



Secure AI Day



Empower AI with Secure AI by Design

<To be filled by presenter>

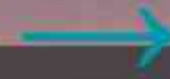
Date

Location



Agenda

Empower AI with
Secure AI by Design



Optional product demos

Secure Employee Use
of GenAI Apps



How to secure GenAI use



How to secure Gen AI
development



Securely Build
GenAI Apps



AI Is Evolving Faster Than Anyone Predicted

1B AI app users
in under two years.

“The ChatGPT launch 26 months ago was one of the craziest viral moments I’d ever seen, and we added one million users in five days.



[More recently] **we added one million users in the last hour.**”

Sam Altman, OpenAI



AI is Revolutionizing Business

Employees are using
GenAI applications.

Enterprises are building
AI applications.

57%
of Employees
Use Public GenAI
Apps Weekly.

Source: ZDNet, Feb. 2024



GenAI is Accelerating Positive Impacts for Your Business

Increased
productivity



40% higher worker
performance.

Better
collaboration



73% use AI to improve
communication
at work.

Transformed
marketing



43% of marketers
use AI to
generate content.

Sources: Harvard Business School, Grammarly, HubSpot

However...

As the Volume of GenAI Traffic Grows...

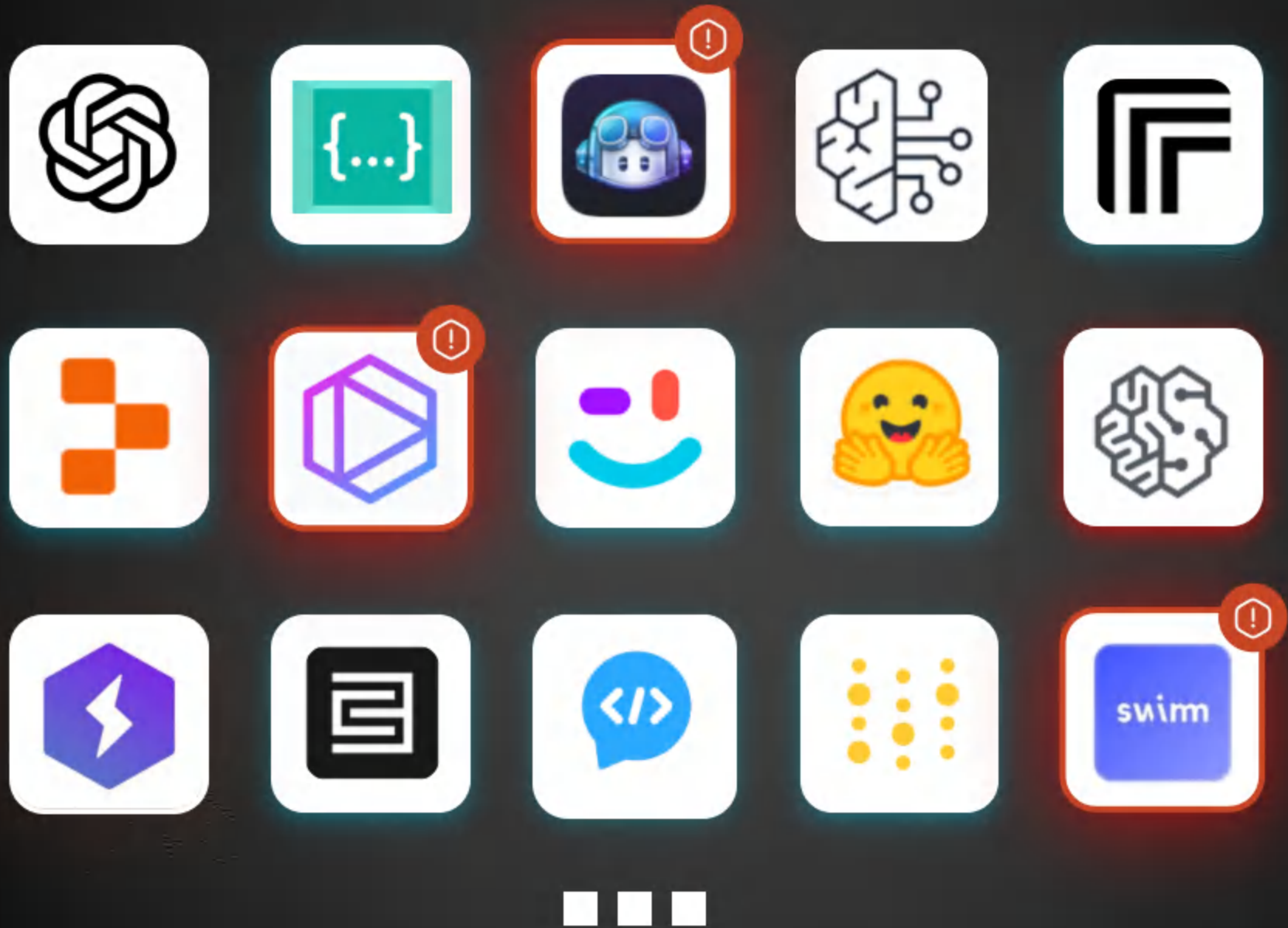
We're Seeing Data Incidents on the Rise



2.5X

Increase in
DLP
incidents
Q1 2025

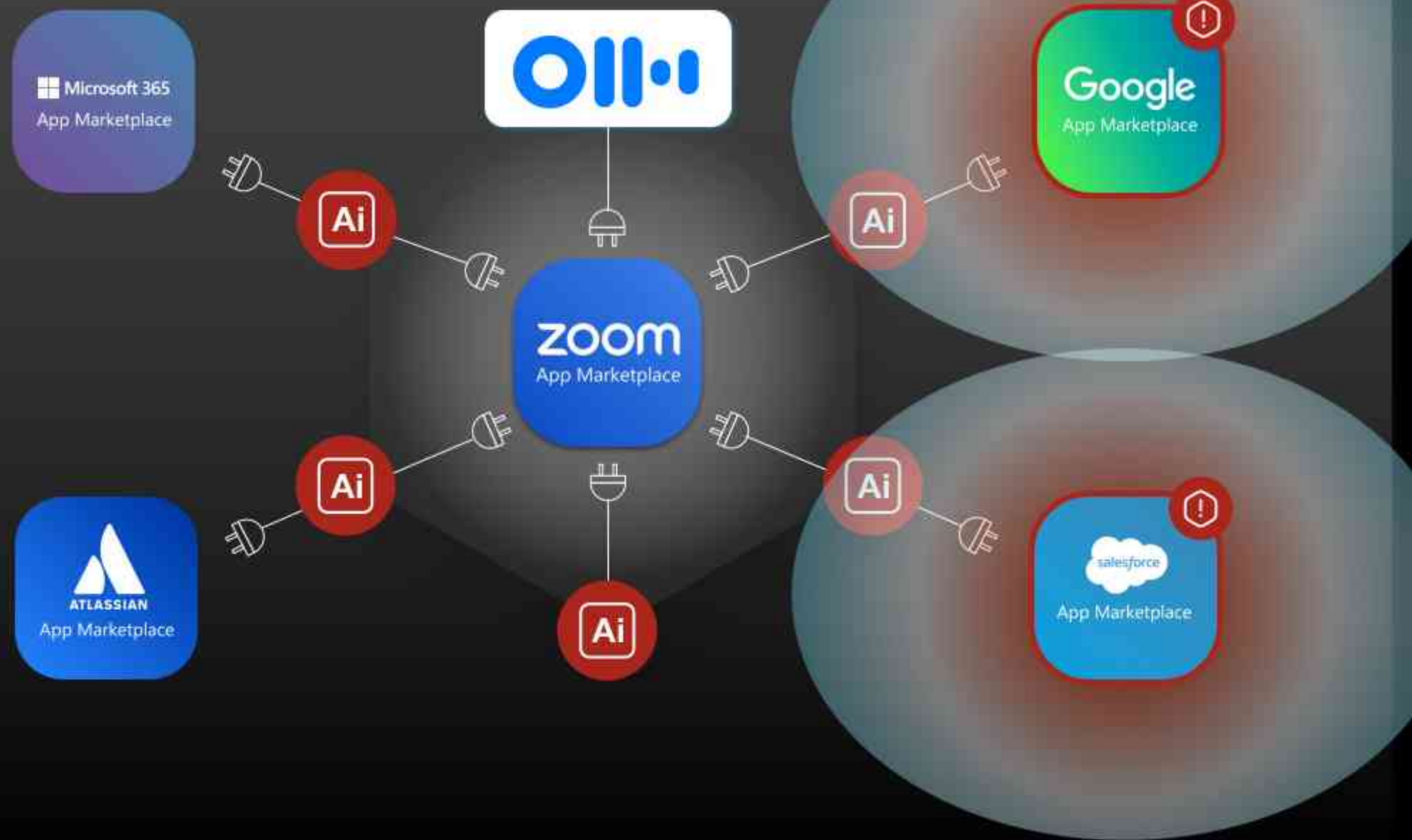
Among This Data May Reside
Protected or Other **Sensitive**
Information.



