



Controlware
Security Day

2025

controlware



Zwischen Innovation und Risiko

GenAI sicher im Griff behalten

Alex Derksen, Major Account Manager
Andreas Hüntten, Senior Solutions Engineer

17.09.2025, Congress Park Hanau



QUIZ



Security

Cloud smart



Question 1

What percentage of organizations today have users accessing Generative AI applications or applications with integrated GenAI capabilities?

A: 52%

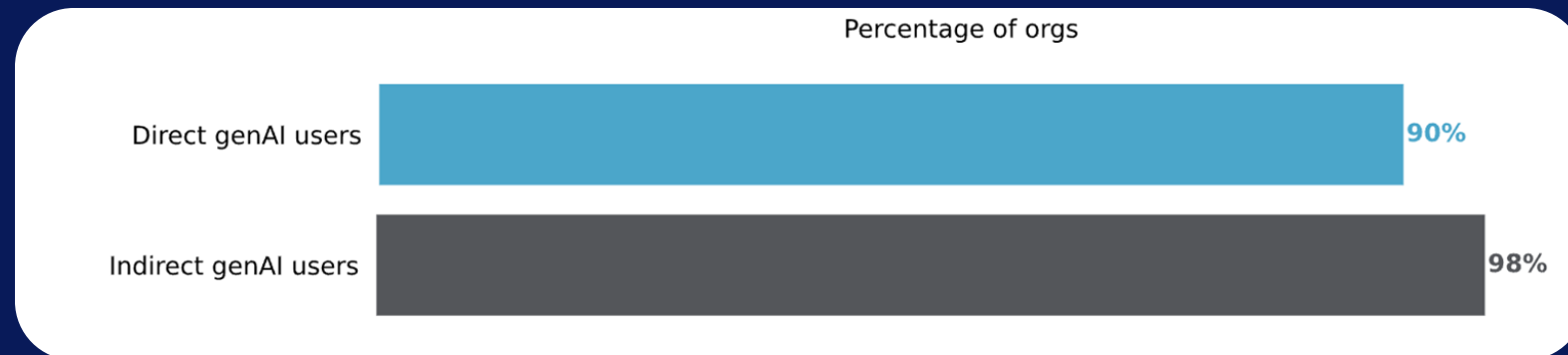
B: 98%

C: 84%

Question 1

What percentage of organizations today have users accessing Generative AI applications or applications with integrated GenAI capabilities?

A: 52% B: **98%** C: 84%



Question 2

What percentage of Generative AI use in the enterprise is shadow AI?

A: 25%

B: 56%

C: 72%

Question 2

What percentage of Generative AI use in the enterprise is shadow AI?

A: 25%

B: 56%

C: 72%

Question 3

What is the leading policy violation we see across the enterprise when it comes to use of AI?

A

Uploading or
pasting sensitive
data



B

Downloading AI-
generated
images without
proper licensing



C

Accessing
unauthorized AI
applications



Question 3

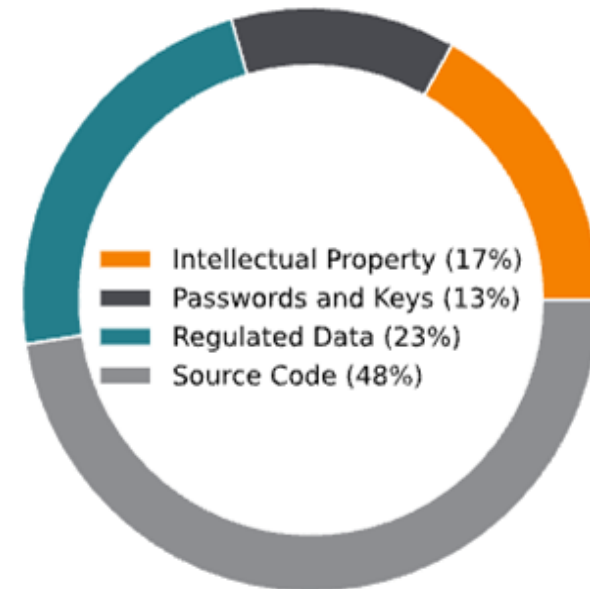
What is the leading policy violation we see across the enterprise when it comes to use of AI?

