



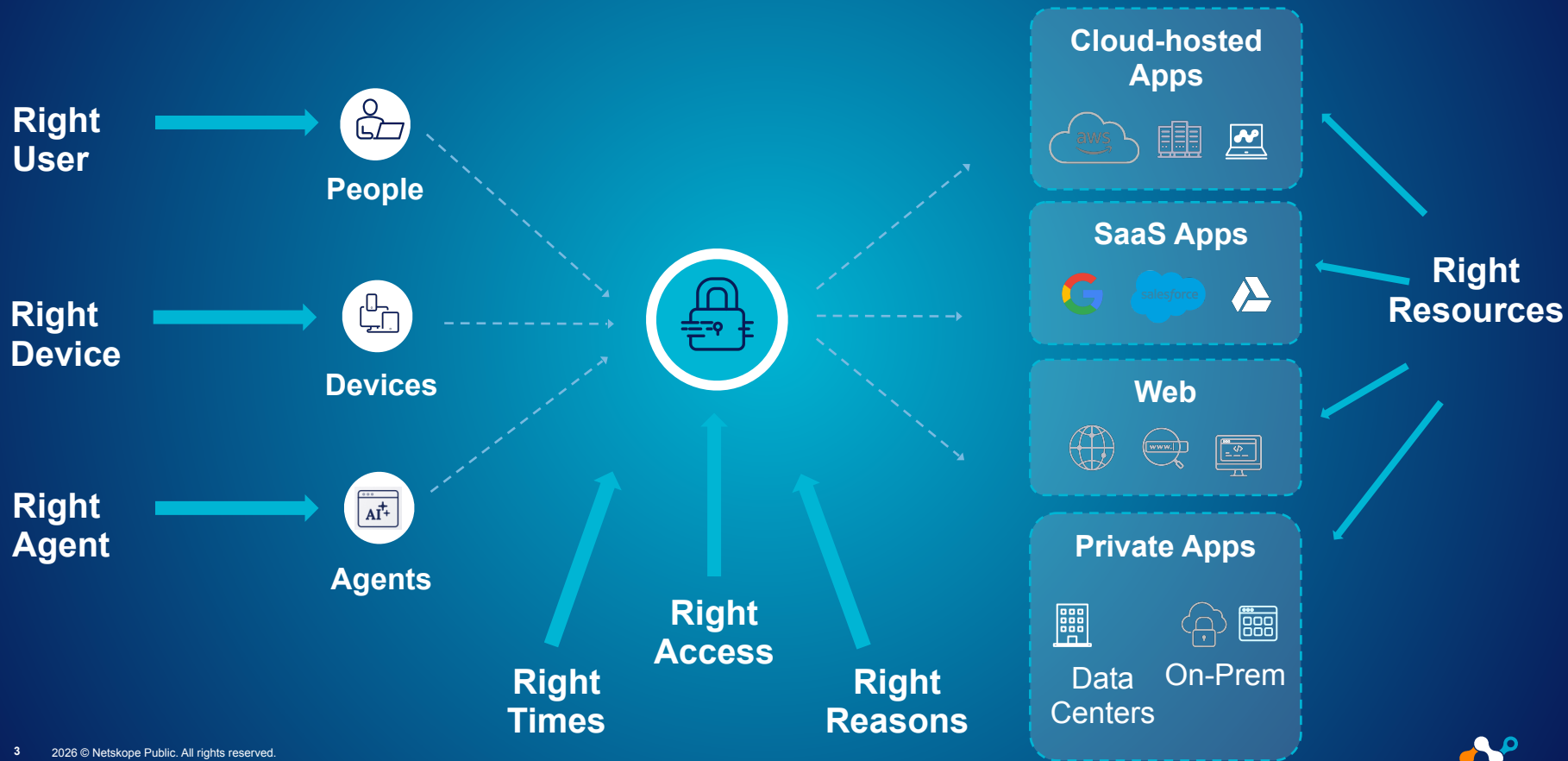
Security & Networking ReAIImagined

Secure and accelerate cloud, data, and AI everywhere

The (AI) Fast Lane



Connect with confidence.





80
Regions



200+
Localization
Zones



11K+
Network
Adjacencies



FULL
Compute



Industry's
Best
SLAs

Netskope NewEdge Network



Government
of Canada



International
Organization for
Standardization



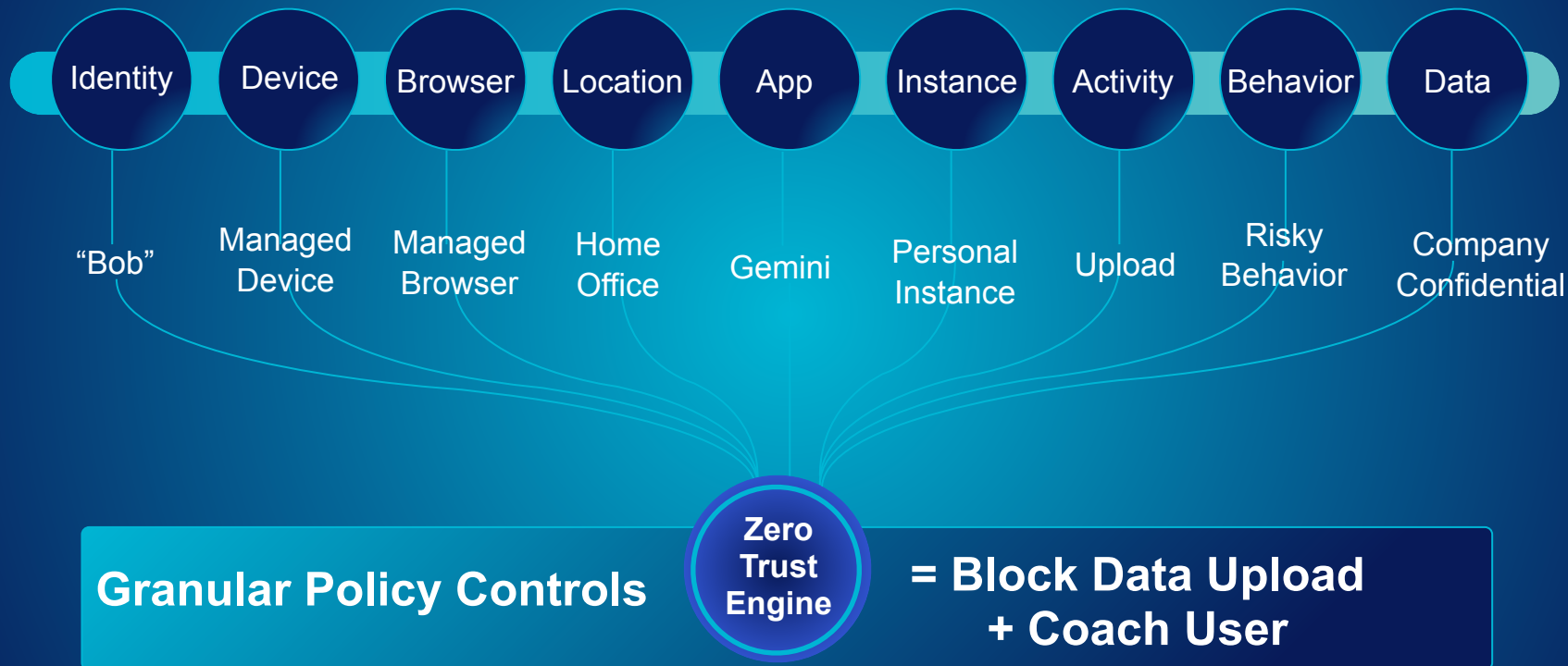
INTERNATIONAL
ELECTROTECHNICAL
COMMISSION



DATA PRIVACY
FRAMEWORK
PROGRAM



Context to Apply & Adapt Policy Controls



Full Data Security



Data Security Today

Protecting digital information from unauthorized access, corruption, or theft



Data in motion



Data in use



Data at rest

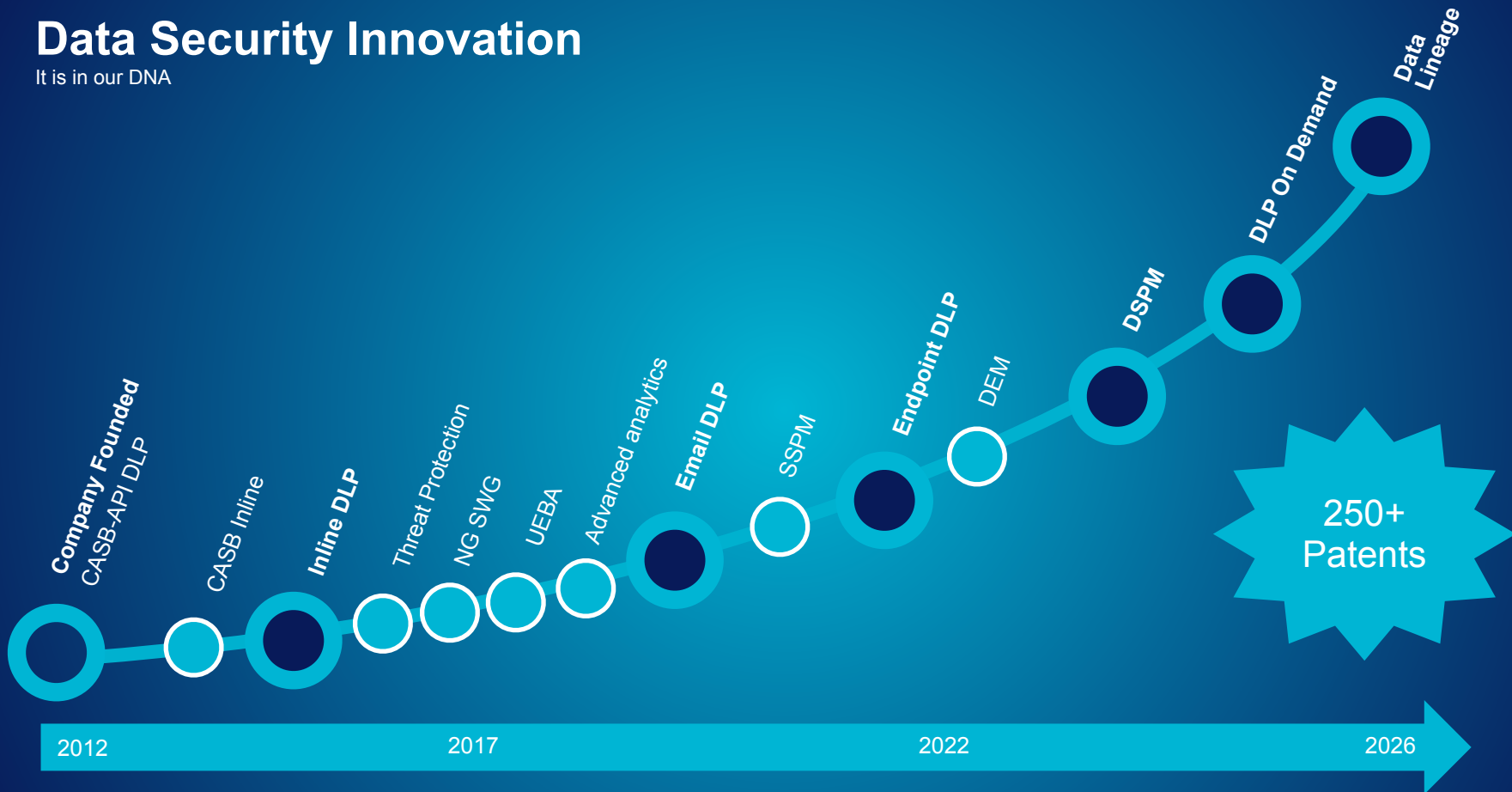
Agentic AI | Ransomware to exfiltration | Heavy rulebooks | Quantum concerns | Operational resilience

