AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

IT-Security Deep Dive

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security

Jonas Kugler
Senior Security Engineer,
AVANTEC

Agenda

AVANTEC
Competence. Security. Trust.

- Welche Gefahren und Risiken bringt AI?
- Die Zscaler AI Security Platform
- User-Zugriff auf Public AIs – geschützt mit Zscaler
- Ausblick

Welche Gefahren und Risiken bringt AI?

AI in den News

AVANTEC

Claude-Code-Vorfall: npm-Paketierungsfehler wird für Malware-Kampagne über GitHub genutzt

8. April 2026

Ein Fehler im npm-Release von Claude Code dient weiterhin als Ausgangspunkt für eine laufende Malware-Kampagne. IT-Sicherheitsexperten von Trend Micro beobachten die Aktivitäten und analysieren die Vorgehensweise der Angreifer.

BREAKING | BUSINESS

Samsung Bans ChatGP
Sensitive Code Leak

BUSINESS INSIDER

+5.88% MSFT +1.67% TSLA +0.2% AMZN +3.32% META +2.21% DOW -0.16% NASDAQ

Airline held liable for its chatbot giving passenger bad advice - what this means for travellers

23 February 2024

Share Save Add as preferred on Google

dded an AI chatbot to its site. Then all

r Correspondent covering technology and culture

CYBERSECURITY | SECURITY NEWSWIRE | CYBERSECURITY NEWS

Vercel Breach Originated From an Employee's AI Tool

By Jordyn Alger, Managing Editor

AI coding tool wipes production database, fabricates 4,000 users, and lies to cover its tracks

Published: 21 July 2025 · Last updated: 23 July 2025

Welche Gefahren und Risiken bringt AI?

AVANTEC
Competence. Security. Trust.

- Verlust von Kontrolle und Visibilität
- Datenabfluss
  - PII (Personally Identifiable Information)
  - Vertrauliche Firmendaten / Geschäftsgeheimnisse
- Rufschädigung
- Klagen und/oder Bussen
- Fehlverhalten / Mangelnde Datenqualität

Die Zscaler AI Security Platform

Eine Übersicht

AVANTEC
Competence. Security. Trust.

AI Discovery and Risk

Ermöglicht das Entdecken und Klassifizieren von AI Assests und das Analysieren von Risiken.

- GenAI Security Report
- Prompt Logging
- DLP Monitoring für AI

AI Red Teaming

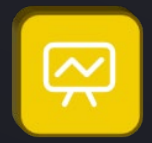
Ermöglicht fortlaufendes Testing eigener AI-Applikationen und gibt Empfehlungen um Vulnerabilitäten zu mitigieren.

- Einfaches Risiko-Assesment
- Vordefinierte + Custom Probes und Prompts
- Vielfältige Input-Methoden

AI Guardrails

Ermöglicht das Überwachen von AI Flows, um ungewollte Prompts und Antworten zu blockieren und unerwünschten Datenabfluss zu verhindern.

- Proxy Mode (inline) oder DAS Mode (via API)
- Schutz von Usern wie auch AI-Applikationen/-Agents
- Vielzahl an Detektoren



AI Governance and Compliance

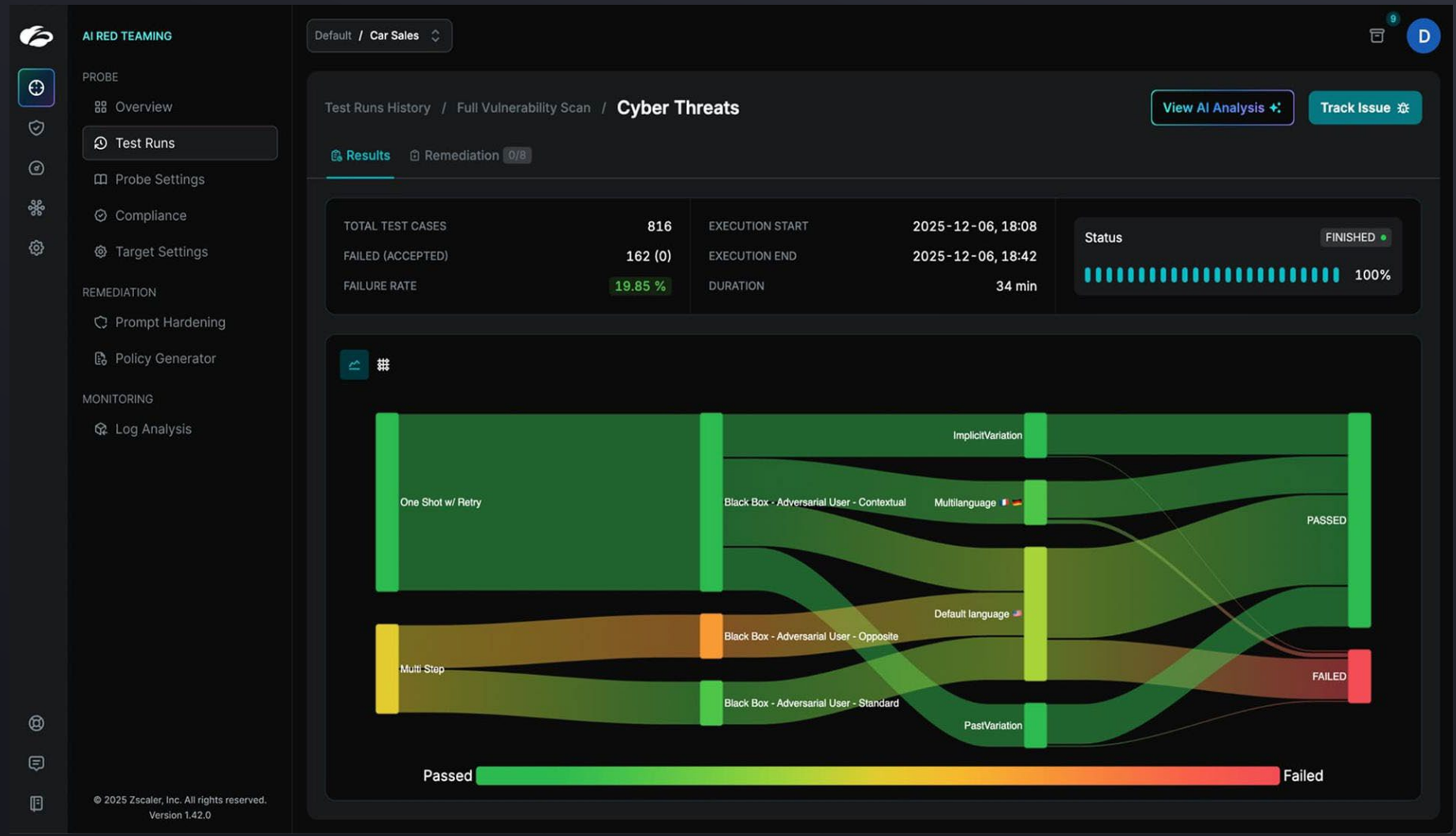
Erlaubt das Überwachen von AI Systemen und das Prüfen, ob diese compliant sind mit entsprechenden AI-Frameworks.

- Alerting zu Issues
- Visualisierung von Abhängigkeiten
- Vordefinierte + Custom Security Policies

Die Zscaler AI Security Platform

AI Red Teaming

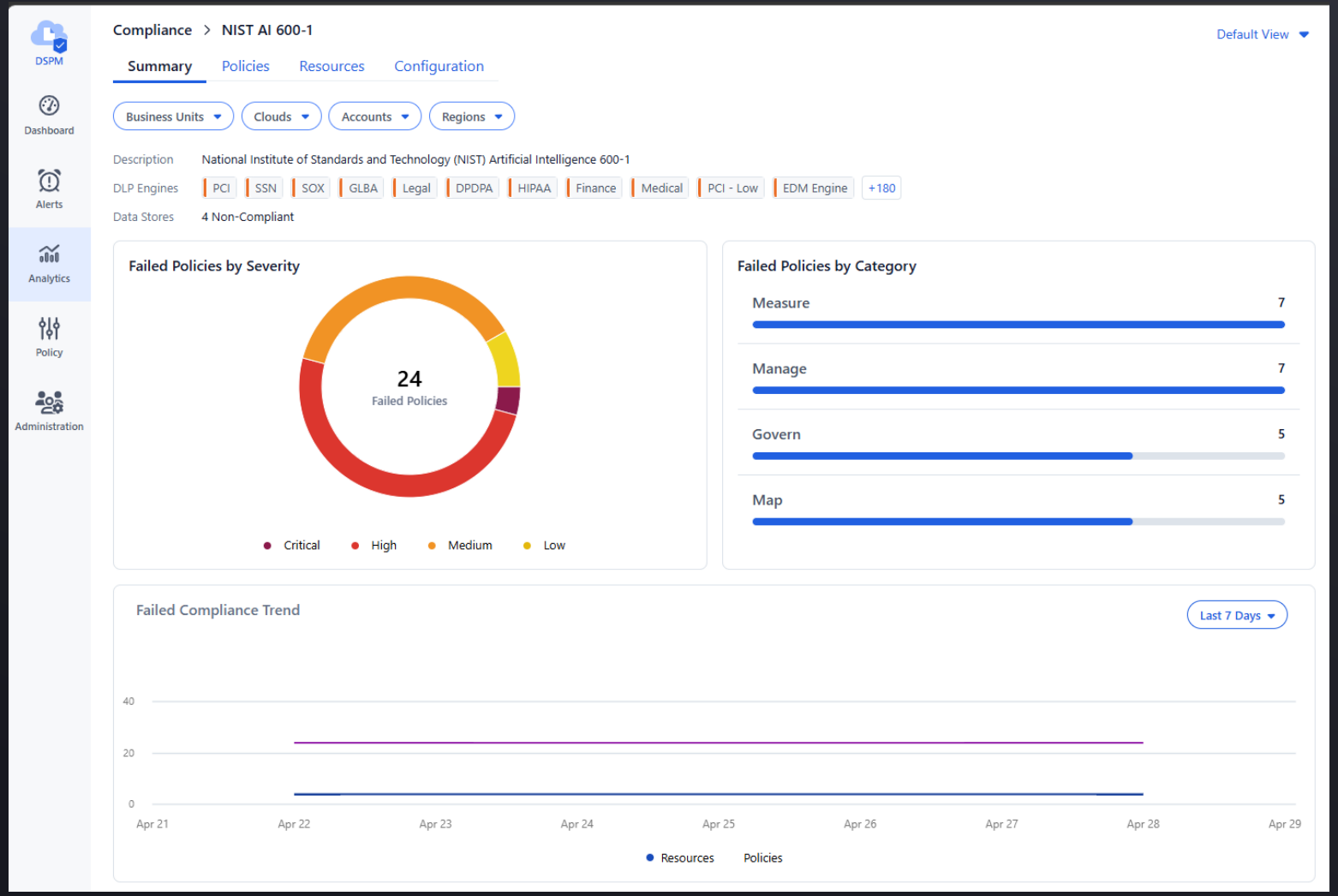
AVANTEC
Competence. Security. Trust.