A

Uploading or
pasting sensitive
data



Type of data policy violations for genAI apps











Secure Innovation with AI

+ Security

Cloud smart +

SkopeAI: Unlocking the Potential of AI Across the Portfolio

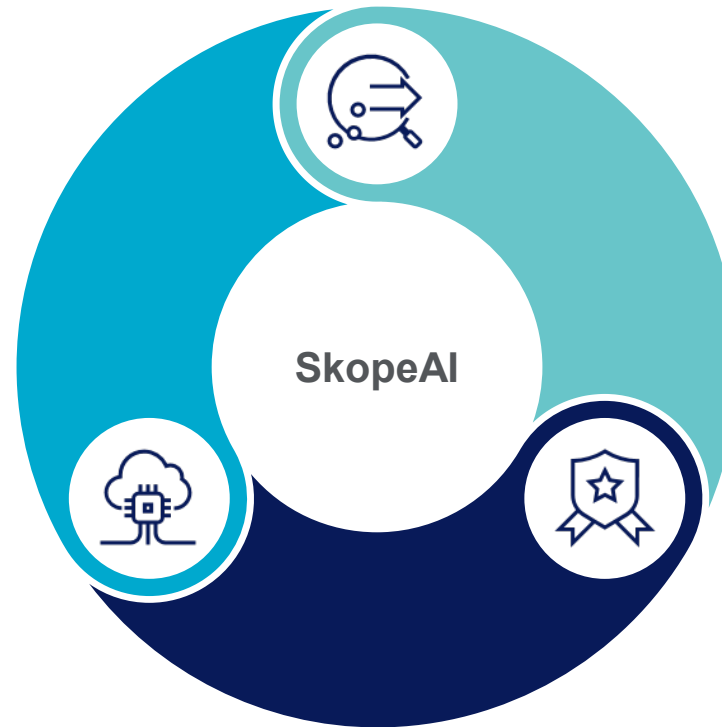
 Data Protection	 Threat Protection	 Generative AI and SaaS	 User & Entity Behavior	 SD-WAN Optimization	 Device Access Intelligence
<ul style="list-style-type: none">• Automatically protect unstructured data with high reliability and speed with pre-trained ML classifiers• Protect novel data with Train Your Own Classifiers (TYOC)	<ul style="list-style-type: none">• Prevent evasive attacks, polymorphic malware, new phishing, zero-day• Faster detection and categorization of malware, web domains, URLs, and web content	<ul style="list-style-type: none">• Discover and govern the use of generative AI and novel SaaS apps• Protect sensitive data across apps like ChatGPT and coach employees in real-time	<ul style="list-style-type: none">• Detect users' unpredictable risky behavior• Identify insiders' anomalous behavior, compromised accounts, data exfiltration	<ul style="list-style-type: none">• Optimal network access through enterprise-wide predictive insights• WAN access anomaly detection, app performance flow analytics	<ul style="list-style-type: none">• Discover newly connected devices and gain deeper device context, activities and behavior• Real-time detection of behavioral anomalies, threats and vulnerabilities



Our mission is to advance AI/ML technology to power the Netskope One platform

Netskope AI Labs

Specialized division advancing cybersecurity by developing large-scale, responsible AI/ML models tailored for real-time SSE SASE applications.



160+ models
deployed

30 AI/ML patents
granted

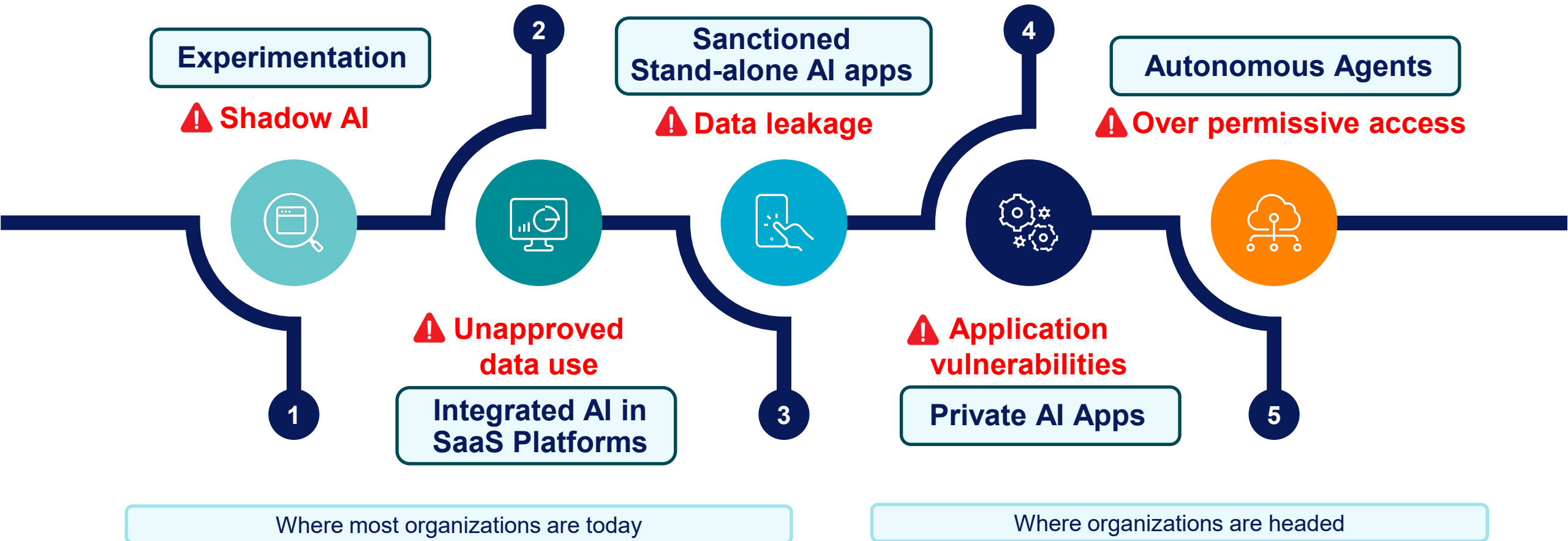




AI Adoption and Risks



Common AI Adoption Journey





How Netskope can help ?