TL;DR: Data has the value of oil but flows like water.
Data needs to be ready for AI or AI Ready
Data value is going up with AI use



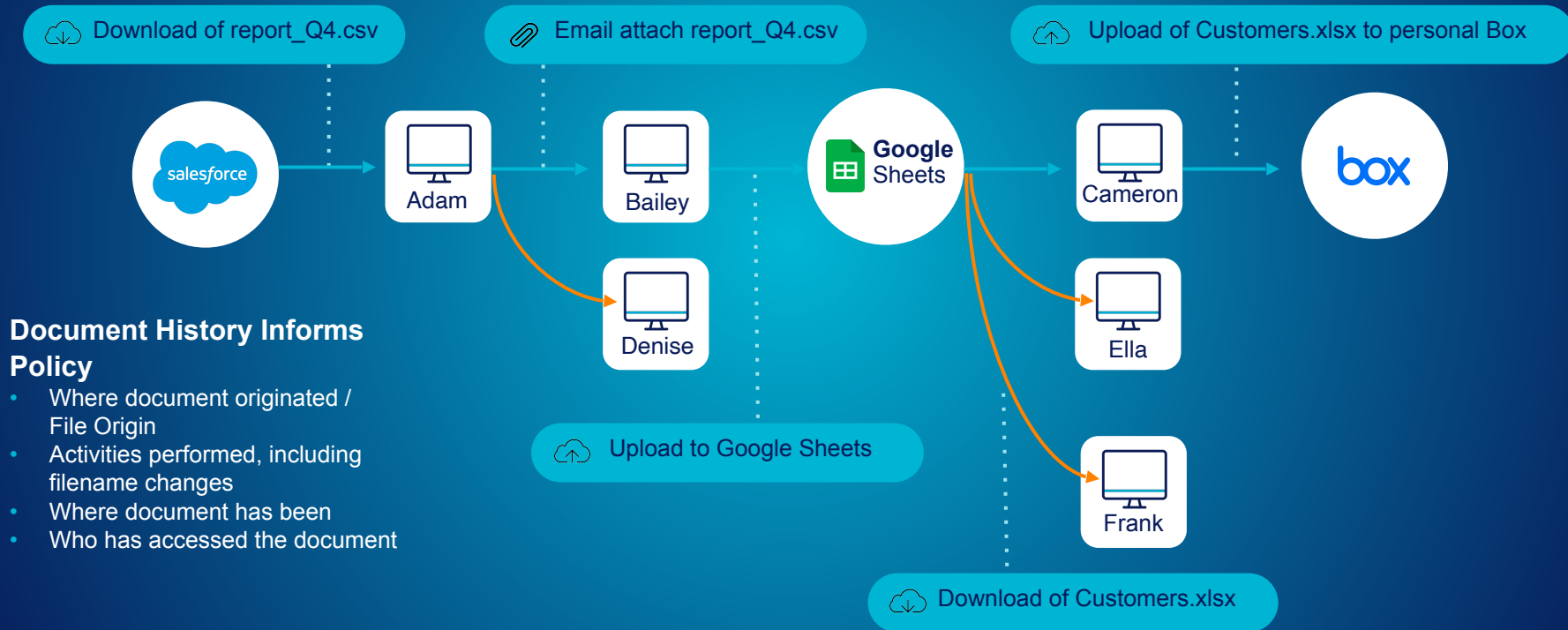
Data Security Innovation

It is in our DNA

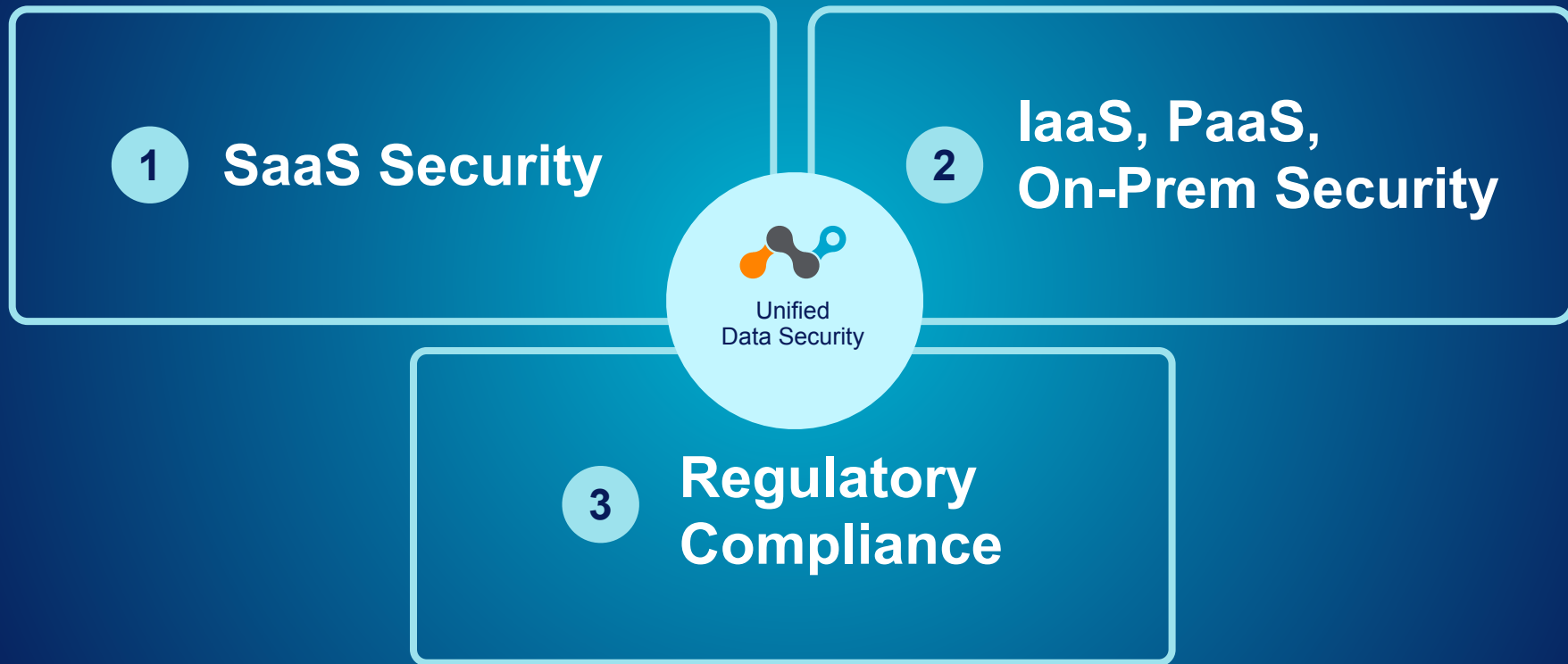


Data Lineage

Follow your sensitive data as it moves and mutates



3 Data Security Solution Areas



Unified Data Security in Netskope One

Unified Contextual Visibility

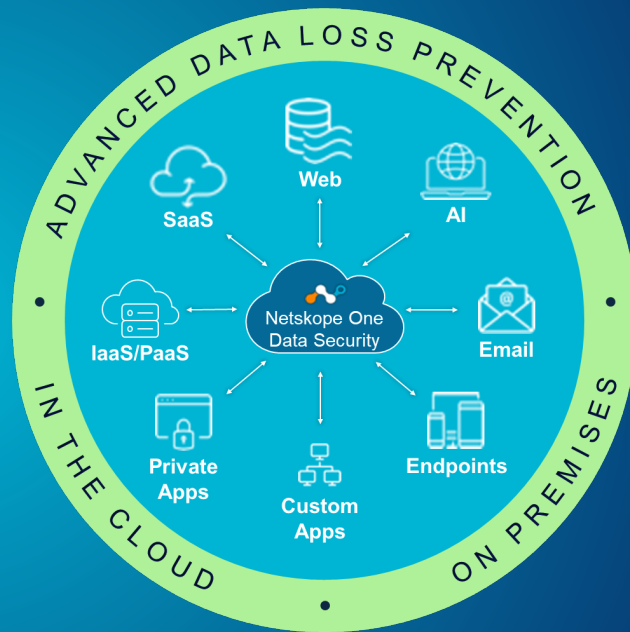
Unified Policy Controls

Unified Data Analytics

Data Journey Tracking

AI-Powered Data Classification

- 3K+ Data Identifiers
- 30+ AI/ML Models
- 40+ Regulatory and Compliance Templates