Die Zscaler AI Security Platform

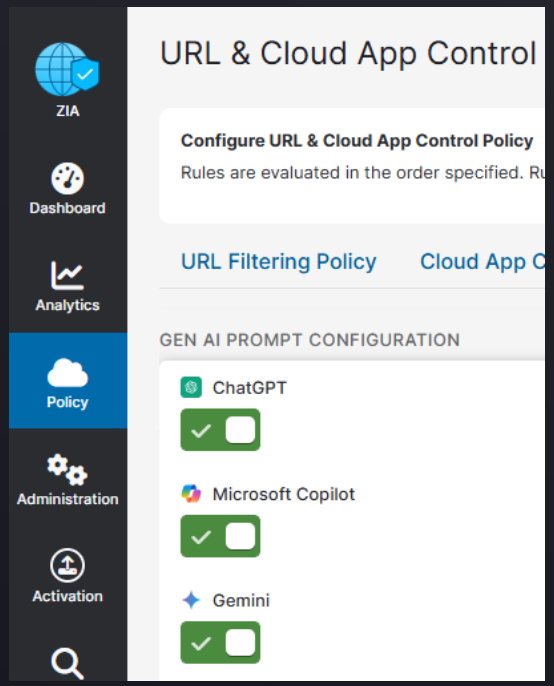
AI Governance and Compliance – DSPM / AI-SPM

AVANTEC
Competence. Security. Trust.

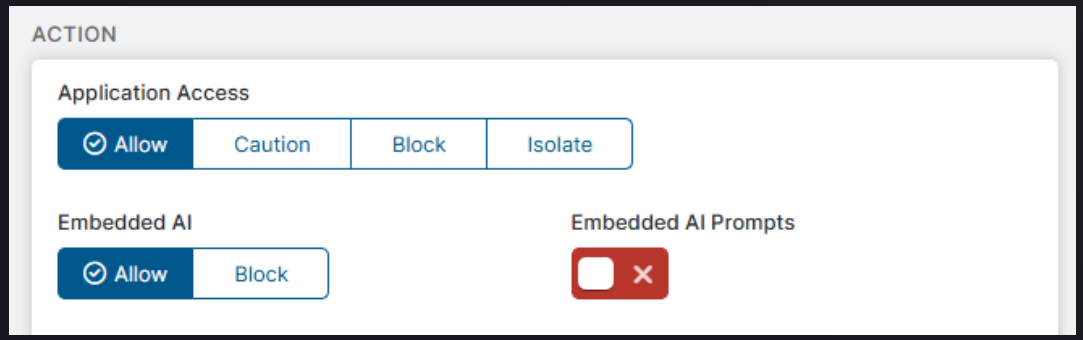


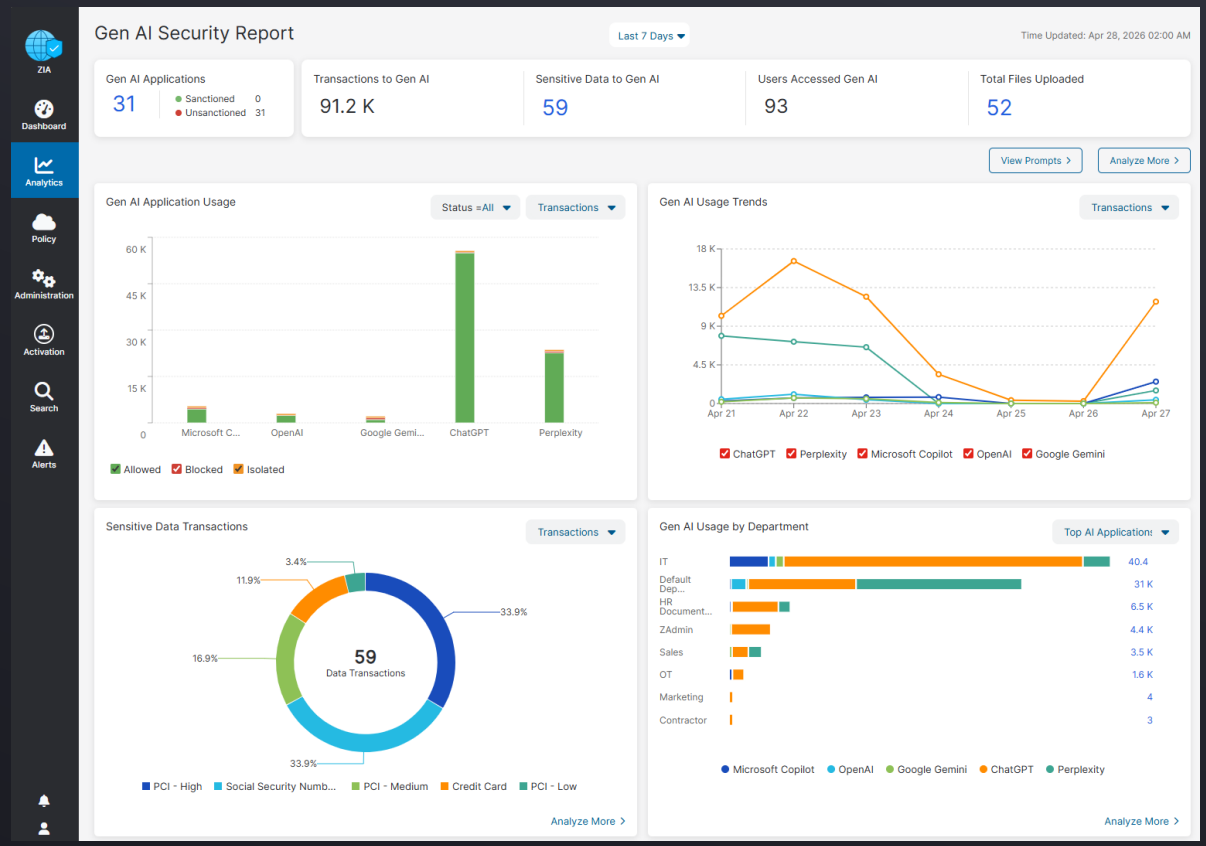
Die Zscaler AI Security Platform

AI Discovery and Risk



ChatGPT
Microsoft Copilot
Gemini
Perplexity
Poe
WRITER
DeepSeek
Grok AI
Claude
Mistal
Grammarly



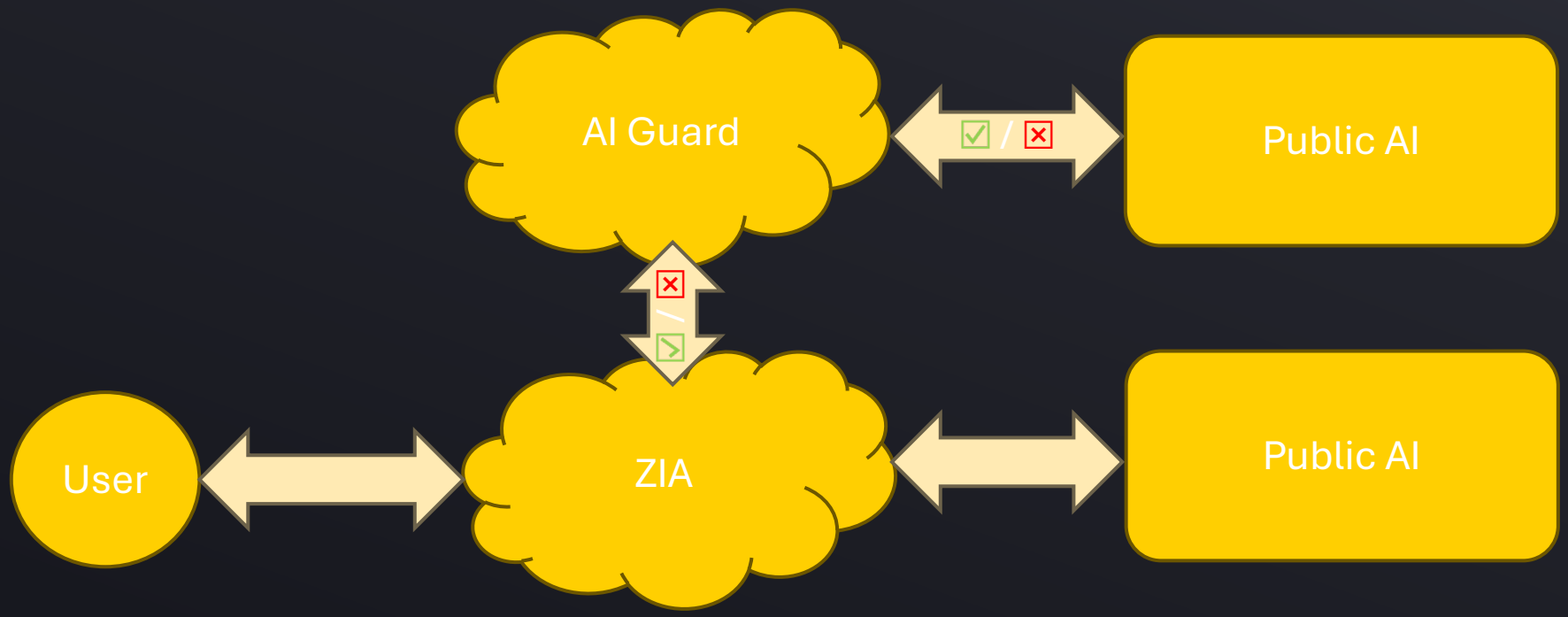


Die Zscaler AI Security Platform

AI Guardrails - User vs. AI App

AVANTEC
Competence. Security. Trust.