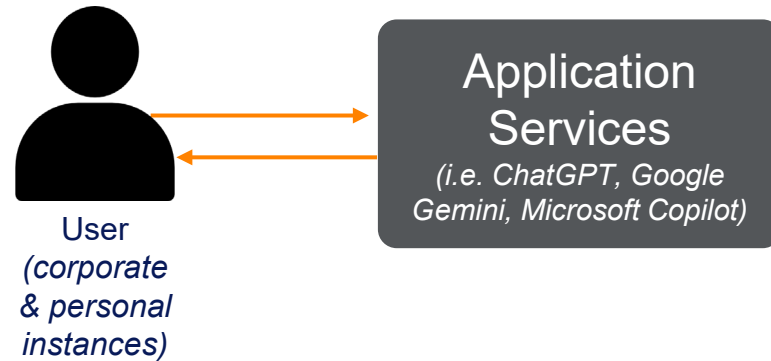
Netskope's Approach to Securing AI



* Roadmap



Use Case 1: Secure Access to AI Tools



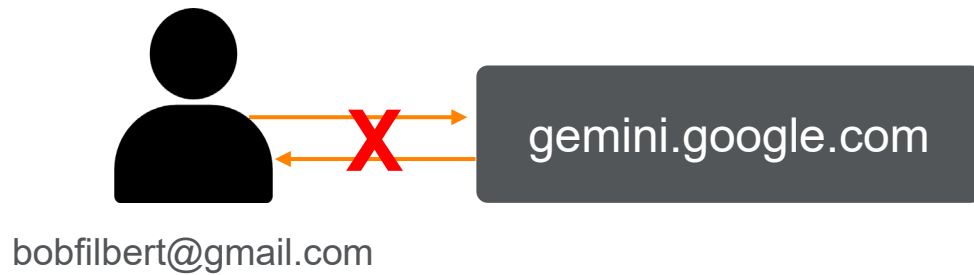
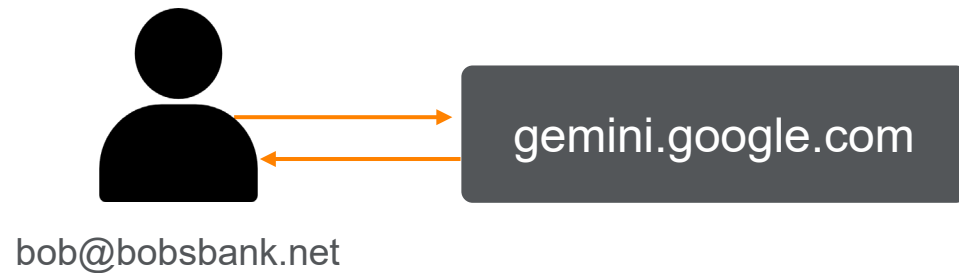
- Shadow AI and unsanctioned tool usage
- Lack of context-aware access controls



- Visibility into shadow AI and AI usage trends
- Inline, context-aware access control
 - Allow safe AI tool usage (e.g., ChatGPT, Gemini, Copilot)
 - Block or restrict risky behaviors (e.g., pasting sensitive data)
 - Apply different policies by user, department, or role



Gen AI App Instance Awareness

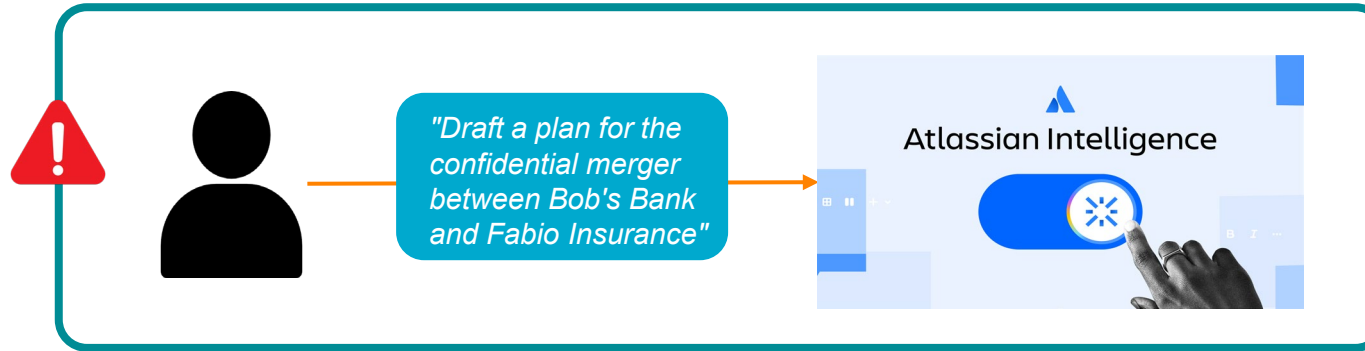


- 60% of enterprise users use a personal instance to access AI apps*
- Non-corporate instances of Gen AI apps allow for data to be used for model training
- Governing data going to prompts is a challenge because hard to differentiate between instance