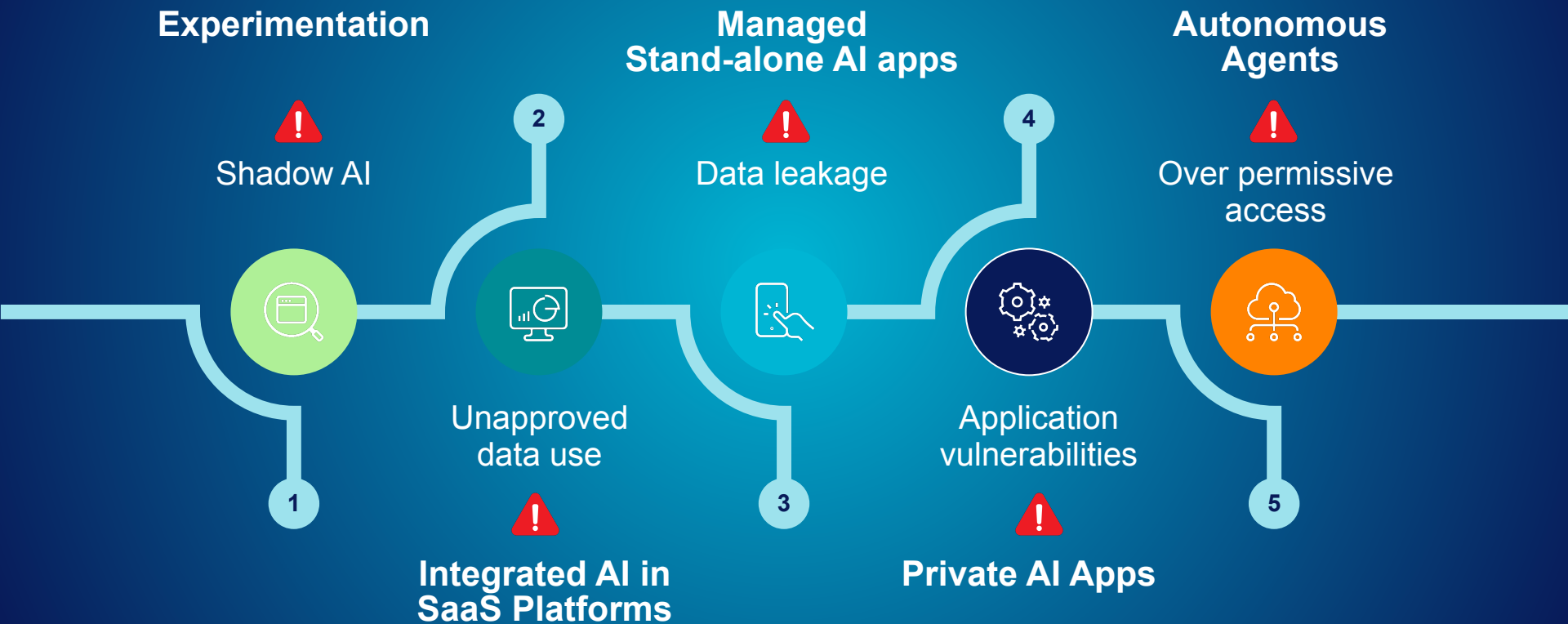


Data at Rest · Data in Use · Data in Motion
Structured and Unstructured

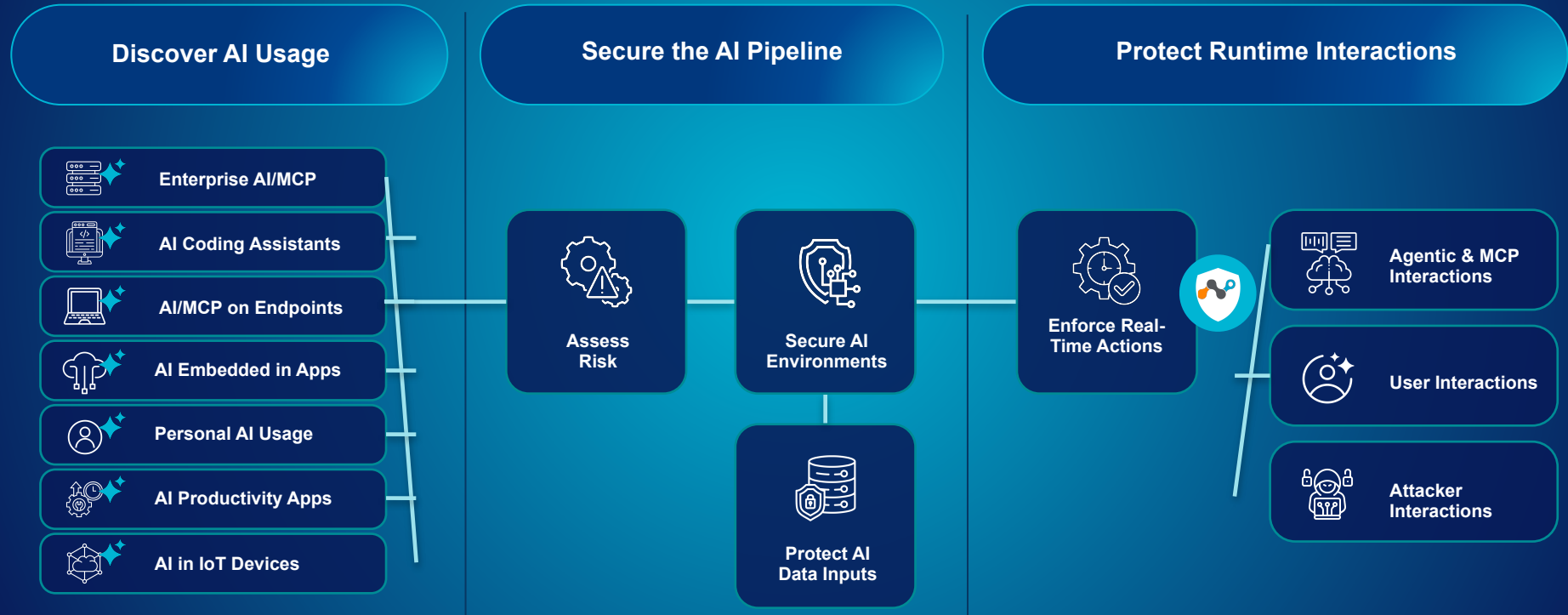
Smart AI Security



Common AI Adoption Journey



A Complete Solution to Protect the Whole AI Lifecycle

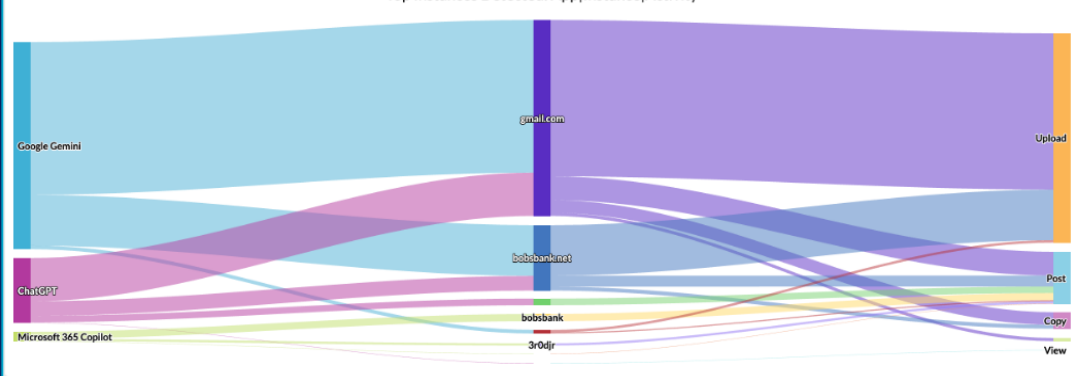




AI Discovery & Visibility

Start With What Is Happening Today

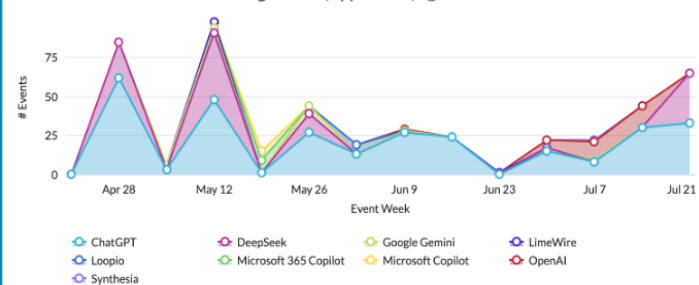
Top Instances Detected: App|Instance|Activity



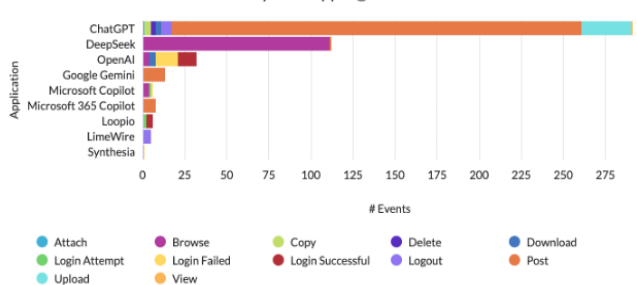
Instance Detail ⓘ

	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

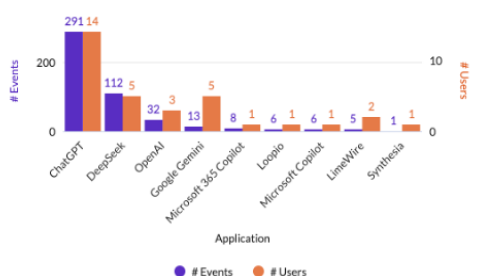
AI Usage Trend (App Events) ⓘ



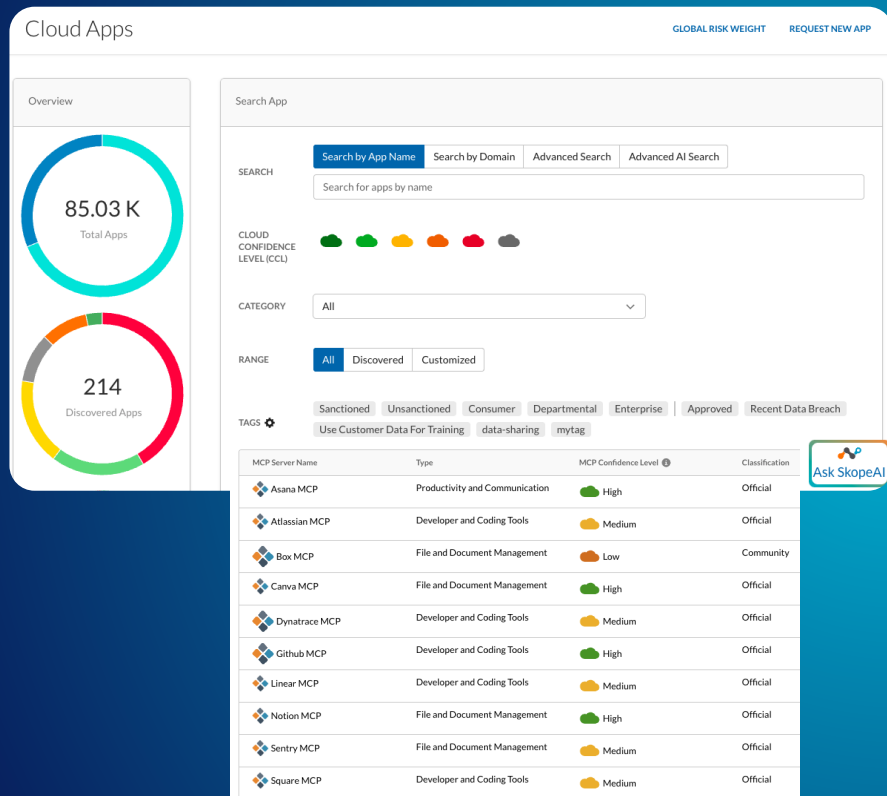
Activity in AI Apps ⓘ



AI Apps in Use (Event & User Count)



Layer On Risk Details



Gen AI-powered risk categorization of apps



Adaptive risk scores



Detail on embedded AI capabilities



Includes MCP risk scoring

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?





Secure the AI Pipeline



Understand Where Your Data Lives and Flows

Data Stores > Data Store Inventory

Data Store Inventory

Connected | Discovered

Sensitive Fields: 30 Sensitive Files: 22

All (12/409) AWS (2/388) GCP (0/6) Azure (0/5) Microsoft 365 (3) Google Workspace (7)

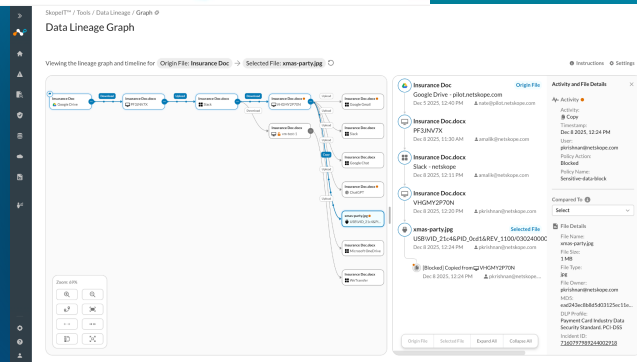
Connected (12) Discovered (397) Archived (0)

Default View: [icon]

Filter [v] Search contents...

12 Data Stores

	Data Store	Platform	Service	Owners	Region	Data Store Sensitivity Score	Data Store Risk Rating	Sensitive Types
▶	developers.kio	Google Worksp...	Google Drive		US-SVS	38	0	Z
▶	niklaudres.on	Microsoft 365	OneDrive	YV	US-SVS	0	0	0
▶	developers.kio	Google Worksp...	Google Drive		US-SVS	0	0	0
▶	developers.kio	Google Worksp...	Google Drive		US-SVS	0	0	0
▶	niklaudres.on	Microsoft 365	OneDrive		US-SVS	0	0	0



Protect Data in AI Interactions



Protect Against Threats Before Model Deployment

Attack Success Rate Breakdown

Categories	Attack Success Rate
 Inappropriate Content - Piracy and Copyright	47%
 Inappropriate Content - Requests for Sensitive Data	28%
 Inappropriate Content - Hate Speech and Discrimination	19%
 Inappropriate Content - Crimes	11%
 Inappropriate Content - Weapons	11%
 Inappropriate Content - Suicide and Self-Harm	6%
 Inappropriate Content - Sex-Related Crimes and Content	6%



- Automate adversarial simulations
- Uncover vulnerabilities
- Ensure your LLMs are safe, secure, and compliant





Protect Runtime Interactions



Secure Your Users and Agents, Everywhere



Protect Against AI-Specific Threats



New 0 Found [Detection Settings](#)

▲	Name	Match Type	Last Edited
	Crimes or Weapons	Predefined Categories	Edited Jan 07, 2026 by bob@netskope.com ...
	Hate Speech and Discrimination	Predefined Categories	Created Jan 07, 2026 by bob@netskope.com ...
	Keyword Matching - Coit Tower	Predefined Categories, Matched Keywords	Edited Feb 07, 2026 by bob@netskope.com ...
	Piracy and Copyright	Predefined Categories	Created Jan 07, 2026 by bob@netskope.com ...
	Prompt Injection and JailBreaking	Predefined Categories	Created Jan 07, 2026 by bob@netskope.com ...
	Requests for sensitive data	Predefined Categories	Edited Feb 07, 2026 by bob@netskope.com ...
	Sex Related Crimes and Content	Predefined Categories	Edited Jan 07, 2026 by bob@netskope.com ...
	Suicide and Self Harm	Predefined Categories	Created Jan 07, 2026 by bob@netskope.com ...