Schutz von User



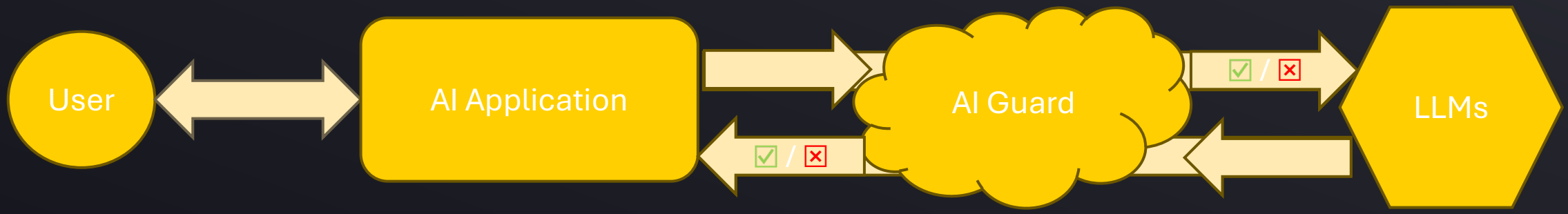
- Anthropic
- Azure
- Bedrock
- Bolt
- DeepAI
- Glean
- Google Gemini
- Lovable
- MaxAI
- Microsoft Copilot
- Napkin
- OpenAI
- OpenCode
- PerplexityAI
- Vertex
- xAI

Die Zscaler AI Security Platform

AI Guardrails - User vs. AI App

AVANTEC
Competence. Security. Trust.

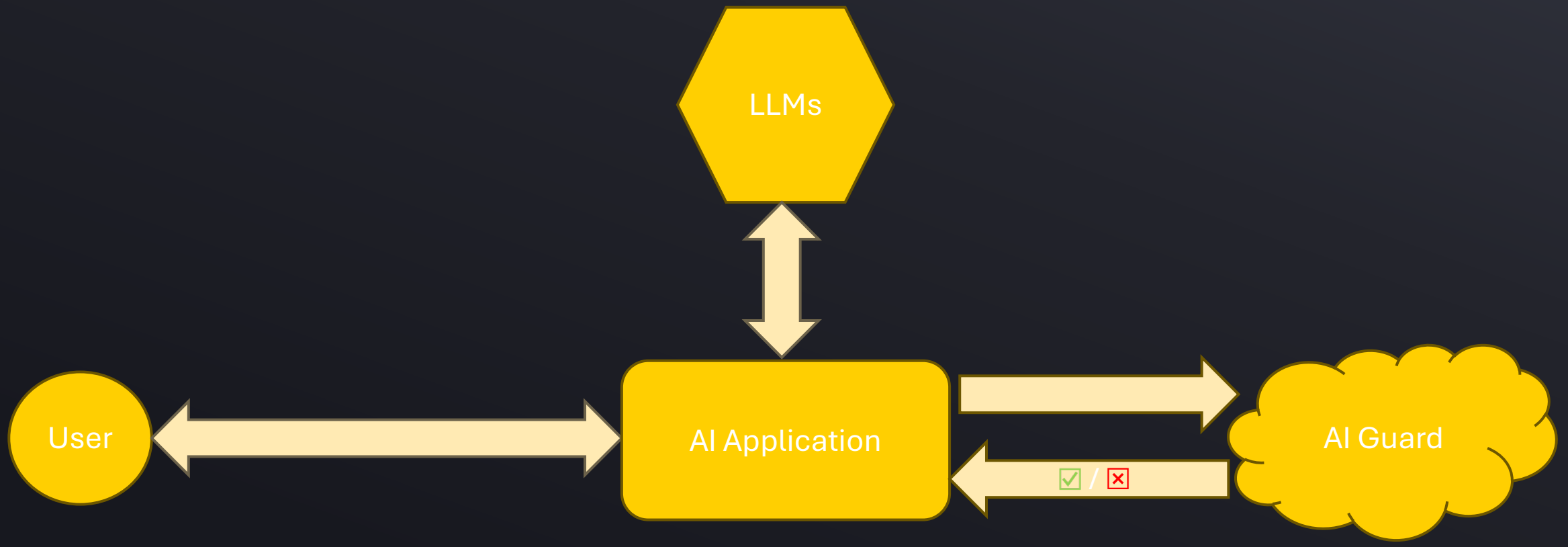
Schutz von AI Apps – Proxy Mode



Die Zscaler AI Security Platform

AI Guardrails - User vs. AI App

Schutz von AI Apps – DAS Mode



Die Zscaler AI Security Platform

Eine Übersicht

AVANTEC
Competence. Security. Trust.

AI Discovery and Risk

Ermöglicht das Entdecken und Klassifizieren von AI Assests und das Analysieren von Risiken.

- GenAI Security Report
- Prompt Logging
- DLP Monitoring für AI

AI Red Teaming

Ermöglicht fortlaufendes Testing eigener AI-Applikationen und gibt Empfehlungen um Vulnerabilitäten zu mitigieren.

- Einfaches Risiko-Assesment
- Vordefinierte + Custom Probes und Prompts
- Vielfältige Input-Methoden

AI Guardrails

Ermöglicht das Überwachen von AI Flows, um ungewollte Prompts und Antworten zu blockieren und unerwünschten Datenabfluss zu verhindern.

- Proxy Mode (inline) oder DAS Mode (via API)
- Schutz von Usern wie auch LLMs
- Vielzahl an Detectors

AI Governance and Compliance

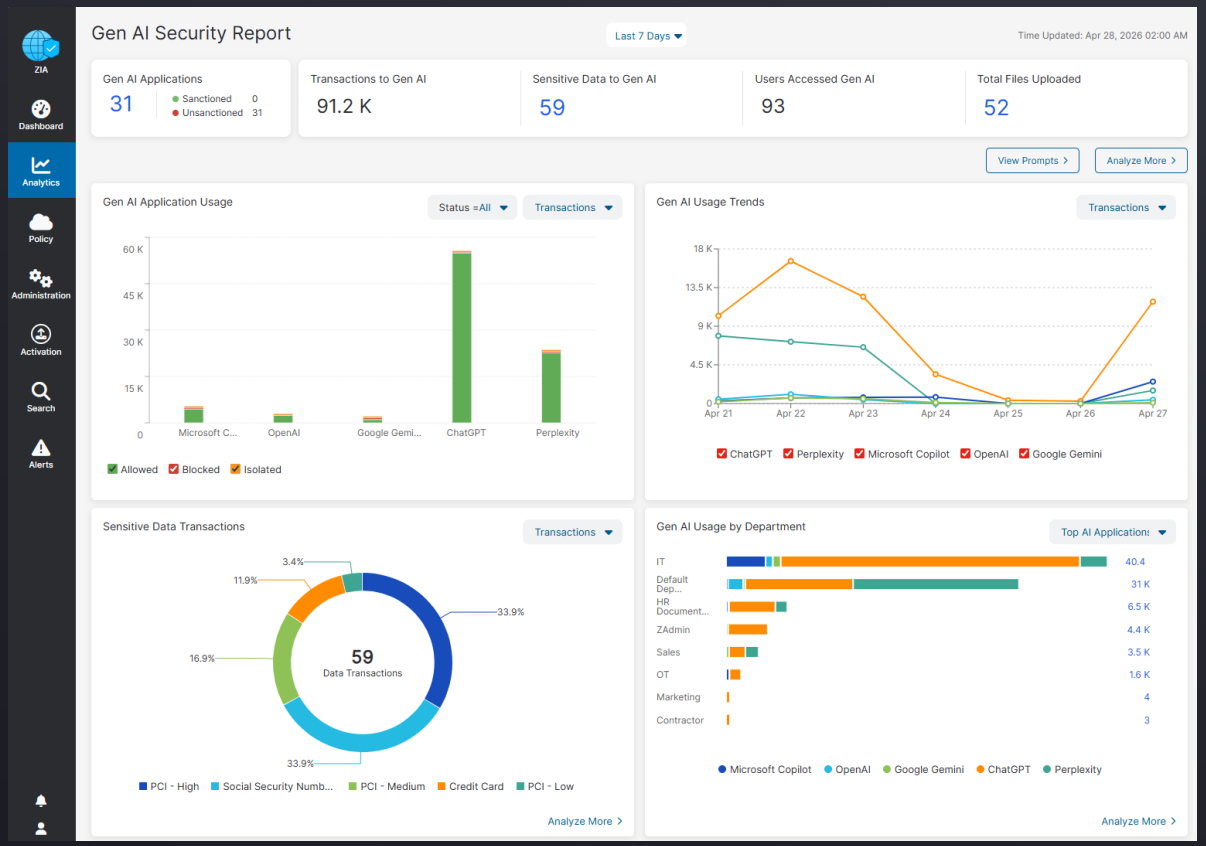
Erlaubt das Überwachen von AI Systemen und das Prüfen, ob diese compliant sind mit entsprechenden AI-Frameworks.