- Only Netskope supports granular controls and data protection based on app instance
- Stop sensitive data going to non-corporate instances
- Safely enable shadow AI usage

See and Control In-App AI Activities



Visibility into In-App AI Activity



Skope IT™ > Events & Alerts > Application Events Last 24 Hours

FILTERS ▾


Q Application Name ~ Activity: AI Post + ADD FILTER 🔍 📄 👁

Application Events						
	TIME	ACTIVITY	USER	APPLICATION	OBJECT	WEBSITE
🔍	7/22/25 2:50:34 PM	AI Post	bob@bobsbank.net	Atlassian Confluence	M&A Plan	Atlassian - JIRA
🔍	7/22/25 2:49:34 PM	AI Post	bob@bobsbank.net	Atlassian Confluence	M&A Plan	Atlassian Confluence

Sort by: Time EXPORT

Rows per page: 100

Control Activity and Stop Data Leakage

**Bob's Bank**

Alert!

The activity you are attempting includes sensitive data so in order to protect against data leakage you are being blocked. Below are the details:

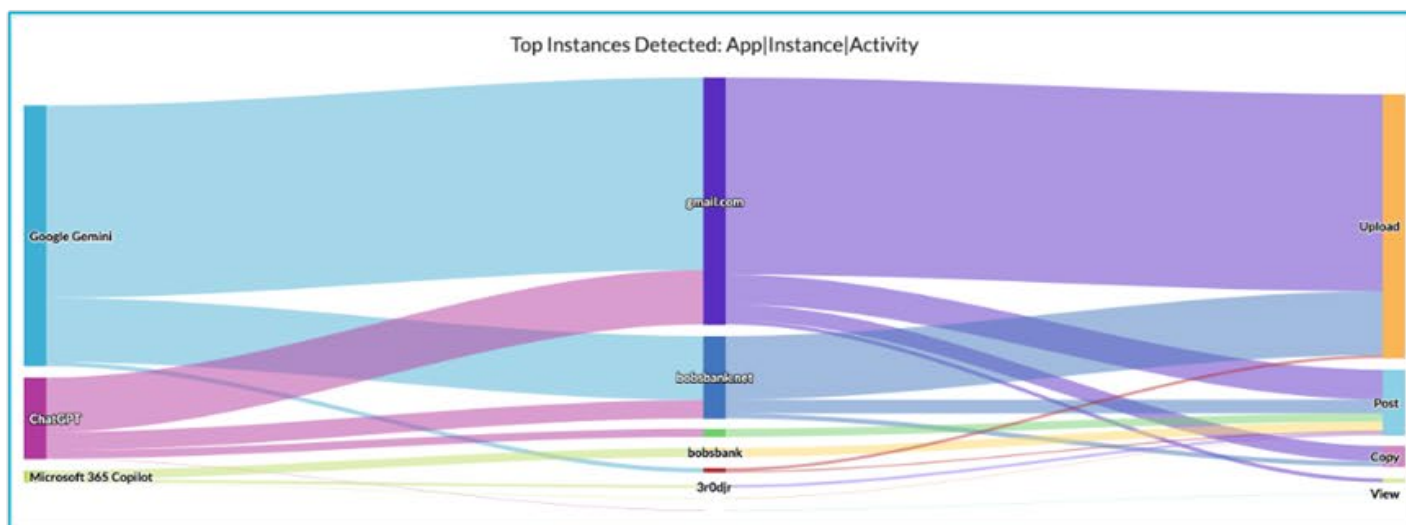
Application: Atlassian Confluence
Activity: AI Post
Policy Triggered: Confluence - Block data about Fabio Insurance acquisition