Thank You!





APPENDIX





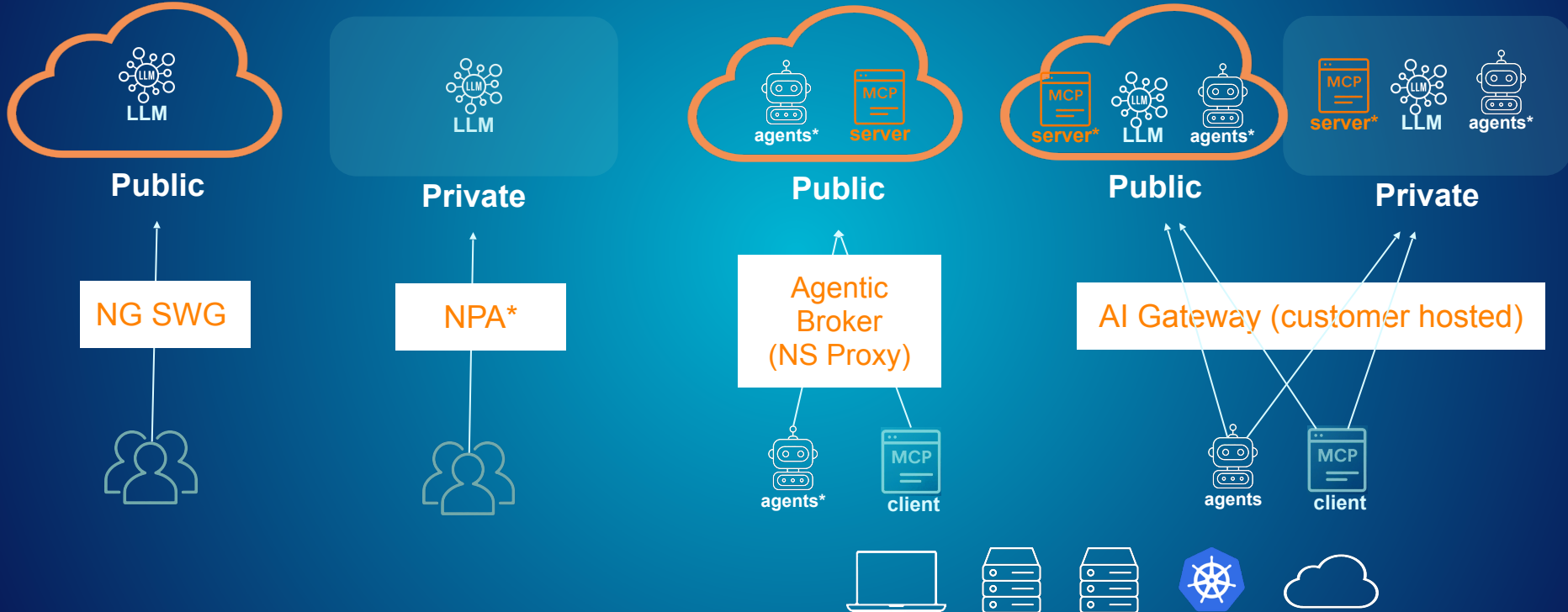
General Architecture



Classes of Interactions and Protection Enforcement Points

User Interactions

Agentic Interactions

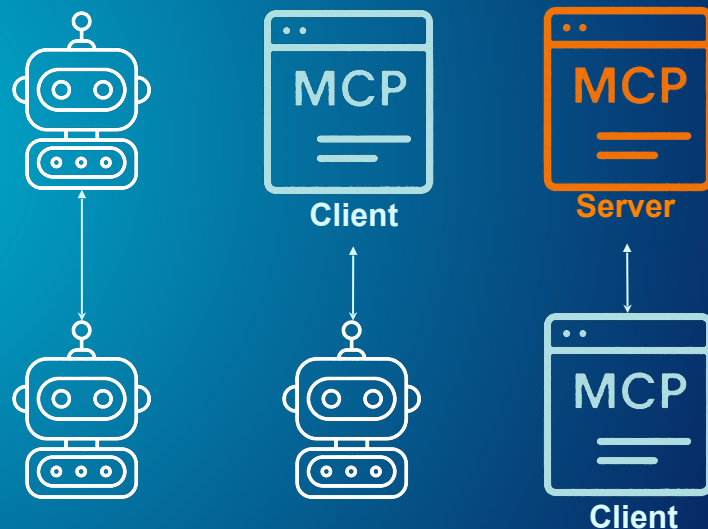


What Does Runtime Interactions Mean?

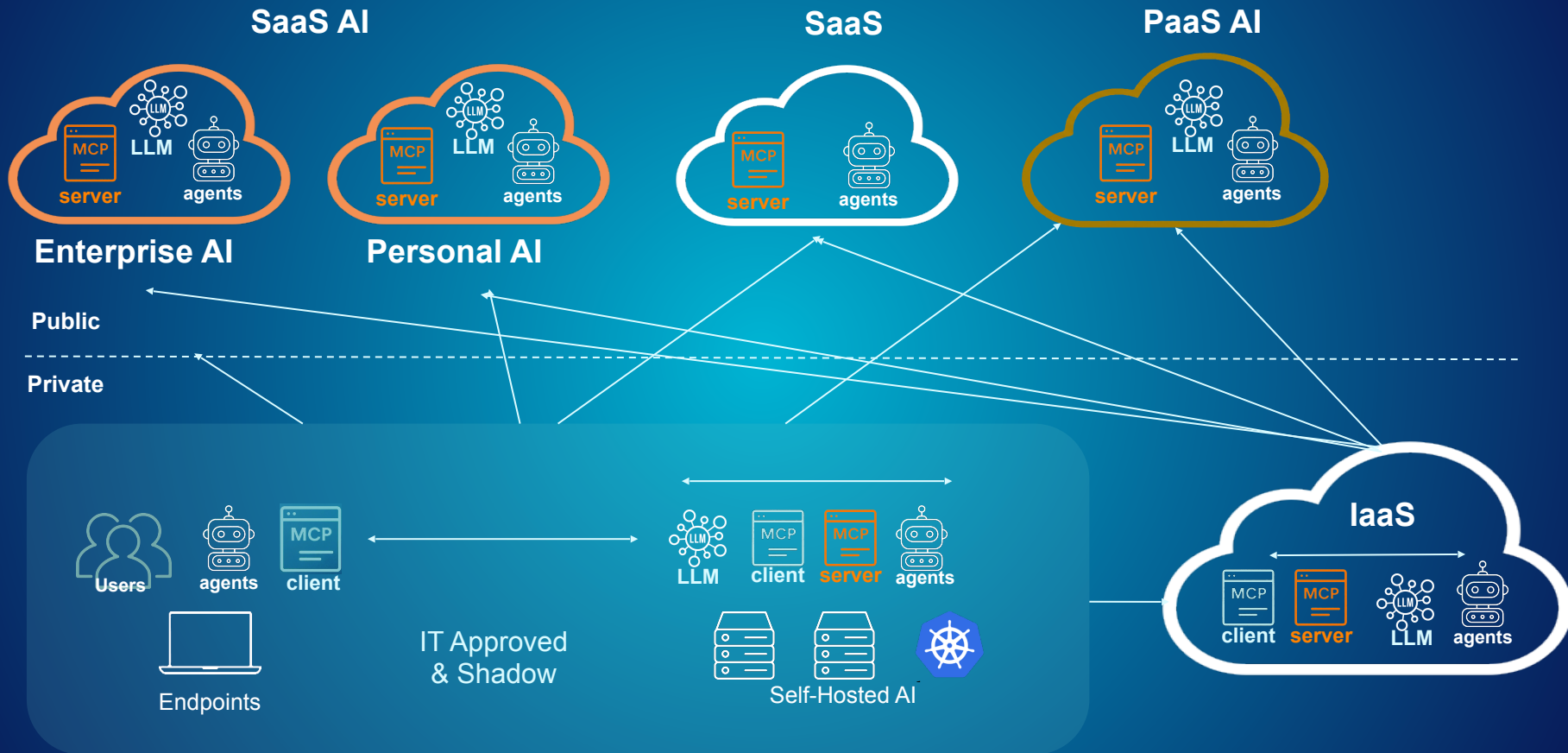
Interactions with the model



Agent to Agent Interactions

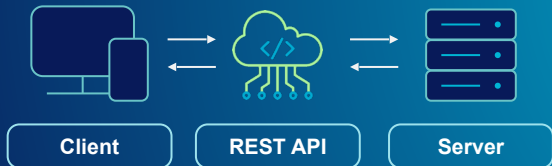


AI Interactions and Deployment Models

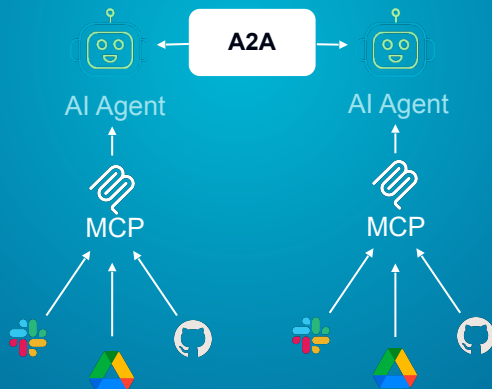


APIs and JSON are the Language of the Modern Internet

Application Programming Interfaces (“API”)

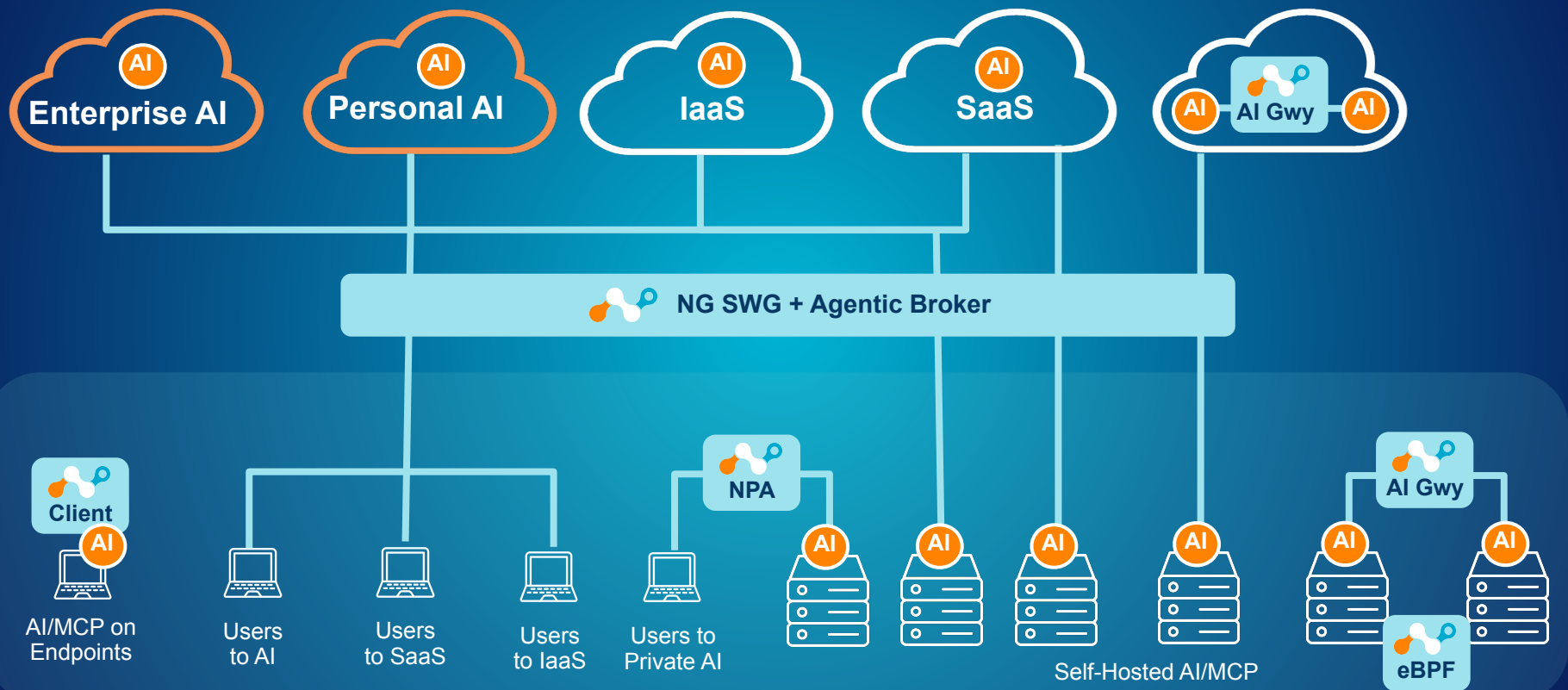


Model Context Protocol (“MCP”) Agent-to-Agent (“A2A”)