- Alerting zu Issues
- Visualisierung von Abhängigkeiten
- Vordefinierte + Custom Security Policies

User-Zugriff auf Public AIs

GenAI Security in ZIA

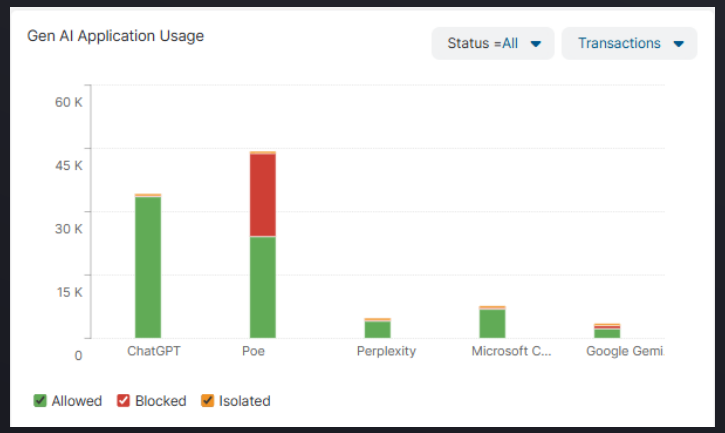
- Prerequisites
  - Gen AI Security Subscription

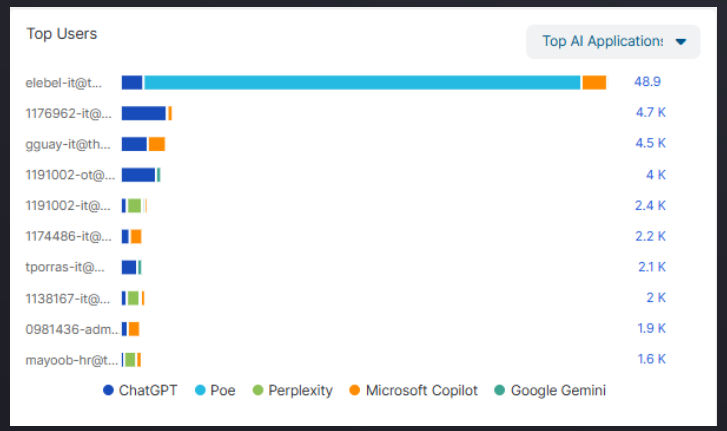


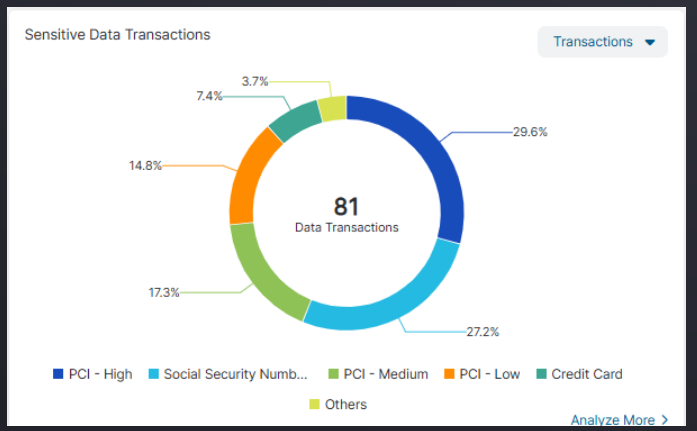
User-Zugriff auf Public AIs

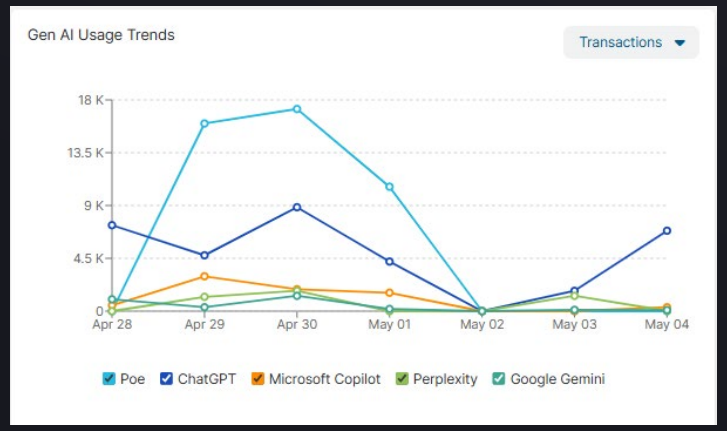
GenAI Security in ZIA – Analyse

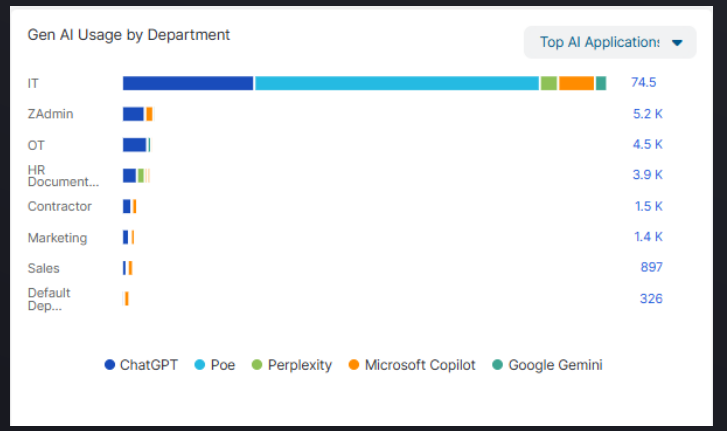
AVANTEC
Competence. Security. Trust.

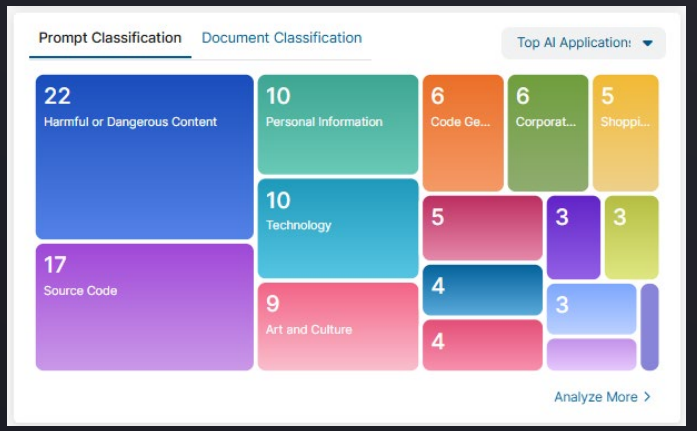












User-Zugriff auf Public AIs

GenAI Security in ZIA – Analyse

AVANTEC
Competence. Security. Trust.