This window will auto-close in **53 seconds**

OK

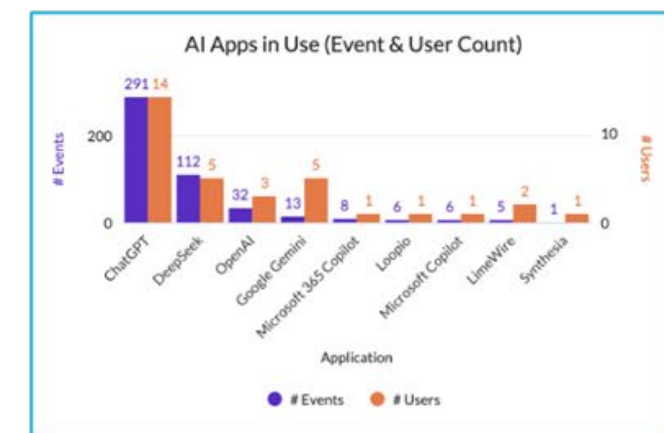
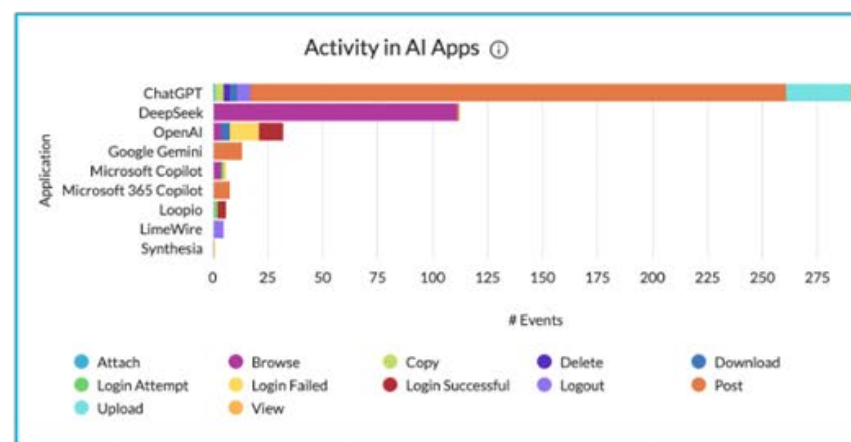
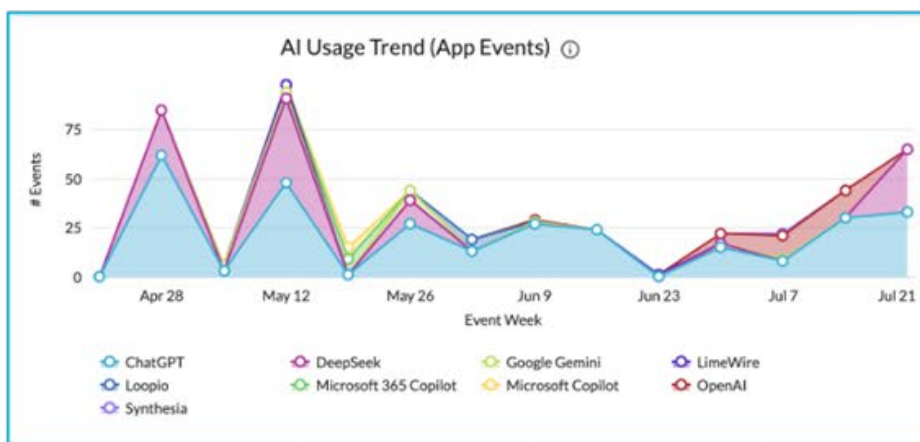


Get visibility into AI usage



Instance Detail ⓘ

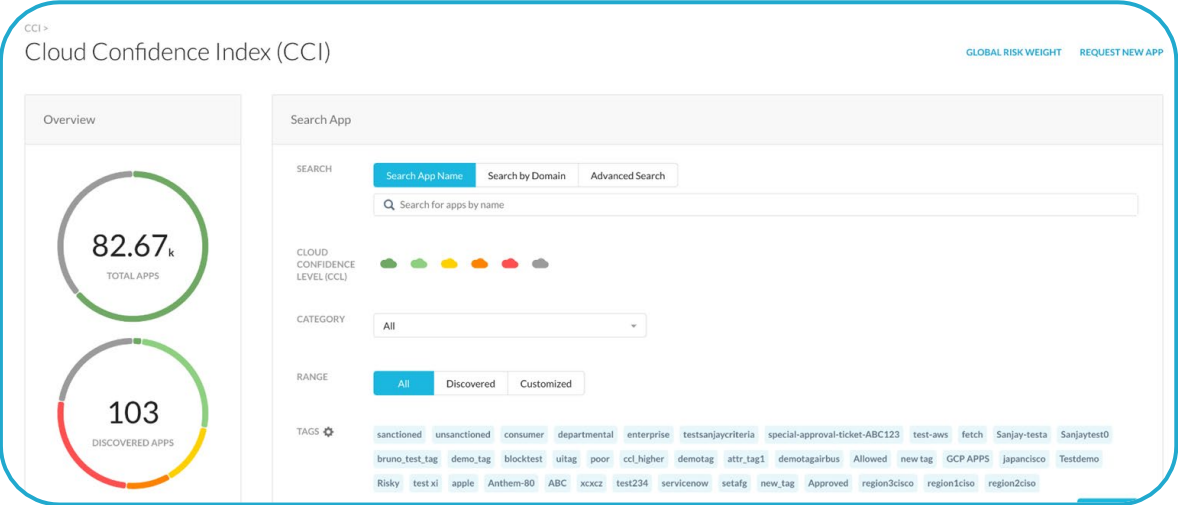
	Application	Application Instance ID	# Users	# Events
1	Microsoft 365 Copilot	bobsbank	1	35
2	ChatGPT	embedded-link	1	2
3	Microsoft 365 Copilot	fabioinsurance	1	2
4	Google Gemini	netskope.com	1	18
5	Google Gemini	bobsbank.net	1	250
6	Google Gemini	gmail.com	1	752
7	ChatGPT	bobsbank.net	1	72
8	Microsoft 365 Copilot	3r0djr	1	11
9	ChatGPT	unauthenticated	1	32
10	ChatGPT	gmail.com	1	213