JavaScript Object Notation (“JSON”)

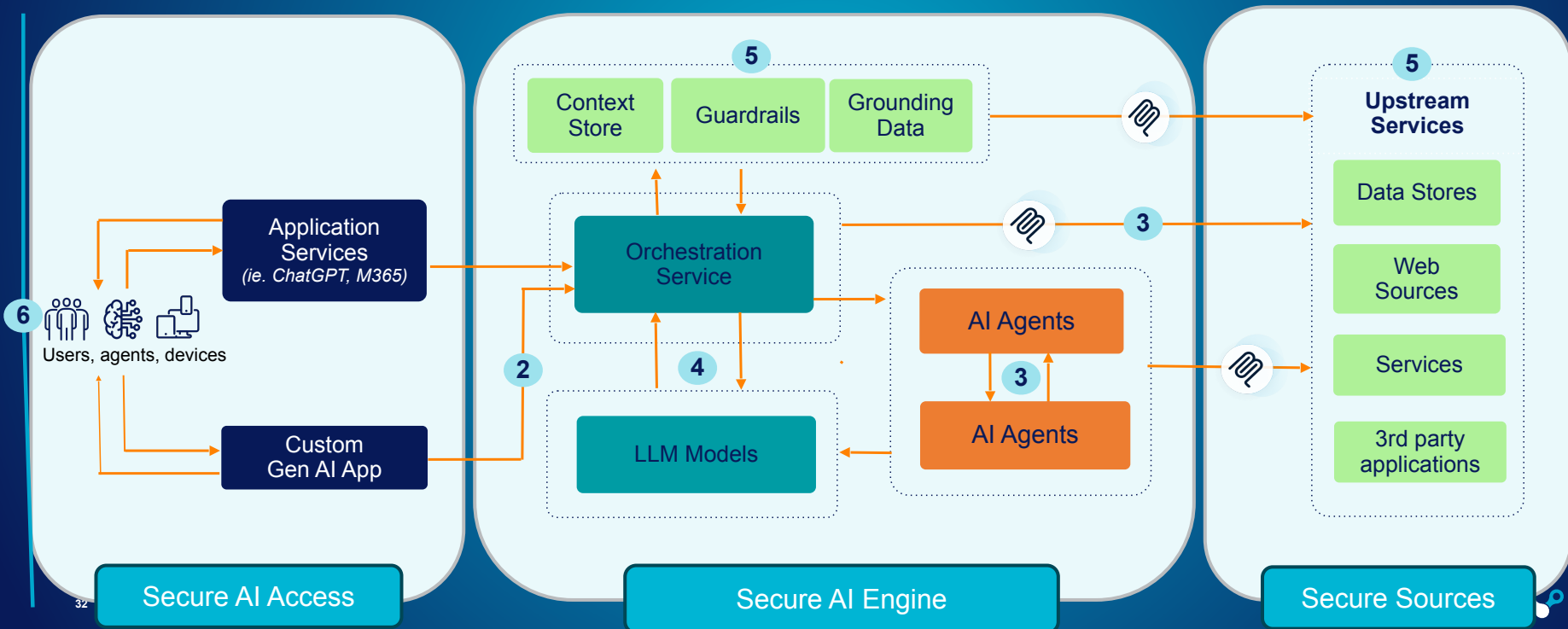
```
{
  "user": "asmith@acmecorp.com",
  "action": "delete",
  "details": {
    "file_id": "q637atu7uds912uib",
    "metadata": {
      "created_date": "2025-04-13",
      "file_size": "2MB"
    }
  }
}
```



AI Architecture: Key Use Cases



- 1 [Secure access to AI tools](#)
- 2 [Secure custom AI apps](#)
- 3 [Secure agentic interactions](#)
- 4 [Protect from emerging AI threats](#)
- 5 [Protect AI data pipeline](#)
- 6 [Maintain a secure and compliant AI posture](#)