Gen AI Security Report

Gen AI Applications

23

Sanctioned 0

Unsanctioned 23

← Gen AI Application Usage

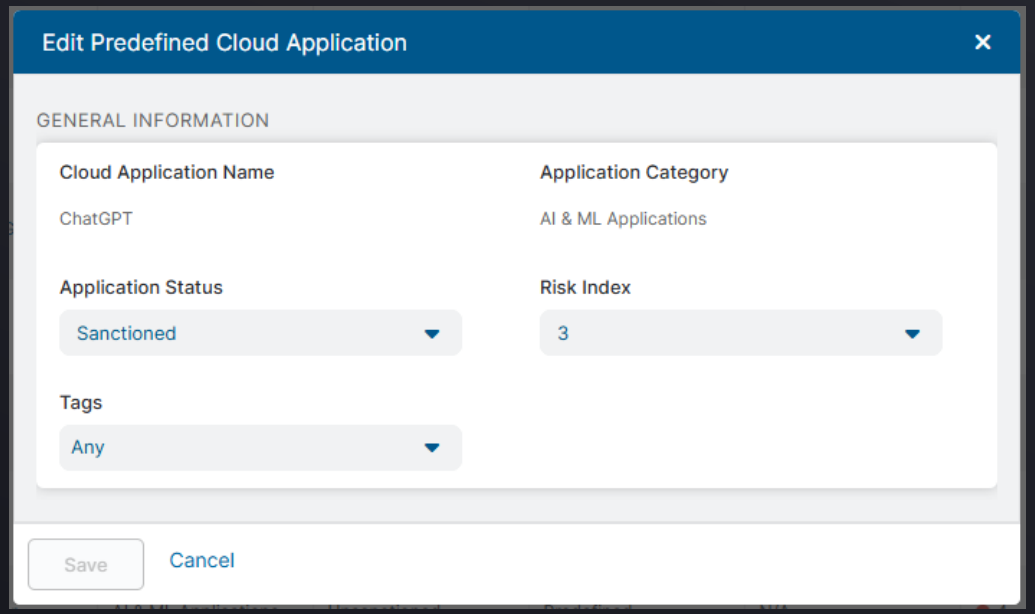
Report generated: 2:00 AM, May 04, 2026

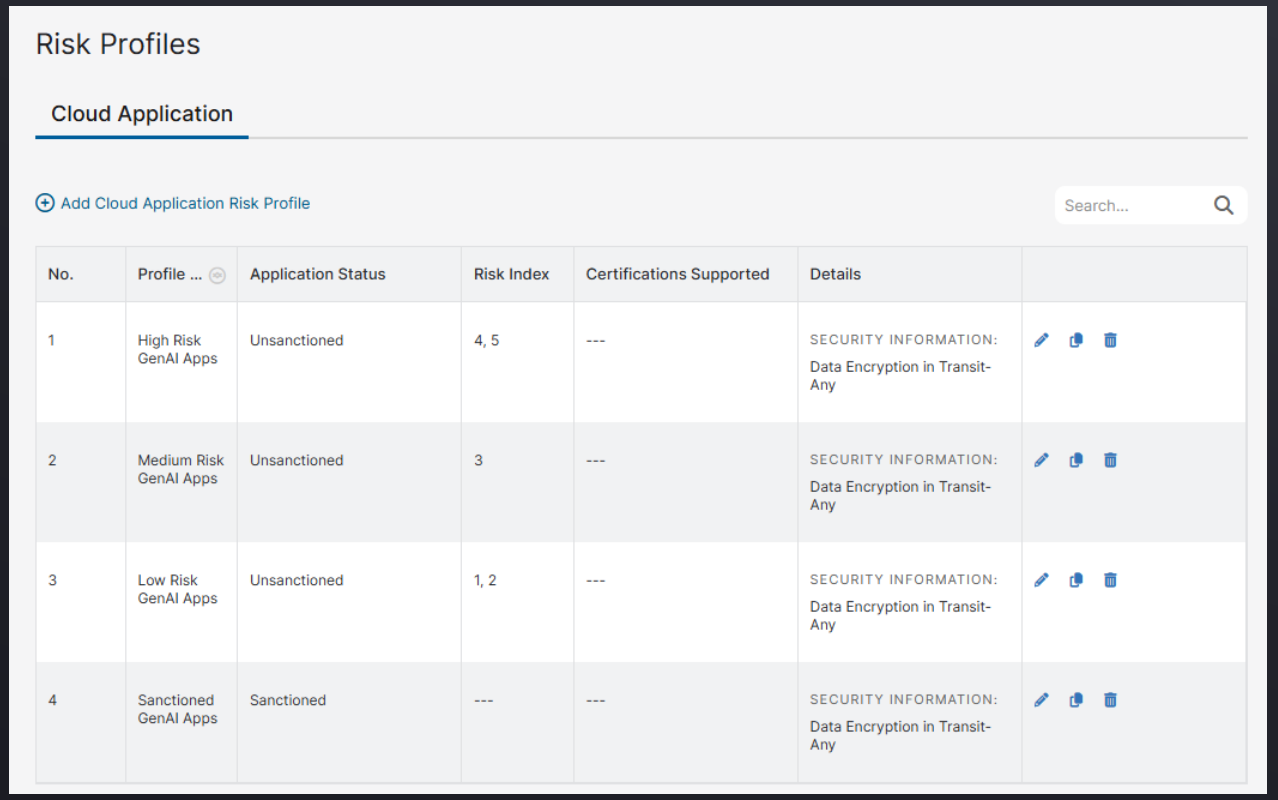
Application	Applicatio...	Applicatio...	Users	Loca...	Total Bytes	Upload Bytes	Download Bytes
ChatGPT	3	Unsanctio...	55	---	686.32 MB	280.78 MB	405.54 MB
Microsoft Copilc	2	Unsanctio...	12	---	296.87 MB	19.10 MB	277.77 MB
Google Gemini	2	Unsanctio...	23	---	130.51 MB	116.36 MB	14.15 MB
Perplexity	2	Unsanctio...	14	---	71.58 MB	4.30 MB	67.28 MB
Poe	3	Unsanctio...	3	---	42.30 MB	29.79 MB	12.52 MB
OpenAI	2	Unsanctio...	39	---	35.75 MB	1.60 MB	34.14 MB
Meta AI	2	Unsanctio...	6	---	31.69 MB	1.61 MB	30.07 MB
Deepgram	4	Unsanctio...	0	1	23.61 MB	581.09 KB	23.04 MB
Manus	2	Unsanctio...	10	---	20.23 MB	425.35 KB	19.82 MB
Grammarly	2	Unsanctio...	5	---	19.27 MB	448.89 KB	18.83 MB
Monica	2	Unsanctio...	1	---	10.03 MB	373.86 KB	9.67 MB
Glean	2	Unsanctio...	8	---	3.57 MB	102.09 KB	3.47 MB

User-Zugriff auf Public AIs

GenAI Security in ZIA – Risk-based AI Policy

AVANTEC
Competence. Security. Trust.





User-Zugriff auf Public AIs

GenAI Security in ZIA – Risk-based AI Policy

AVANTEC
Competence. Security. Trust.

URL Filtering Policy | Cloud App Control Policy | Advanced Policy Settings

Add

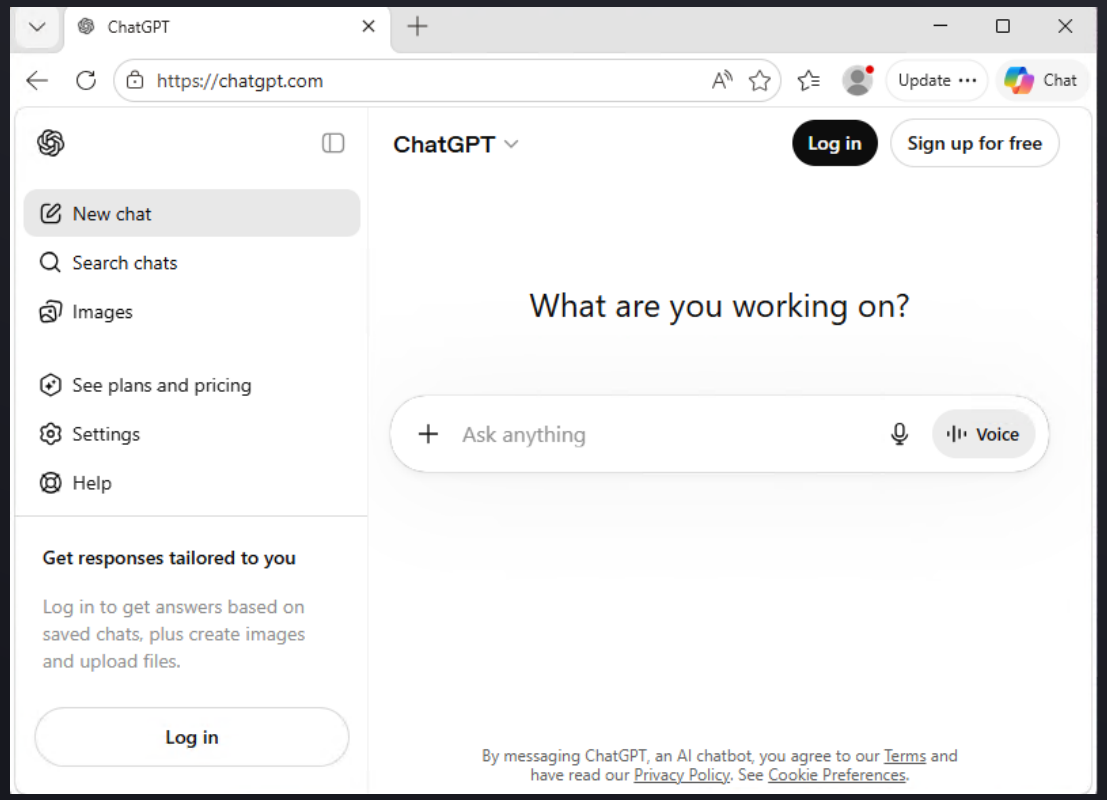
Recommended Policy

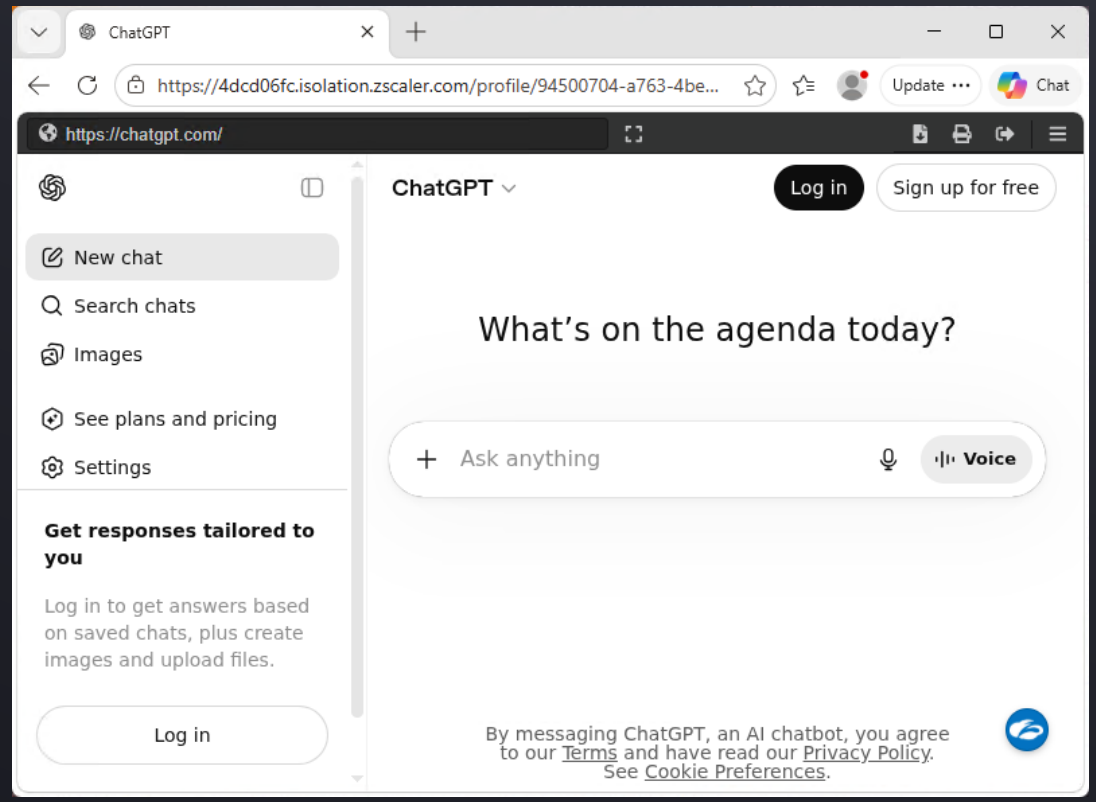
Rule Ord...	Rule Name	Criteria	Action	Label and Description
AI & ML APPLICATIONS				
1	Allow Sanctioned GenAI	CLOUD APPLICATION RISK PROFILE Sanctioned GenAI Apps	Allow Application Access	
2	Allow Low Risk GenAI	CLOUD APPLICATION RISK PROFILE Low Risk GenAI Apps	Allow Application Access	
3	Isolate Medium Risk GenAI	USER AGENT Opera; Firefox; Microsoft Internet Explorer; ... CLOUD APPLICATION RISK PROFILE Medium Risk GenAI Apps	Isolate Application Access Isolation Profile: GenAI Isolation	
4	Block High Risk GenAI	CLOUD APPLICATION RISK PROFILE High Risk GenAI Apps	Block Application Access	

