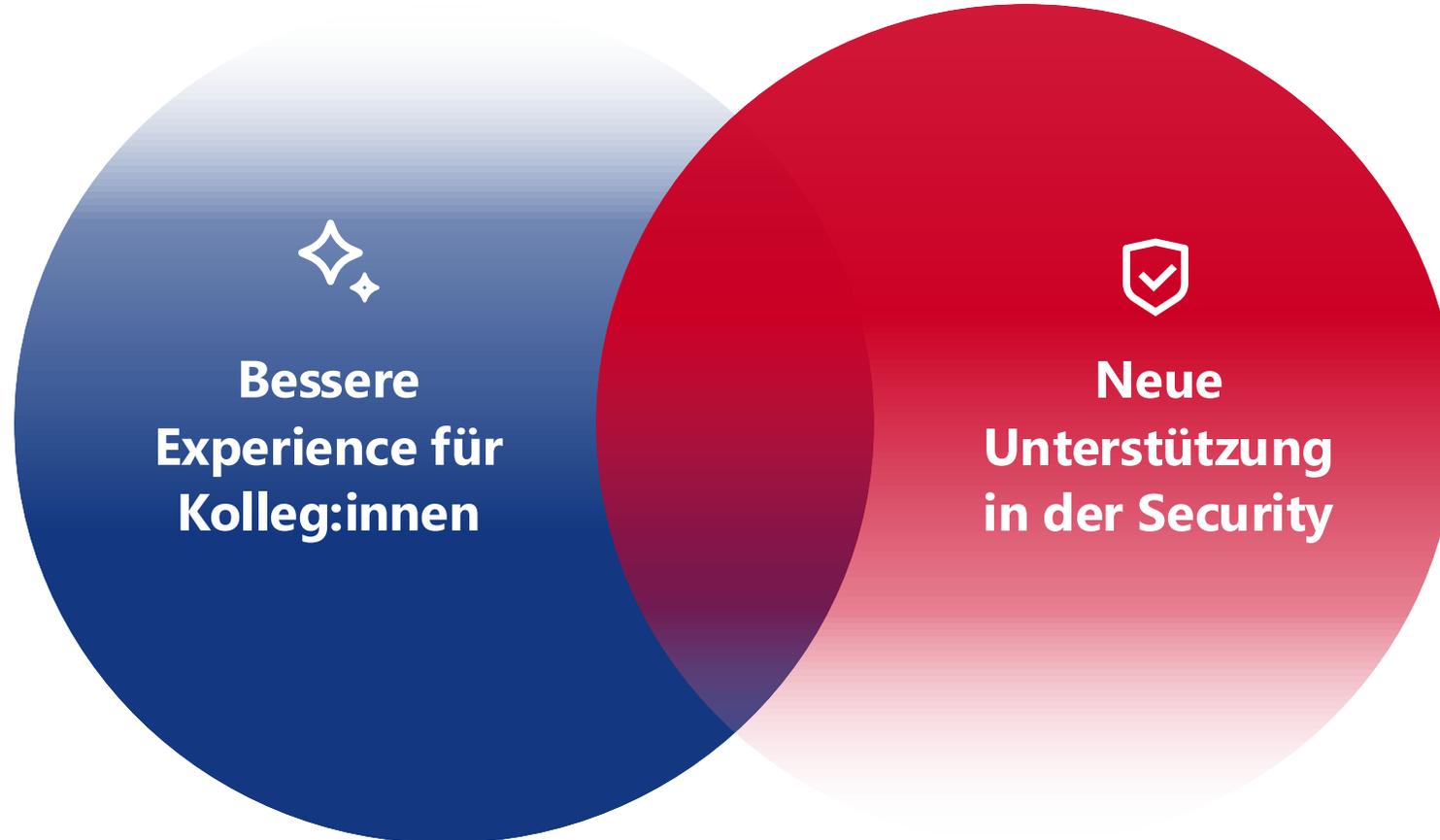
# Unsere Thesen: KI ist Enabler für Security – kein Gegenspieler

A screenshot of the Microsoft Defender Cloud Discovery interface. The page title is "Cloud Discovery" and it shows a list of discovered apps. The interface includes a search bar, filters for app tags and risk scores, and a table of app details. The table columns include App, Risk score, Tags, Traffic, Upload, Transa..., Users, IP add..., Last s..., and Actions. The table lists several AI apps with their respective risk scores and actions.

App	Risk score	Tags	Traffic	Upload	Transa...	Users	IP add...	Last s...	Actions
Microsoft Bing Chat Generative AI	10		20 MB	6 MB	167	142	120	Jan 14, 2024	⊙ ⊗ ⋮
Google Gemini Generative AI	10		2 MB	447 KB	13	13	11	Jan 14, 2024	⊙ ⊗ ⋮
OpenAI ChatGPT Generative AI	9		18 MB	5 MB	151	131	100	Jan 14, 2024	⊙ ⊗ ⋮
Soundful Generative AI	5		3 MB	962 KB	28	28	21	Jan 14, 2024	⊙ ⊗ ⋮
Nichess Generative AI	5		2 MB	550 KB	16	16	9	Jan 14, 2024	⊙ ⊗ ⋮
Framework Generative AI	3	UNSANCTIONED	2 MB	481 KB	14	14	9	Jan 14, 2024	⊙ ⊗ ⊛ ⋮

**AI Apps in der Umgebung einsehen und blockieren**  
(Defender for Cloud Apps)

# KI im Unternehmenskontext: Vorteile für User und IT



# KI im Unternehmenskontext: Vorteile für User und IT



***Bessere Experience  
für Kolleg:innen***



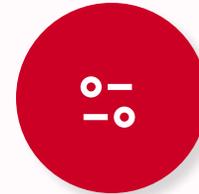
***Neue Unterstützung  
für Security***



**GenAI in täglichen  
Aufgaben nutzen**



**Neue Art des  
Data Labeling**



**Controls**



**Copilot for Security**

SEBASTIAN NIPP

# Ich hoffe, Sie konnten heute etwas für Ihr Unternehmen mitnehmen

Jetzt scannen für weitere Informationen & Kontakt



**Wenn Sie noch Fragen haben:**

Ich bin heute noch länger vor Ort und natürlich auch im Nachgang erreichbar 😊.



# Vielen Dank!

**novaCapta GmbH**

[www.novacapta.de](http://www.novacapta.de)

**novaCapta Schweiz AG**

[www.novacapta.ch](http://www.novacapta.ch)