Securing AI with Netskope One Platform



CASB Inline

NPA

AI Adv Threat

SSPM

CASB API

DSPM

DLP-aaS

AI-SPM

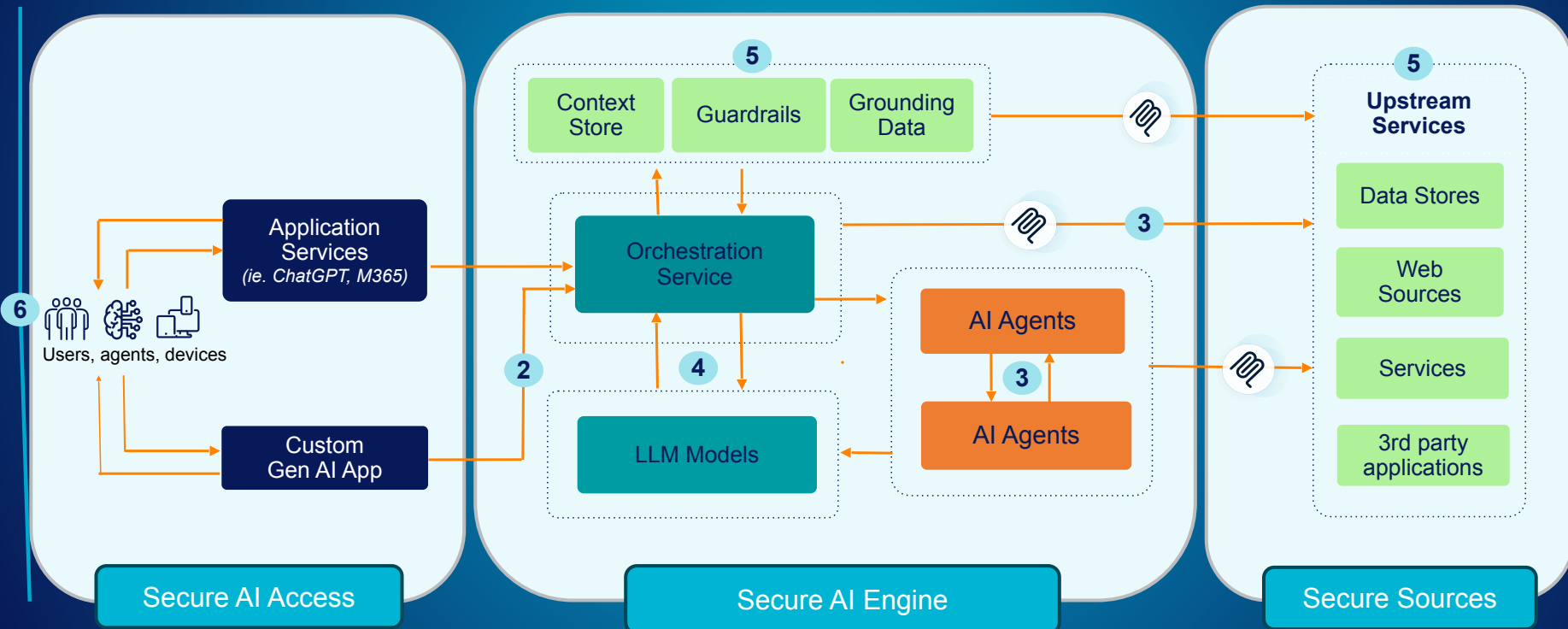
AI Gateway

Red Teaming

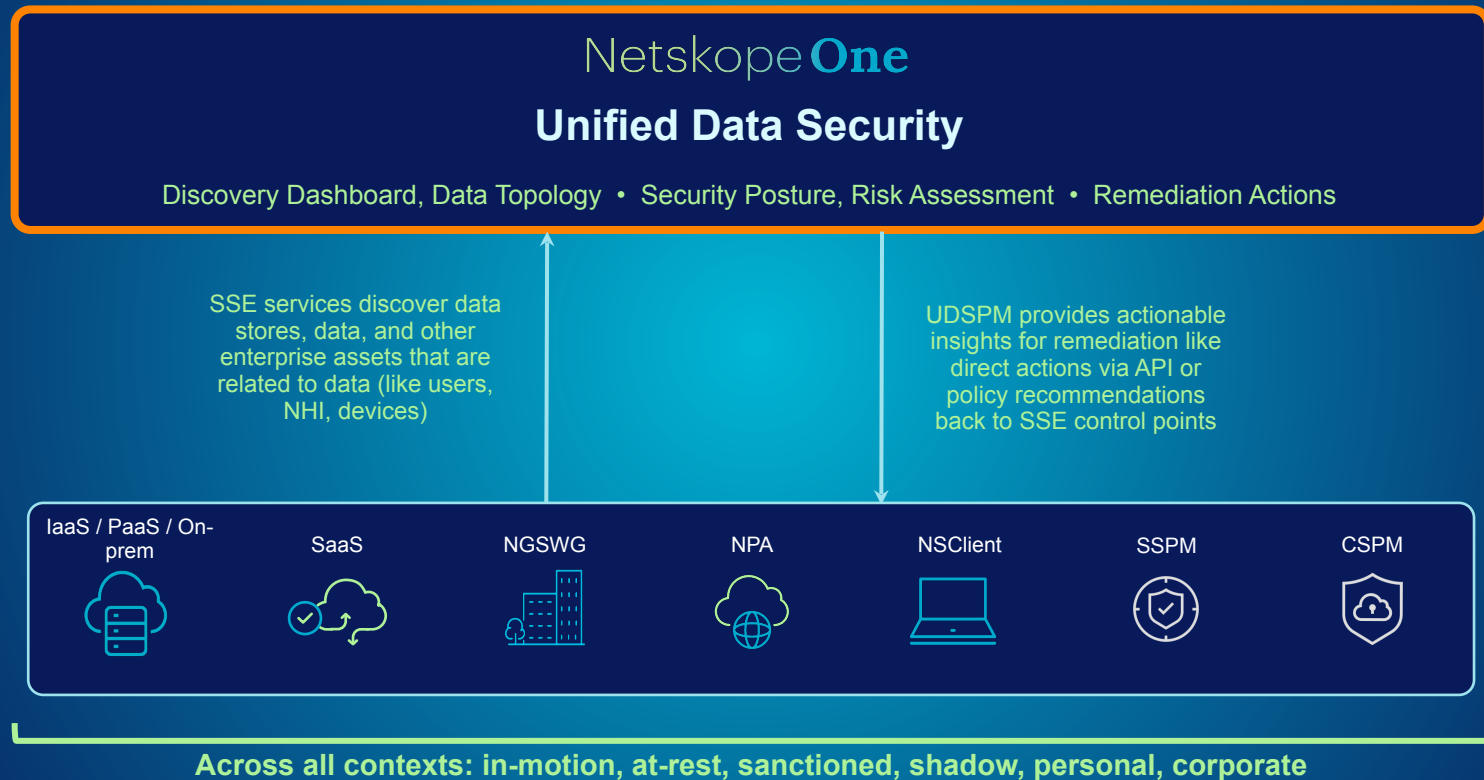
DSPM

SSPM

CASB API

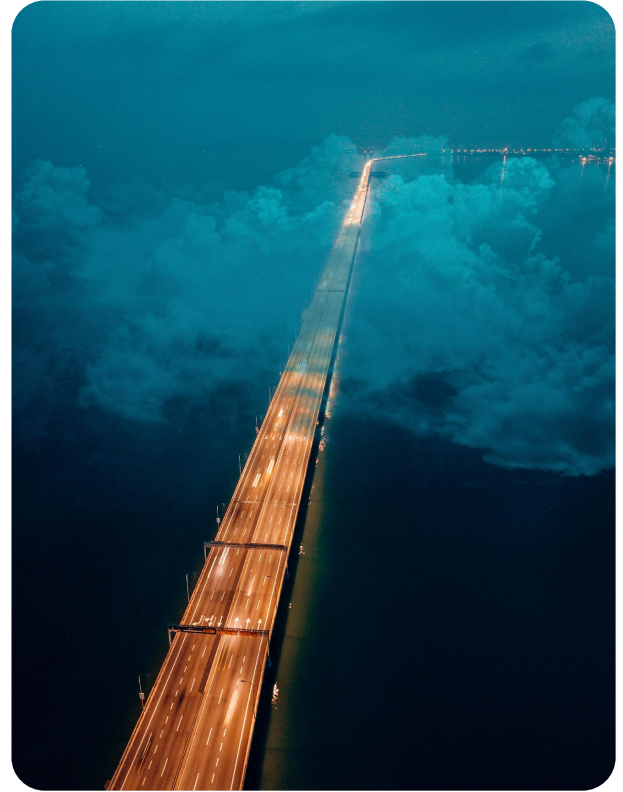


AI Security with Unified Data Security





Additional Use Cases



Overcoming AI Concerns



I want...

No blind spots

No shadow AI

**To get full visibility,
I need:**

Discover AI usage

- Apps usage
- User, API, and MCP activity
- Embedded AI in SaaS
- Managed vs. Shadow AI

AI Governance

- Dataflow and policy triggers
- App and MCP
Server Inventory



AI Discovery & Visibility

User to App

User to SaaS traffic

NG SWG

AI Guardrails

Personal & Managed AI Apps

AI Embedded in SaaS

Agents

Agentic Traffic (MCP)

Agentic Broker

MCP Servers

Custom App to LLM

App to LLM Traffic (API)

AI Gateway

Custom Built Apps

Data Sources

Data Flows

CASB Inline

Data Flows & Policy Triggers



3 Ways We Remove AI Concerns



Blind to unauthorized AI use



Discovered 40+ shadow AI tools



Silent roll-out embedded AI in SaaS



Visibility of app AI features



Unsafe use of AI by development



Visibility of policy violations and user coaching / app steering

3 Ways We Remove AI Concerns



Blind to unauthorized AI use



Discovered 40+ shadow AI tools



Silent roll-out embedded AI in SaaS



Visibility of app AI features



Unsafe use of AI by development



Visibility of policy violations and user coaching / app steering

3 Ways We Remove AI Concerns



Blind to unauthorized AI use



Discovered 40+ shadow AI tools



Silent roll-out embedded AI in SaaS



Visibility of app AI features



Unsafe use of AI by development



Visibility of policy violations and user coaching / app steering

Questions to Reveal AI Concerns

Q.

How does official AI adoption compare to unauthorized employee usage?



Blind to unauthorized AI use



Discovered 40+ shadow AI tools

Q.

What's your process for approving new AI tools and features and how quick is it?



Silent roll-out embedded AI in SaaS



Visibility of app AI features

Q.

How often do business units / teams bypass IT to use AI?



Unsafe use of AI by development



Visibility of policy violations and user coaching / app steering





Total AI & Data Control



I want...

**Secure models
& data**

**Compliant AI
by design**

**To get full AI control,
I need:**

- Automated risk assessment (App, LLM, MCP)
- Integrate security in dev pipelines

**To get full data control,
I need:**

- Discover, classify, and label data
- Understand where data lives and flows
- Test model prompts and responses pre-deployment



Secure the AI Pipeline

**User to
App**

Assess SaaS AI Risk

NG SWG

AI Guardrails

AI App Risk

AI Risk in SaaS App

Agents

Assess MCP Risk in SaaS

Agentic Broker

MCP Server Risk

**Custom
App to
LLM**

LLM Vulnerability Testing

AI Red Teaming

Public & Private LLMs

**Data
Sources**

Data Inputs for AI

DSPM

Discover, Classify, & Label



3 Ways We Control AI and Data



✗ MCP integrations pose security & compliance risk

✓ Evaluate over 1K MCP servers for risk



✗ Malicious prompts expose sensitive internal secrets.

✓ Simulate attacks to harden models before deployment



✗ Unsecured ingestion leaks sensitive patient data

✓ Discover & classify training data to ensure compliance

3 Ways We Control AI and Data



✗ MCP integrations pose security & compliance risk

✓ Evaluate over 1K MCP servers for risk



✗ Malicious prompts expose sensitive internal secrets

✓ Simulate attacks to harden models before deployment



✗ Unsecured ingestion leaks sensitive patient data

✓ Discover & classify training data to ensure compliance

3 Ways We Control AI and Data



✗ MCP integrations pose security & compliance risk

✓ Evaluate over 1K MCP servers for risk



✗ Malicious prompts expose sensitive internal secrets

✓ Simulate attacks to harden models before deployment



✗ Unsecured ingestion leaks sensitive patient data

✓ Discover & classify training data to ensure compliance

Questions to Uncover Control Needs

Q.
How do you assess
the risk of AI tools to
the business

✗ MCP integrations pose
security & compliance risk

✓ Evaluate 1K MCP
servers for risk

Q.
How are you securing
AI development
through the lifecycle?

✗ Malicious prompts expose
sensitive internal secrets

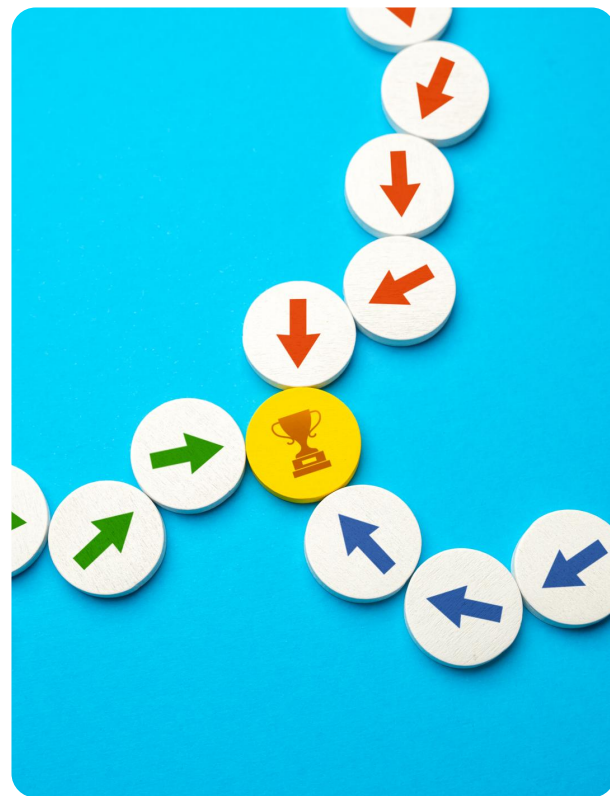
✓ Simulate attacks to
harden models before
deployment

Q.
How do you manage
sensitive data
fuelling your AI
models?

✗ Unsecured ingestion leaks
sensitive patient data

✓ Discover & classify training
data to ensure compliance





Achieve AI Acceleration



I want to...

**Manage AI behavior
in real time**

**Protect against AI
threats**

To Accelerate AI, I need:

- Inline inspection of all AI interactions
- Block prompt injection, jailbreaks, and data exfiltration
- Moderate content for safe use
- Apply rate limits and cost controls



**User to
App**

Access & Content Inspection

NG SWG

AI Guardrails

User Access

Agents

MCP Server Access

Agentic Broker

Access & Interactions

**Custom
App to
LLM**

Access & Content Inspection

AI Gateway

NPA

Access & Rate Limiting

**Data
Sources**

Data Usage & Interactions

DLP

Data Protection



**Protect Runtime
Interactions**



3 Ways We Accelerate AI



✗ Employees paste sensitive PII into AI chats

✓ Inline DLP stops data loss in prompts



✗ Clever prompts trick AI into leaking secrets

✓ Block jailbreaks and connects events



✗ Overprivileged public bot exploited via prompt injection

✓ Extend zero trust access to agentic AI

3 Ways We Accelerate AI



✗ Employees paste sensitive PII into AI chats

✓ Inline DLP stops data loss in prompts



✗ Clever prompts trick AI into leaking secrets

✓ Block jailbreaks and connects events



✗ Overprivileged public bot exploited via prompt injection

✓ Extend zero trust access to agentic AI

3 Ways We Accelerate AI



✗ Employees paste sensitive PII into AI chats

✓ Inline DLP stops data loss in prompts



✗ Clever prompts trick AI into leaking secrets

✓ Block jailbreaks and connects events



✗ Overprivileged public bot exploited via prompt injection

✓ Extend zero trust access to agentic AI

Questions to Identify How Fast They Are Going

Q.
How would you
prove no PII had
been uploaded to a
public LLM?

✗ Employees paste sensitive
PII into AI chats

✓ Inline DLP stops data
loss in prompts

Q.
How do your
analysts reconstruct
a suspicious AI
interaction?

✗ Clever prompts trick AI into
leaking secrets

✓ Block jailbreaks and
connects events

Q.
How are you
evolving zero trust
strategies to cope
with agents?

✗ Overprivileged public bot
exploited via prompt injection

✓ Extend zero trust access
to agentic AI



Six Key Challenges for Securing GenAI



Visibility into managed and unmanaged AI usage across the organization

1

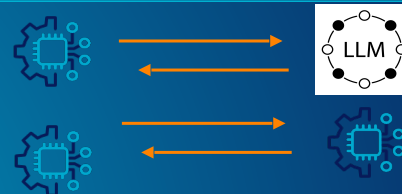
Securing user access to AI tools



AI Guardrails

4

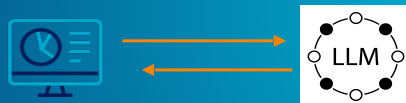
Securing agentic interactions*



Agentic Broker

2

Securing custom AI apps



AI Gateway

5

Protecting from emerging AI threats*



AI Red Teaming

3

Protecting the AI data pipeline



AI Gateway

6

Maintaining secure and compliant AI posture*



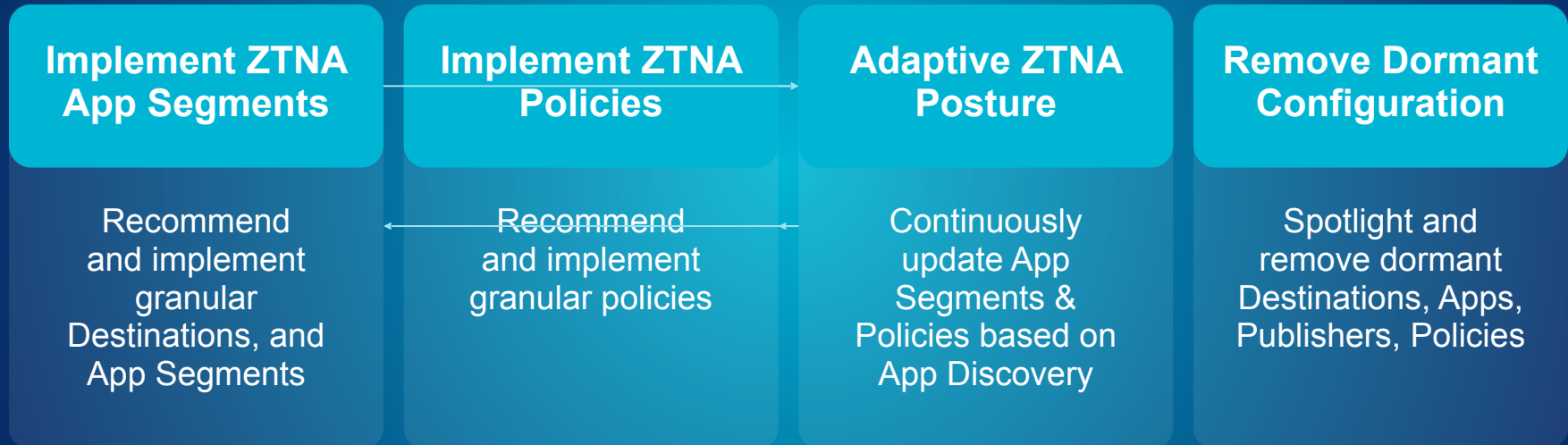
- AI asset inventory, usage
- Attack paths
- Misconfigurations
- Access privileges