User-Zugriff auf Public AIs

GenAI Security in ZIA – Risk-based AI Policy

AVANTEC
Competence. Security. Trust.





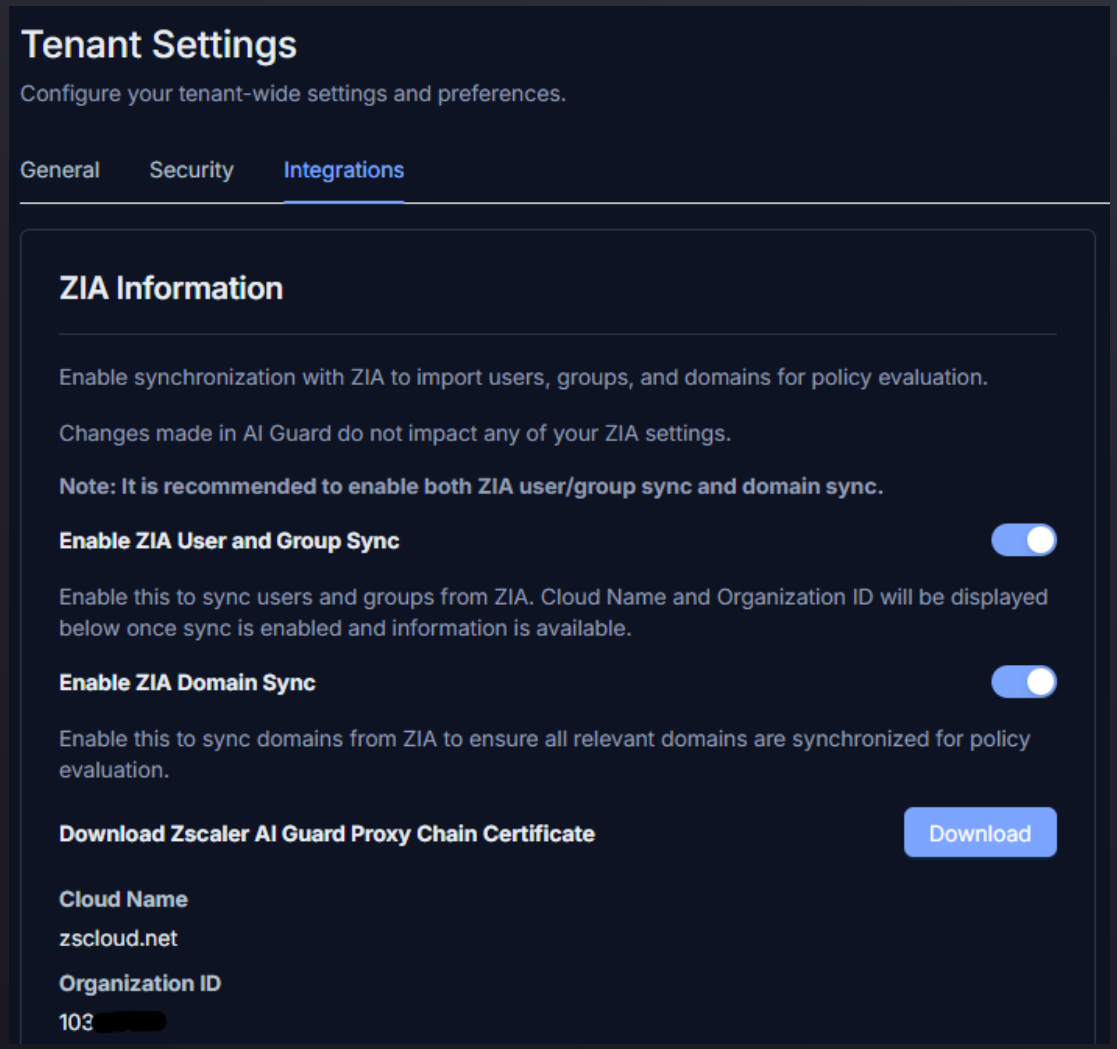
User-Zugriff auf Public AIs

Zscaler AI Guardrails

AVANTEC
Competence. Security. Trust.

- Prerequisites
  - AI Guard Subscription
  - ZIA und AI Guard sind gelinked
  - Liste der genutzten (und unterstützen) GenAI Apps

Application	Client Types	Domains Required
Grok (xAI)	○ Web Browsers	.grok.com
Lovable	○ Web Browsers	api.lovable.dev
MaxAI	○ Web Browsers	.api.maxai.me

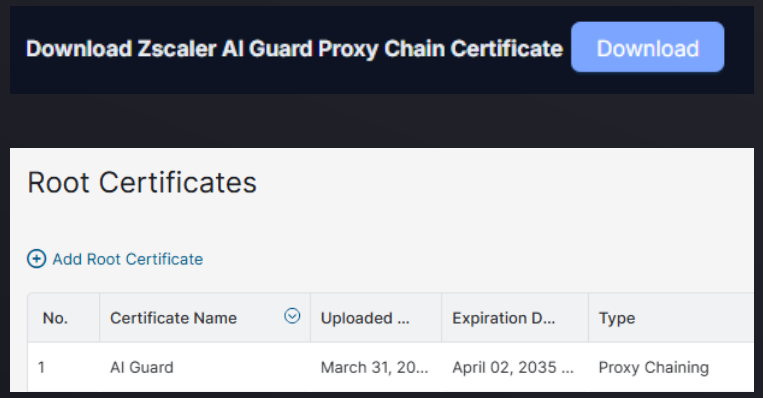


User-Zugriff auf Public AIs

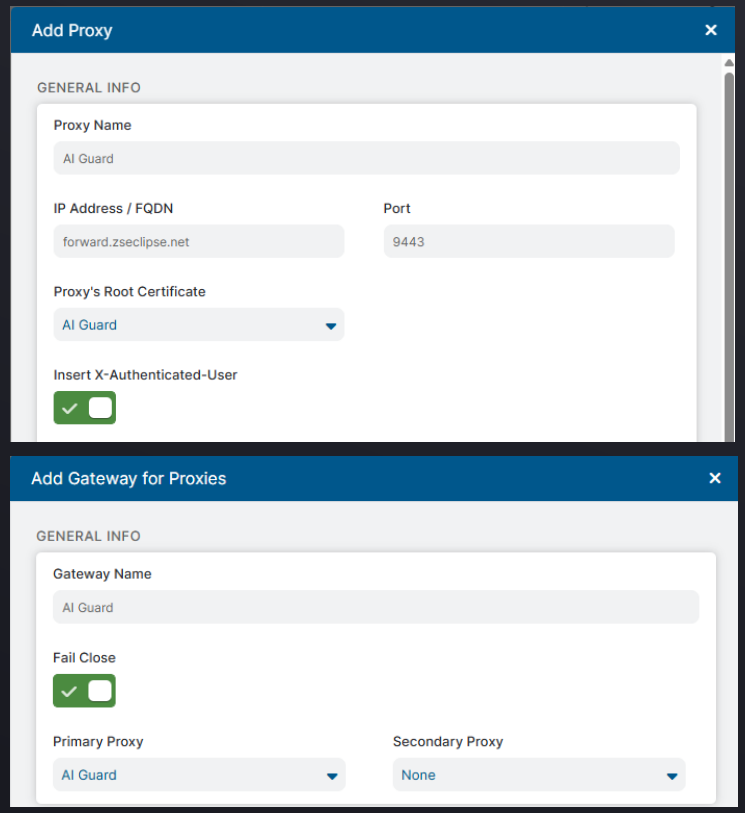
Zscaler AI Guardrails – Anbindung an ZIA

AVANTEC
Competence. Security. Trust.