AI App Usage Trends + App Instance Usage + Activity and DLP Violations + Policy Actions



Have visibility into AI App Risk



Gen AI-powered risk categorization of apps



Adaptive risk scores

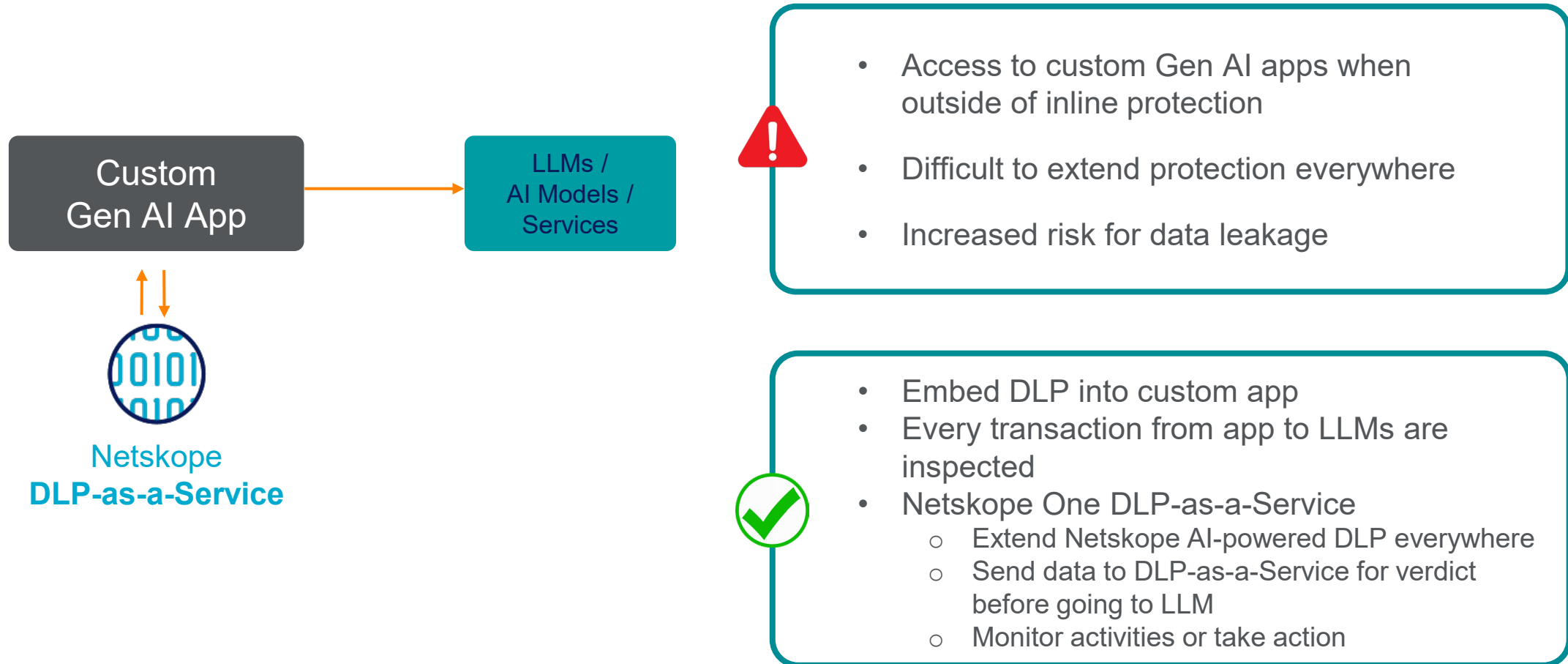


Detail on embedded AI capabilities

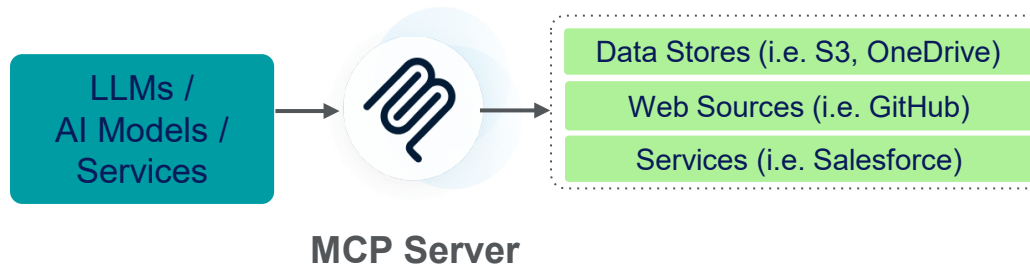
Field Name	Field Description
Uses GenAI	Does the App use Gen AI?
Disable GenAI	Does it allow disabling Gen AI?
Customer data for learning	Does it use customer data for training AI models?
Data sharing with GenAI vendor	Does it share the data with third-party Gen AI vendor?
Tenant isolation or private instances for GenAI	Does it support tenant isolation or private instance for Gen AI?
AI risk regulations and compliance	Adoption of regulatory & compliance standards
GenAI usage policy	Is there a documented Gen AI policy?