AI-SPM



Example 1: Operationalizing ZTNA Agent

Agent drives ZTNA Posture



App Discovery feedback



Example 1: Adaptive ZTNA Posture

The screenshot displays the Netskope interface for policy management. The main window is titled "Policy Improvement Recommendation" and shows a recommendation based on 380 events by 27 users from July 1, 2025, to July 31, 2025. The current policy is "NPA-US-Policy for wordpress". The recommendation is divided into "Current" and "Recommendations" sections. The "Current" section lists users (User Group 1, 2, 3, 4) and app segments ([private-app-1], [private-app-2], [private-app-3], [Wordpress], [private-app-4]). The "Recommendations" section lists users (User Group 1, 2, 3, 4, 5, 8) and app segments ([private-app-1], [private-app-2], [private-app-3], [Wordpress], [private-app-4]). A "Wordpress" changes section shows new destinations (10.1.1.0/28, 192.168.1.1) and new ports (TCP 443). The interface includes buttons for "Ignore", "Preview Changes", and "Approve & Auto Create".

Policy Improvement Recommendation

This recommendation is based on 380 events by 27 users from Jul 1, 2025 to Jul 31, 2025. [View Raw Events](#)

Policy Name
NPA-US-Policy for wordpress

Current

Users

User Group 1 User Group 2 User Group 3
User Group 4

App Segments

[private-app-1] [private-app-2]
[private-app-3] [Wordpress] [private-app-4]

Recommendations

Users

User Group 1 User Group 2 User Group 3
User Group 4 User Group 5 User Group 8

App Segments

[private-app-1] [private-app-2]
[private-app-3] [Wordpress] [private-app-4]

[Wordpress] Changes

New Destinations
10.1.1.0/28 192.168.1.1

New Ports
TCP 443

[Ignore](#) [Preview Changes](#) [Approve & Auto Create](#)

Copilot Recommendation

- Update Private App Segment [Wordpress]
- Update policy NPA-US-Policy for wordpress

Step 1 Update [Wordpress] Step 2 Update Policy

Edit Private App Policy

What's the policy's goal:
Select policy goal you are trying to achieve with this Private App policy

Private App Access DLP Threat Protection

Criteria
Source, and Destination sections are AND'ed together.

Source

Match ALL of the following selections

User = User Group 1 User Group 2
User Group 3 User Group 4
User Group 5 User Group 6

Access Method = Client

Destination

Private App = [Wordpress]

[Ignore](#) [Edit Note](#) [Approve & Save](#)





Competitive/Differentiators



3 Top Differentiators

1

Ease of Operationalization

- Single Console integration of NG-SWG with AI Guardrails, AI Red Teaming and AI Gateway
- Single Policy Engine of AI Guardrails alongside Threat and Data Protection Profiles
- Flexible CPU/GPU-based containerized guardrail deployment for regulated environments
- Phased Rollout Capabilities (monitor > coach > enforce)

2

Securing GenAI apps, MCP traffic, and Private LLMs

- Granular GenAI URL Sub-Categories
- GenAI CCI Attributes & Tags
- GenAI app instance awareness and activity-based controls (GenAI App Connectors)
- Risk Rating for 1000s of MCP servers
- Granular activity visibility & control for MCP
- Auth and Rate Limiting for cost control
- Tight integration with DLP on Demand for file scanning
- Coaching instead of blocking responses ("Replace" action)

3

Data Security Leadership

- Supporting over 3,000 data identifiers, AI/ML classifiers, exact data matching, OCR, and fingerprinting
- Covers data in motion and at rest across SaaS, web, email, endpoints, and private apps
- End-to-end data lineage capabilities that track data from origin to destination
- Comprehensive across all channels including SaaS, web, email, private apps, and endpoints



Security & Networking Differentiators

Security

- + We speak the language of the Internet (API/JSON). Competitors don't, they're web proxies.
- + Robust, granular data protection.
- + AI is foundational and embedded throughout Netskope One

Networking

- + Unrivaled visibility and control. Competitors are at the mercy of cloud providers. We see every packet.
- + Industry leading performance and connectivity. 10k network adjacencies.





Product Tech Slides



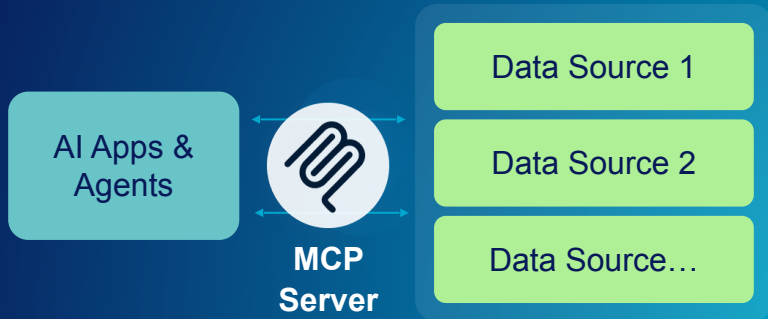


Secure MCP (Model Context Protocol) Usage

Netskope One Agentic Broker



Secure MCP (Model Context Protocol) Usage



- MCP servers enable simple bi-directional data sharing between apps, agents, and LLMs
- Risk of data leakage or unauthorized access
- Lack of visibility, control, and protection



Netskope One Agentic Broker

- Visibility, Control, and Protection for MCP usage
- Real-time policy enforcement and DLP
- Prevent risky activities and data leakage



Securing MCP: Private Preview (Beta): Inventory

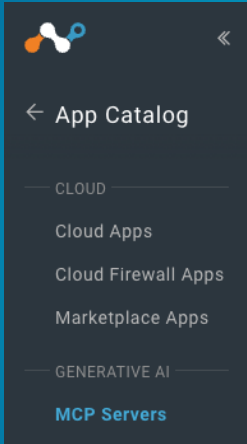
"Give me a list of our MCP servers and clients"

1. MCP Servers Catalog

- MCP Servers in AppCatalog (e.g., Atlassian) with risk score
- New category="MCP" added to CCI and all the MCP servers listed in the same
- Risk score based on 19 attributes like protocol version, authentication, installation type, transport type etc.
- 100+ MCP Servers (Q1 '26)
- 1000+ MCP Servers (Q2 '26)

2. MCP Registry (Q2 '26)

- For active in-use MCP servers



The screenshot shows a mobile app interface for 'App Catalog'. It has a dark theme with a sidebar menu. The menu categories are 'CLOUD' (Cloud Apps, Cloud Firewall Apps, Marketplace Apps) and 'GENERATIVE AI' (MCP Servers). The 'MCP Servers' category is highlighted in blue.

MCP Server Name	Type	MCP Confidence Level ⓘ	Classification
 Asana MCP	Productivity and Communication	 High	Official
 Atlassian MCP	Developer and Coding Tools	 Medium	Official
 Box MCP	File and Document Management	 Low	Community
 Canva MCP	File and Document Management	 High	Official
 Dynatrace MCP	Developer and Coding Tools	 Medium	Official
 Github MCP	Developer and Coding Tools	 High	Official
 Linear MCP	Developer and Coding Tools	 Medium	Official
 Notion MCP	File and Document Management	 High	Official
 Sentry MCP	File and Document Management	 Medium	Official
 Square MCP	Developer and Coding Tools	 Medium	Official



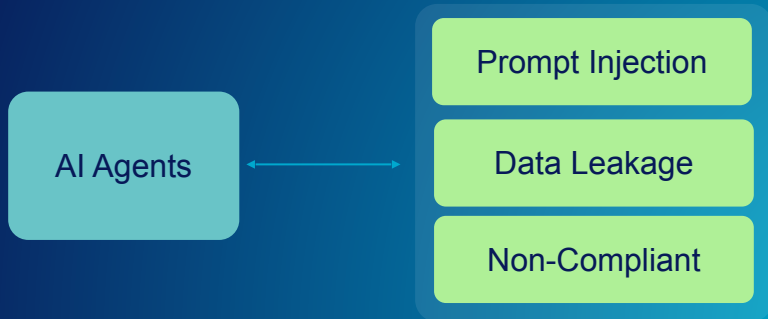


Secure Agentic Interactions

Netskope One AI Gateway & AI Guardrails



Secure Agentic Interactions



- Agentic Interactions present a blind spot
- Risk of data leakage and threats
- Lack of visibility, control, and protection



Netskope One AI Gateway & AI Guardrails

- Visibility, Control, and Protection for AI Agents
- Content moderation and DLP
- Detect and stop threats in real-time



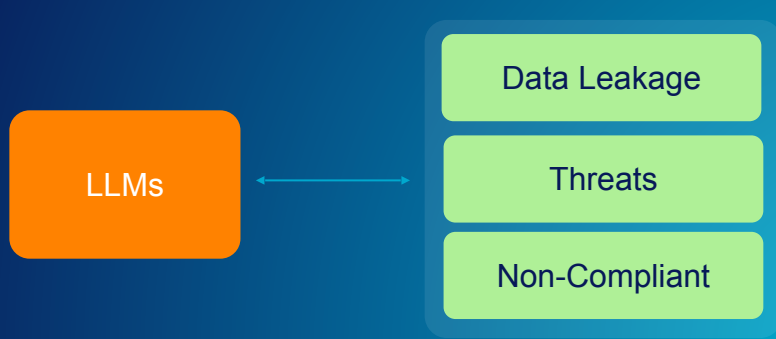


Secure your LLMs

*Netskope One AI Red Teaming & AI-SPM**



Secure Your LLMs



- LLMs are becoming a key part of enterprise apps
- LLM providers lack adequate built in guardrails
- Risk of data leakage, compliance issues, threats



Netskope One AI Red Teaming & AI-SPM*

- Automate adversarial simulations
- Uncover vulnerabilities
- Ensure your LLMs are safe, secure, and compliant
- Continuous assessment of misconfigurations/vulns across AI models, data pipelines, and deployment environments*