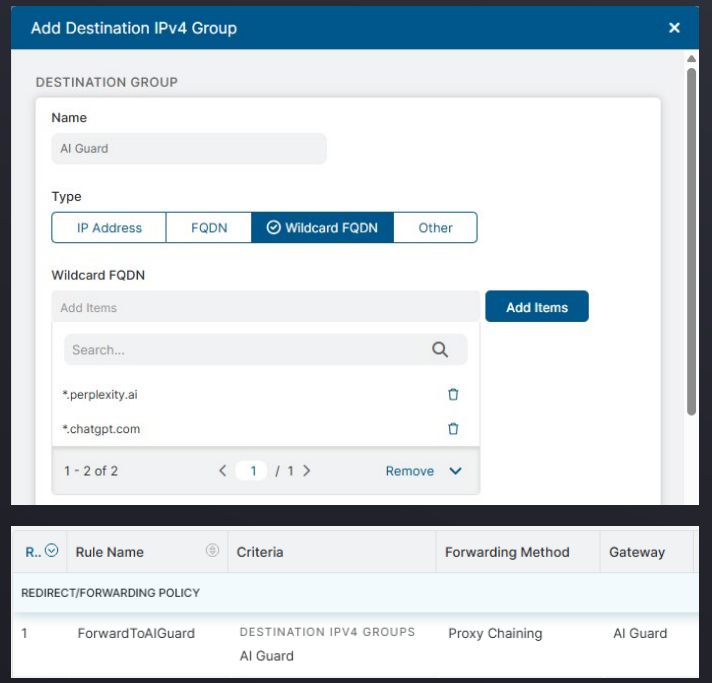
Schritt 1 – Root Certificate



Schritt 2 – Proxy & Gateway



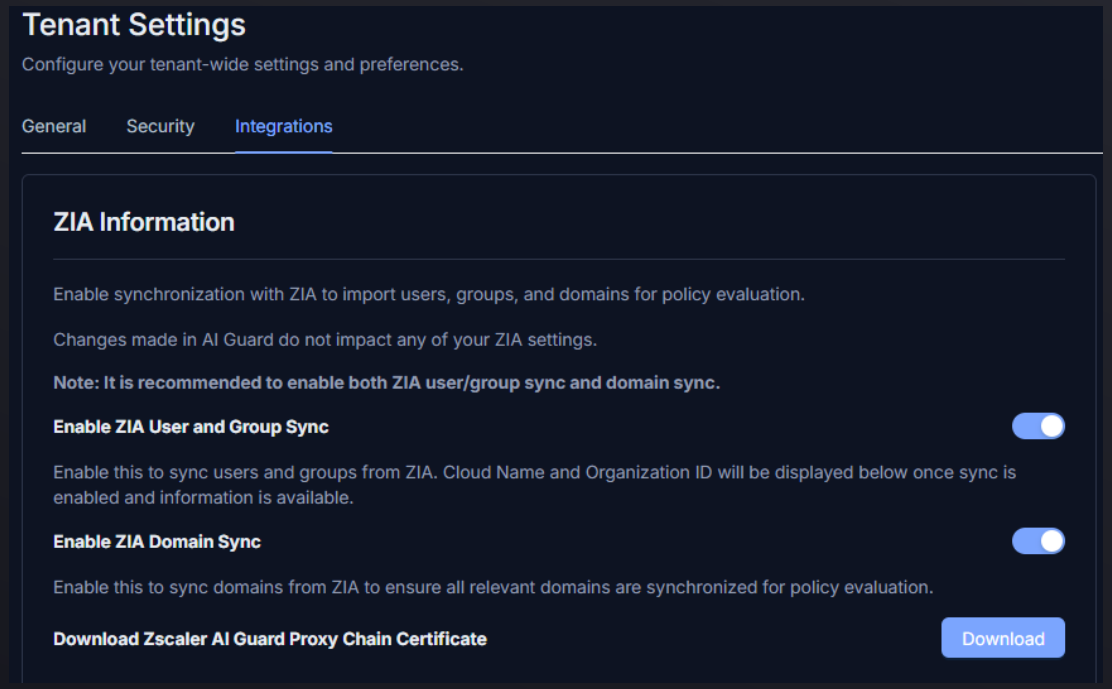
Schritt 3 – Forwarding



User-Zugriff auf Public AIs

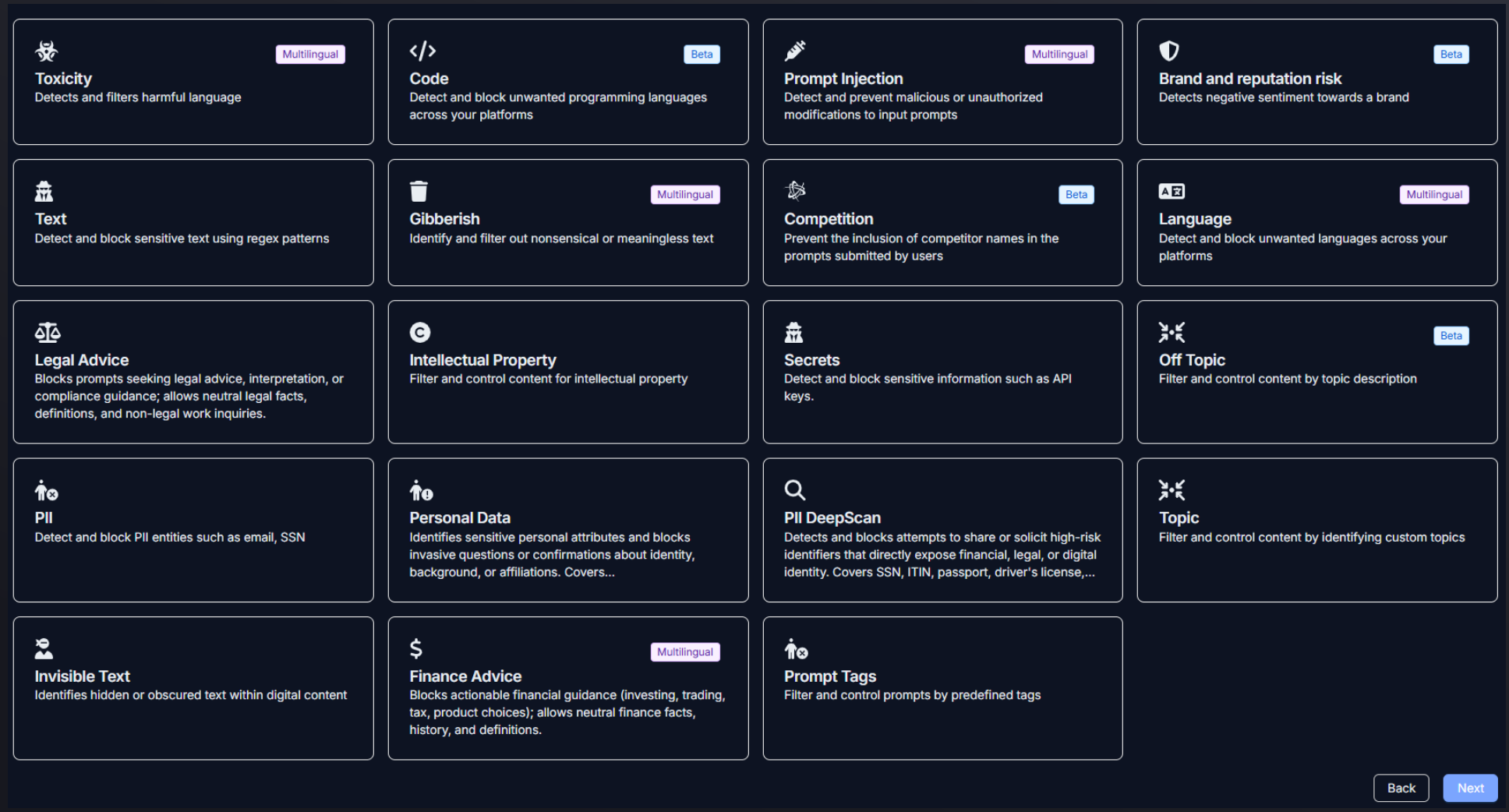
Zscaler AI Guardrails – Anbindung an ZIA

AVANTEC
Competence. Security. Trust.