Security assessment of GenAI vendor	Does the vulnerability assessment include checks for OWASP top 10 vulnerabilities for LLM's?



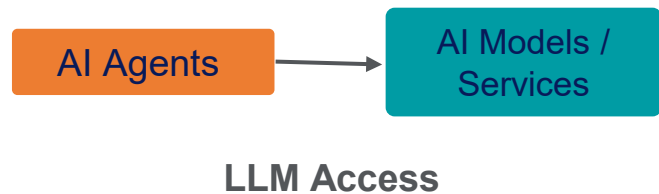
Use Case 2: Secure Custom AI Apps



Use Case 3: Secure Agentic Interactions



- Blind spots in AI-to-AI and service-to-service communications
- Risk of data leakage or unauthorized access
- Difficulty in auditing and explaining AI-driven decisions
- API and integration vulnerabilities in AI workflows
- No central policy enforcement point

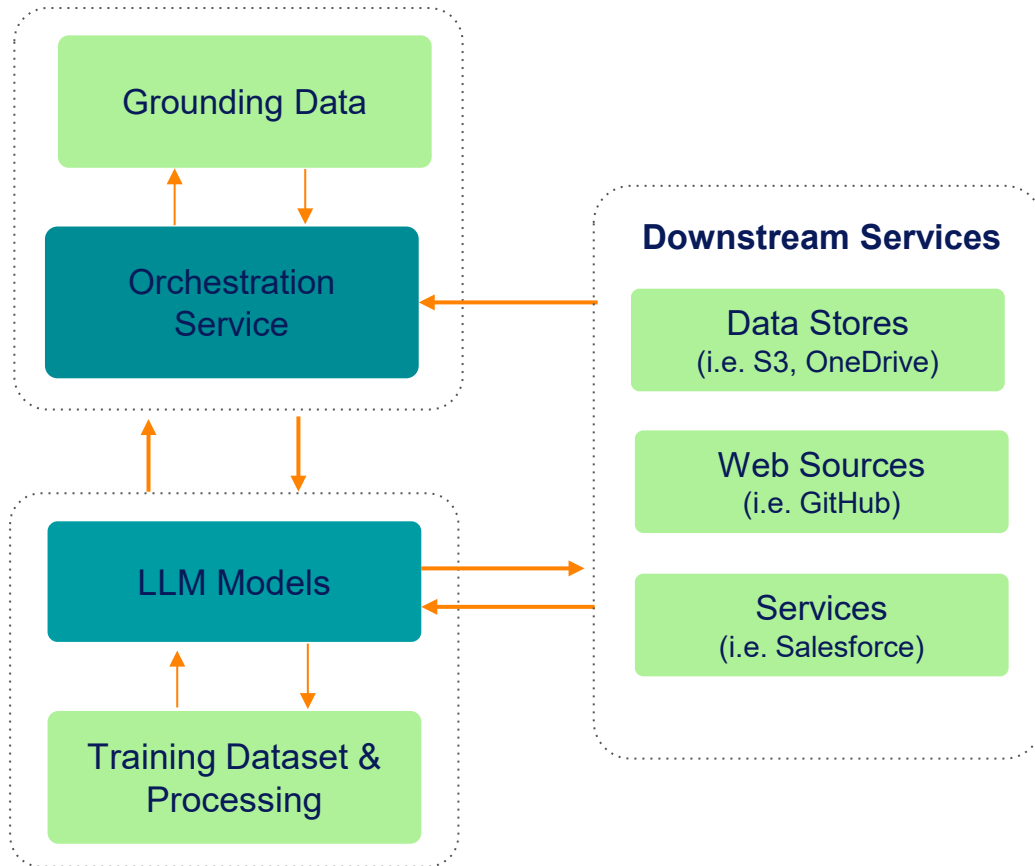


AI Gateway*

- Visibility & access control - logging, monitoring, centralized authentication & rate limiting
- Content inspection for securing request / response, detecting malware & prompt attacks, implementing custom defined guardrails & preventing data leakage
- Optimized operations with auditability, model switching for reliability and performance, caching & audit of the communications