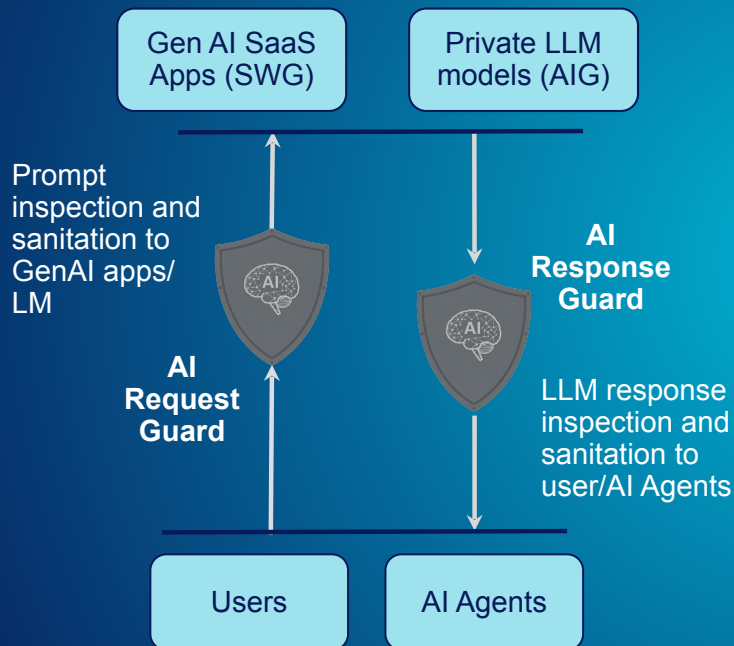
AI Guardrails

Deep inspection & content moderation with comprehensive threat mapping



Protect from Emerging AI Threats with AI GuardRails

Inline Security from AI Threats and Content Moderation for **SWG and AI Gateway**



New Engine with LLM for Gen AI and Agentic AI content moderation

- Inspect Requests to Gen AI
- Inspect Responses from Gen AI
- Detection for AI threats - prompt injection and jailbreaking
- Detection of inappropriate content categories such as violence, hate & discrimination, weapons, sexual content, piracy and copyrighted material
- Custom keyword matching

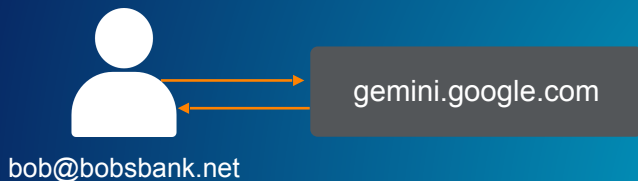
Integrated with SWG and AI Gateway for GenAI and Agentic AI

Framework mapping to OWASP T10, MITRE ATLAS

Integration with UEBA for anomalous interactions



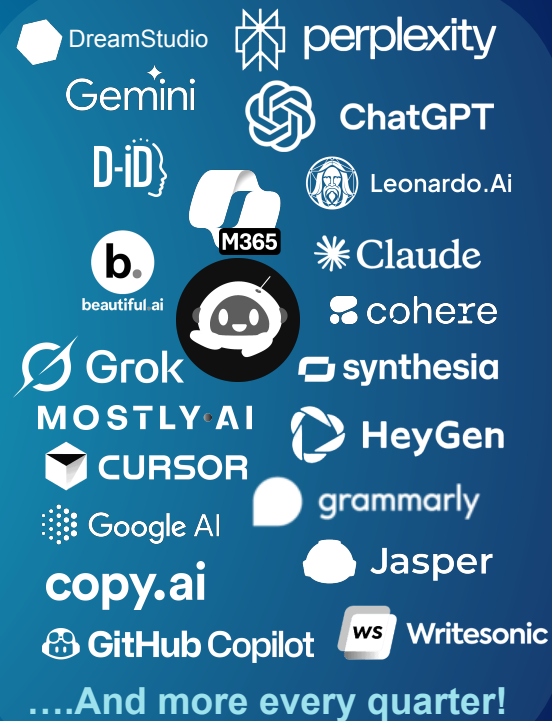
Protect: Control non-compliant AI Usage



- 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



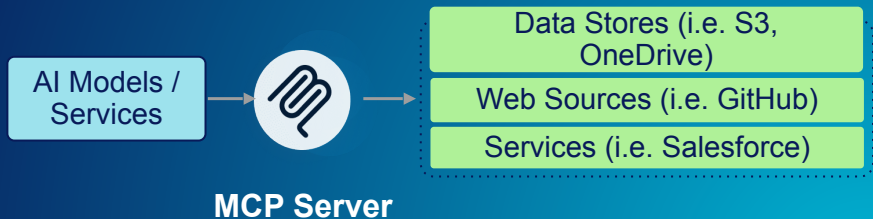


AI Gateway

Critical enforcement point for interactions between internal AI apps and private or public managed LLMs



Secure Agentic Interactions in Private Deployments



- 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

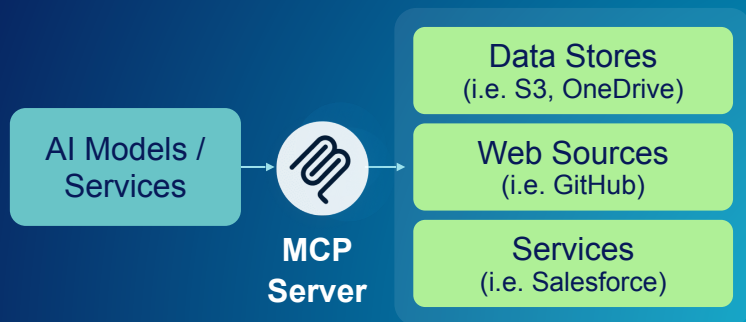


AI GW for

- Support for LLM gateway, MCP/A2A GW (roadmap)
- Visibility & access control + logging, monitoring, centralized authentication & rate limiting
- Content inspection for prompts and responses with DLP, Threat Protection and AI Guardrails



Protect: Secure Agentic Interactions



- Blind spots in AI-to-AI & 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 protects AI, MCP and A2A Interactions*

- Visibility & access control - logging, monitoring, auth & rate limiting
- Content inspection secures request / response, detects malware & prompt attacks, custom defined guardrails and prevents data leakage
- Optimized operations with auditability, model switching for reliability and performance, and data caching





AI Red Teaming

Stress tests models to ensure safety, availability, and continuity throughout the lifecycle



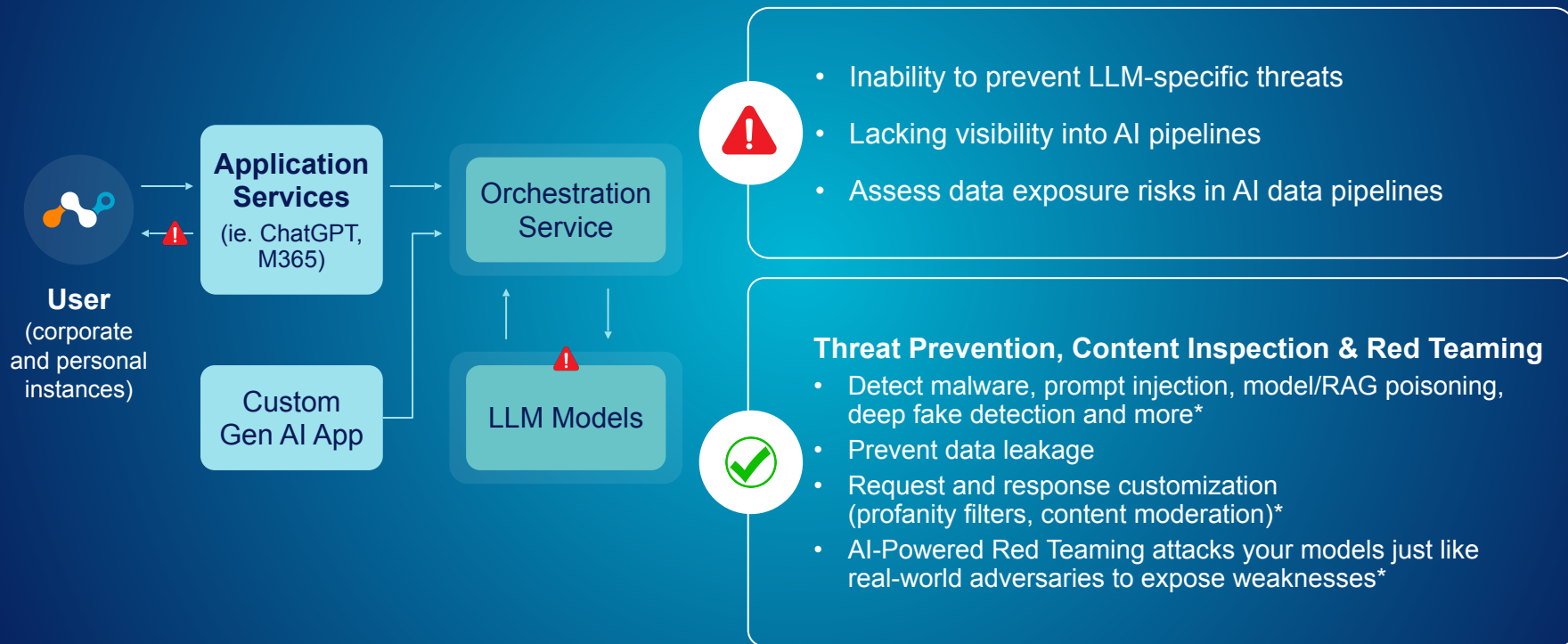
What is AI Red Teaming?

- 1. Sends simulated adversarial prompt testing requests to LLM models (or applications)
- 2. Assesses the security risks (including LLM vulnerabilities) based on the responses



The following outlines our product vision and direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Netskope's products remains at the sole discretion of Netskope.

Protect: Mitigating Attacker Threats





Agentic Broker

*Provides visibility, inventory, and control for public MCP
Server interactions*



Netskope's Securing Agentic Ecosystem - Strategy

- 1 Provide capabilities to discover & detect Agentic AI communication (e.g., MCP, A2A) to create visibility of their use in a customer environment
- 2 Provide ability to choose public MCP servers and agents for use (a risk rated Catalog), and track their deployments with live risk profiles in the enterprise (Registry)
- 3 Provide an integrated threat detection and access control through policy implementation in an organization to provide comprehensive enterprise wide coverage

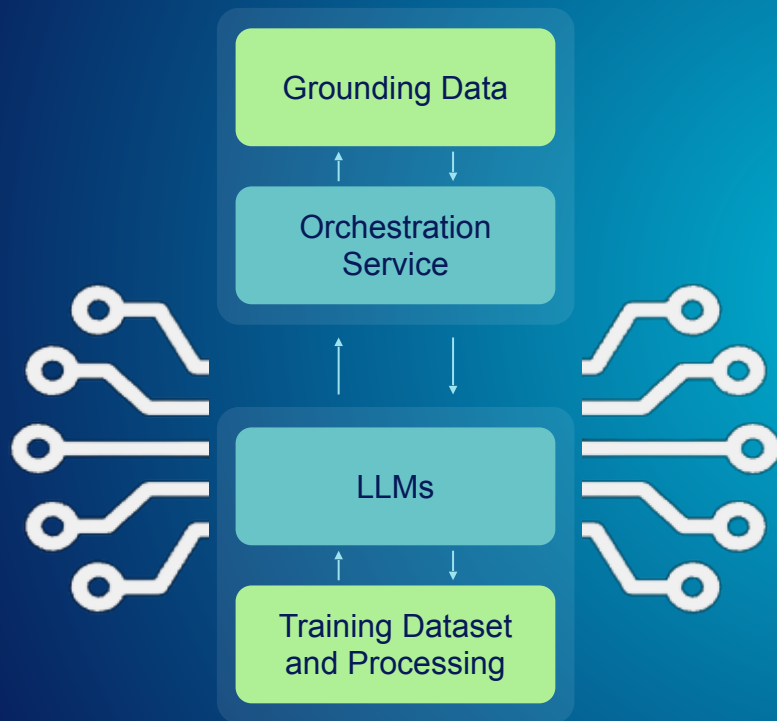


AI-SPM

continuous AI posture compliance



Secure: Protect The AI Environment



- Compliance at risk from AI-driven data use
- Inconsistent security controls across AI workloads
- Data leakage and misuse in prompt interactions
- Difficulty enforcing policy across distributed environments



AI Security Posture Management (AI-SPM)*

- Visibility to AI assets used in the organization
- Visibility into relationship between AI assets
- Identification of attack paths to the data stores
- Continuous assessment of misconfigurations/vulns across AI models, data pipelines, and deployment environments
- Access privilege evaluation