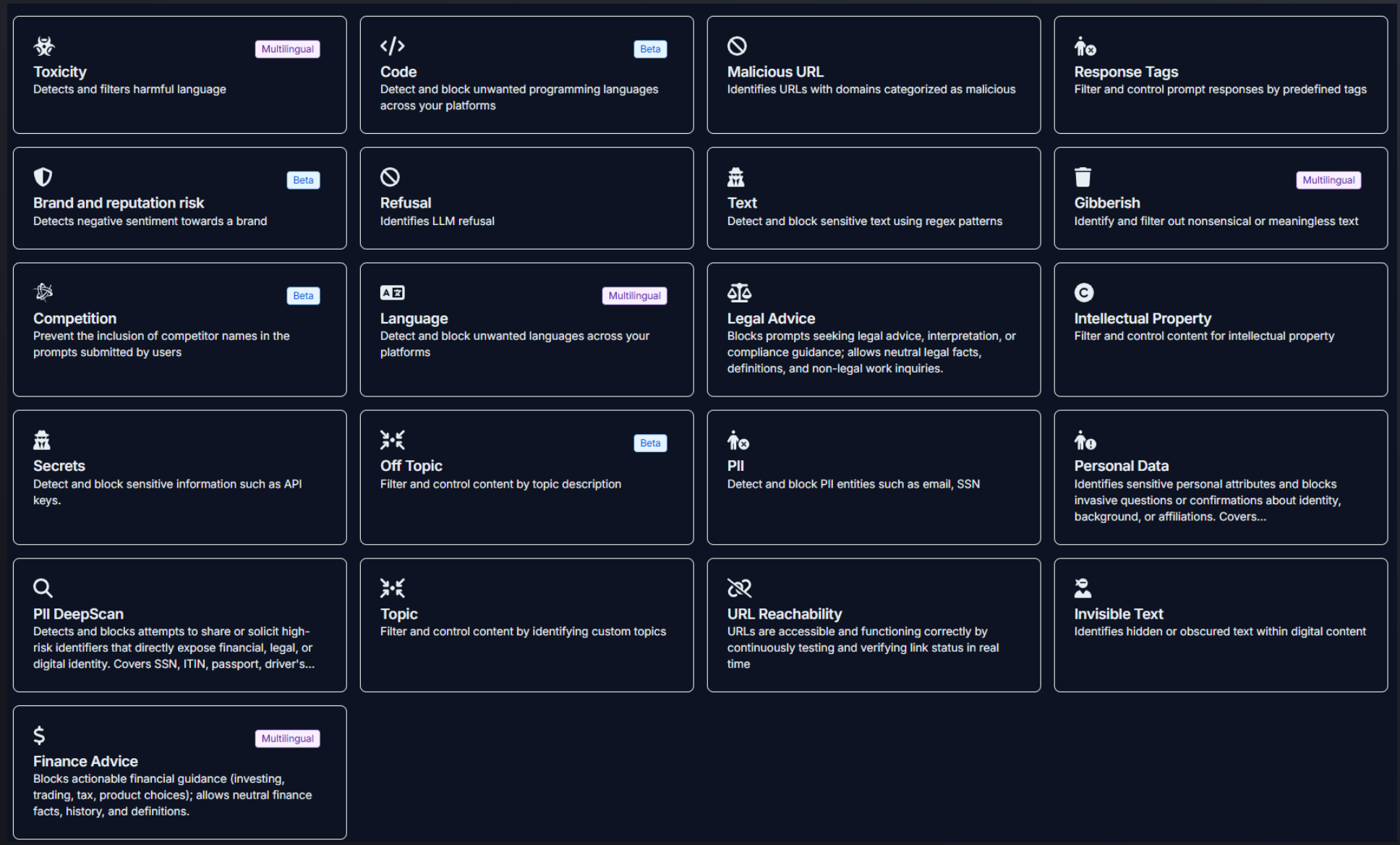
User-Zugriff auf Public AIs

Zscaler AI Guardrails – Policies für Prompts



User-Zugriff auf Public AIs

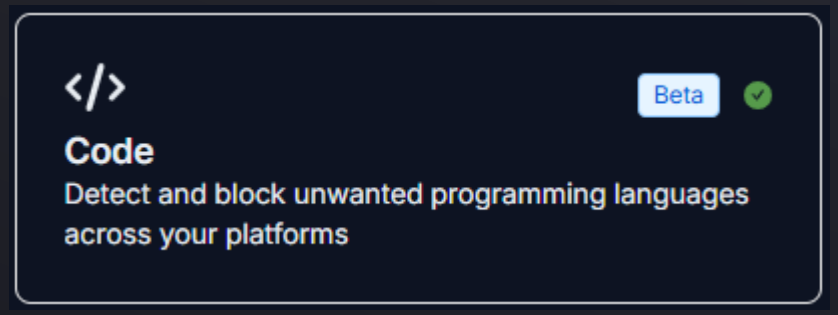
Zscaler AI Guardrails – Policies für Responses



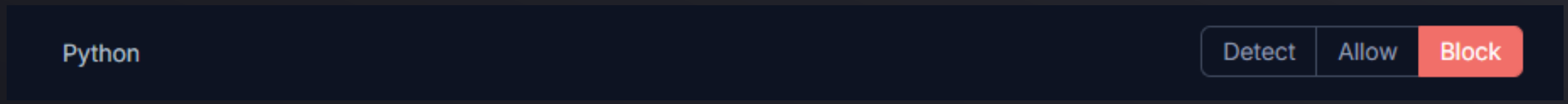
User-Zugriff auf Public AIs

AVANTEC
Competence. Security. Trust.

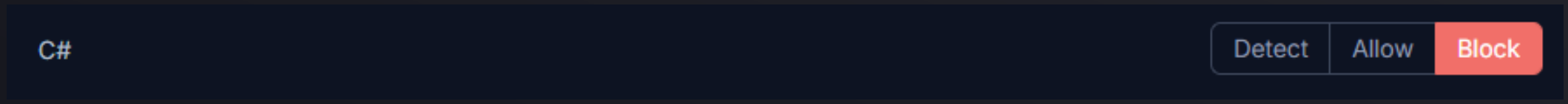
Zscaler AI Guardrails – Test-Policy



Prompt:

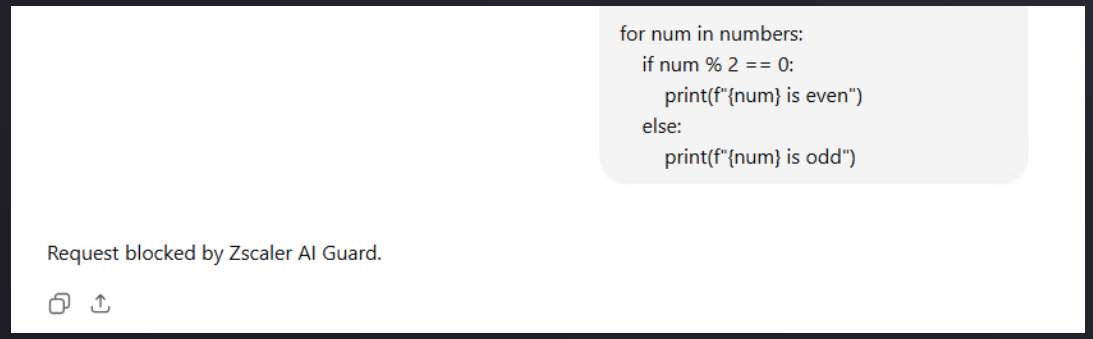


Response:



User-Zugriff auf Public AIs

Zscaler AI Guardrails – Test-Policy in Action

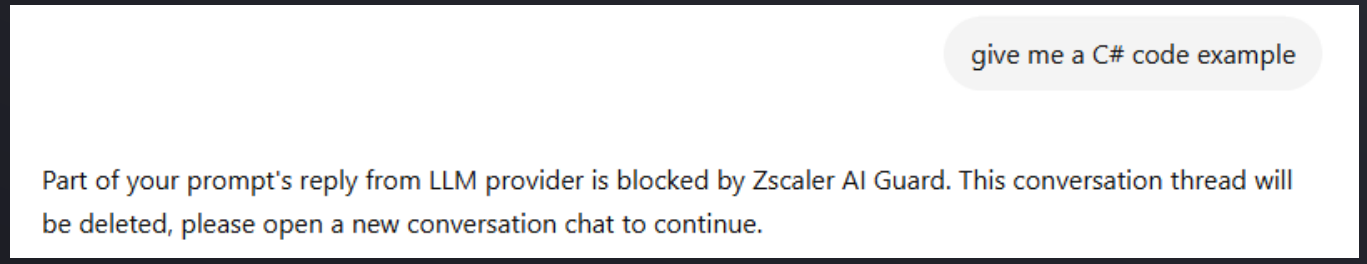


User	Policy Name	Severity	Prompt Detections	Response Detections	LLM	Prompt Action	Response Action
kugler@ava...	Test Policy	LOW	Code, PII, Prompt Tags	--		Blocked	--

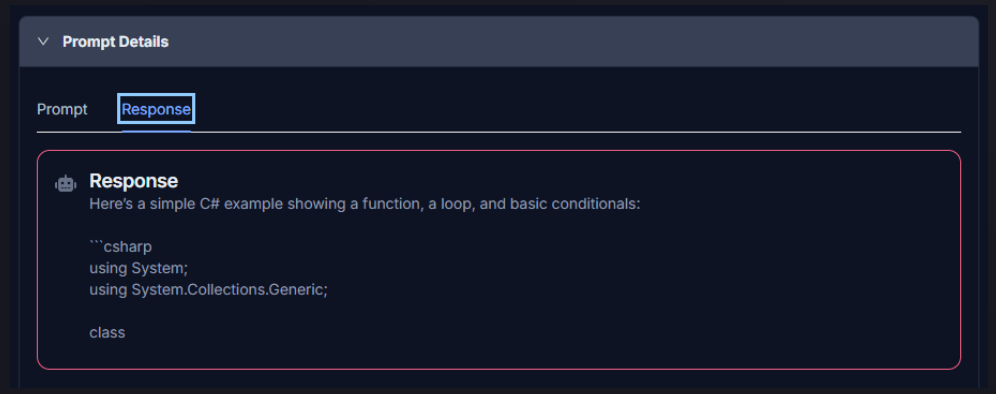
User-Zugriff auf Public AIs

Zscaler AI Guardrails – Test-Policy in Action

AVANTEC
Competence. Security. Trust.



User	Policy Name	Severity	Prompt Detections	Response Detections	LLM	Prompt Action	Response Action
kugler@ava...	Test Policy	LOW	Prompt Tags	Code, Response T..., PII		Allowed	Blocked



Ausblick

AVANTEC
Competence. Security. Trust.

- Kontinuierliche Weiterentwicklung
- Direktere Integration in ZIA


AVANTEC
Competence. Security. Trust.
Q&A
+
Diskussion

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

DANKE

BeyondTrust · CHECK POINT · CROWDSTRIKE · digicert · netskope · THALES · tenable · xorlab · zscaler

AVANTEC
Competence. Security. Trust.

Nächste Session 14:45

Session 3

Zero Trust Branch (ZTB) mit Airgap – wozu ist das gut? — **Holdener, 5. OG**
Produkt: zscaler
Referenten: René von Arx, Raffael Späni

Thread Huntig Deep Dive: Von Hypothese zu Detection Engineering — **Frei, 4. OG**
Produkt: CROWDSTRIKE
Referent: Alessandro Salucci

Disaster Recovery im Cloud-Zeitalter — **Lehmann Steingruber, 5. OG**
Produkte: zscaler netskope
Referent: Matthias Geiser

Authentication – passwordless, strong, secure — **Odermatt, 4. OG**
Produkt: THALES
Referent: Dirk Gluch

Zscaler Automatisierung — **Cancellara, 4. OG**
Produkt: zscaler
Referent: Christian Schnittert