Use Case 5: Protect AI Data Pipeline



- Lack of visibility into where AI data lives and flows
- Unintended data exposure in AI workflows



Data Security Posture Management (DSPM)

- Delivers unified visibility into structured & unstructured data posture across multi-cloud environments
- Continuously discovers and classifies sensitive data across SaaS, IaaS, & cloud data stores
- Maps data flows & access patterns to uncover risk from shadow AI, third-party sharing, or over-permissioned users
- Identifies misconfigurations & exposure risks (e.g., open buckets, public links, overly broad access)
- Enables proactive policy enforcement through integration with DLP, SSPM, & access controls

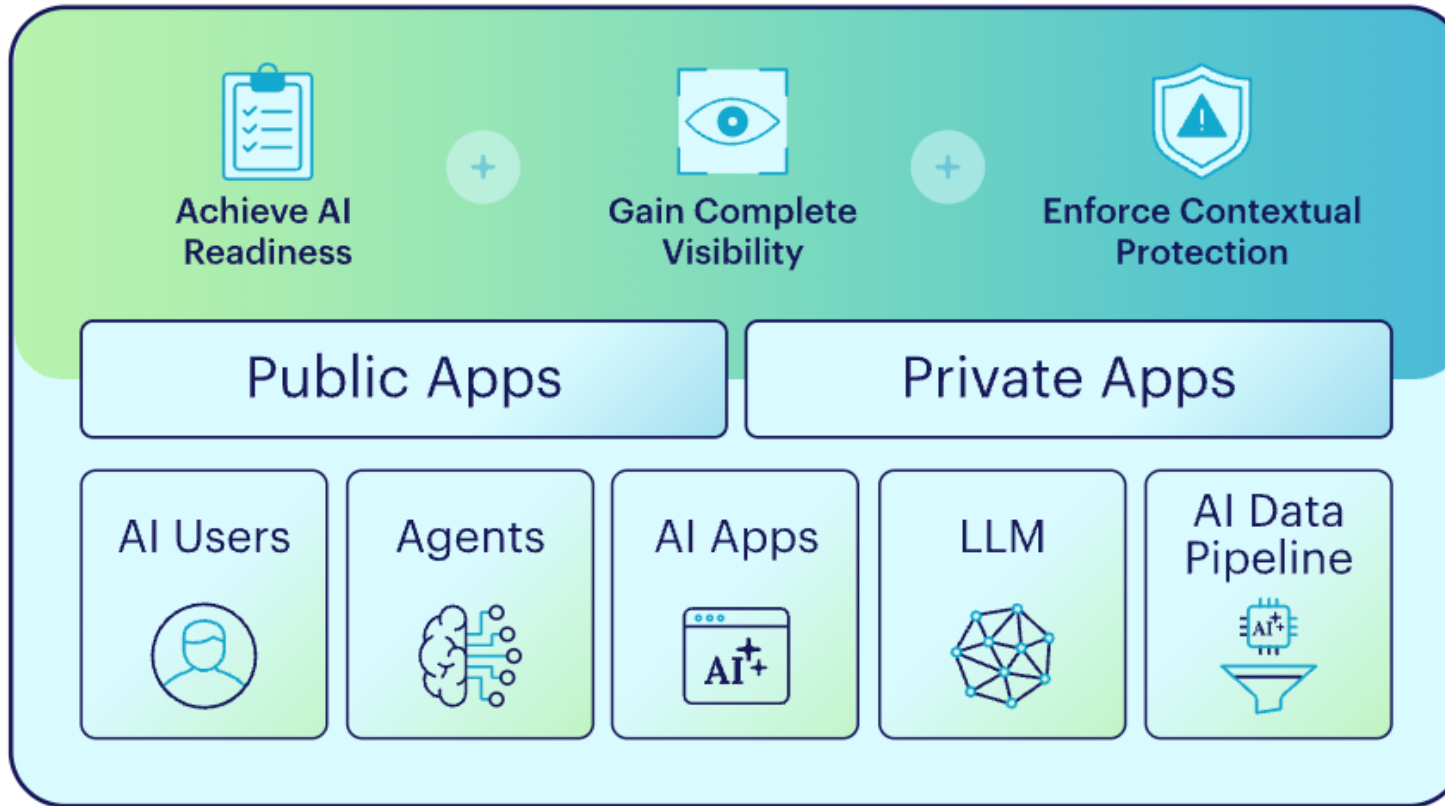


+ Demo ?

Please come to our booth !



Netskope: Securing AI End-to-End, Everywhere



AI-Powered Data
Security

Comprehensive AI
Visibility

Granular, Context-
based Protection





Thank you !

aderksen@netskope.com, +49 173 663 0 257

ahuenten@netskope.com, +49 176 810 18 177





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.