GenAI Apps Need Rigorous Scrutiny for Data Uploads

Employees may **unknowingly share confidential data** when using GenAI apps.

Uploaded data can be used to train AI models, potentially compromising proprietary information or **leading to unintended data leak**.



Undetected GenAI Plugins May Lead to Unauthorized Data Access

Interconnected SaaS ecosystems with **AI-powered third-party integrations** create **security vulnerabilities, complicating detection and control.**

This leads to **increased risk of security breaches and non-compliance** with regulatory requirements.



AI is Revolutionizing the Way We Work

Employees are using
GenAI applications.



How to secure
employee use of
GenAI applications?

Safely Embrace GenAI for Your Workforce



Show me what GenAI applications my employees are using.



Reduce the attack surface by limiting which AI tools employees can use and how they can use them.



Stop sensitive and proprietary data from being shared.



Secure against the next generation of threats.

Palo Alto Networks Puts You Back in Control of AI



Best-in-class visibility

- **4,000+** GenAI apps catalog
- Deep visibility into **80+ app** attributes by risk



Most options for access control

- **Policies** follow InfoSec guidance
- **Deepest controls** for sanctioned and tolerated apps
- **Responsible** GenAI coaching for users



AI-powered data protection

- LLM-powered, context-aware models classify data for **300+ categories**
- Easy **customization** for unique data
- Prevent data loss with **industry's only** SASE-integrated secure enterprise browser



Built on industry leading security platform

- Uncover interconnected **GenAI apps** in SaaS marketplaces
- Threat intelligence data from **70,000 customers** worldwide
- Natively **integrated** with industry-leading Cloud-Delivered Security Services

A modern glass skyscraper is shown from a low angle, reflecting the warm, golden light of a sunset. The building's facade is composed of many rectangular glass panels, some of which are illuminated from within, creating a glowing effect. The sky is a mix of orange, yellow, and blue, with some clouds visible. The overall mood is futuristic and innovative.

AI is Revolutionizing How We Do Business

Enterprises are building
AI applications.

AI Is Accelerating Outcomes Across All Industries

Launch
products faster



3x drug molecule
design.

Improve
customer service



72% of European companies
already benefiting from AI-
assisted customer support.

Accelerate
the business

Wendy's

75% of drive-through
orders automated.

Sources: McKinsey, Digitalization World, Google Cloud Blog

But This Is Leading to New Threats

61%

lack visibility
into ML assets.

**New AI ecosystem
risks from code
to runtime**

OWASP Top 10 LLM risks

Prompt injection

Sensitive information disclosure

Supply chain vulnerabilities

Data and model poisoning

Improper output handling

Excessive agency

System prompt leakage

Vector and embedding
weaknesses

Misinformation

Unbounded consumption

**Multiple new
attack types to
protect against**

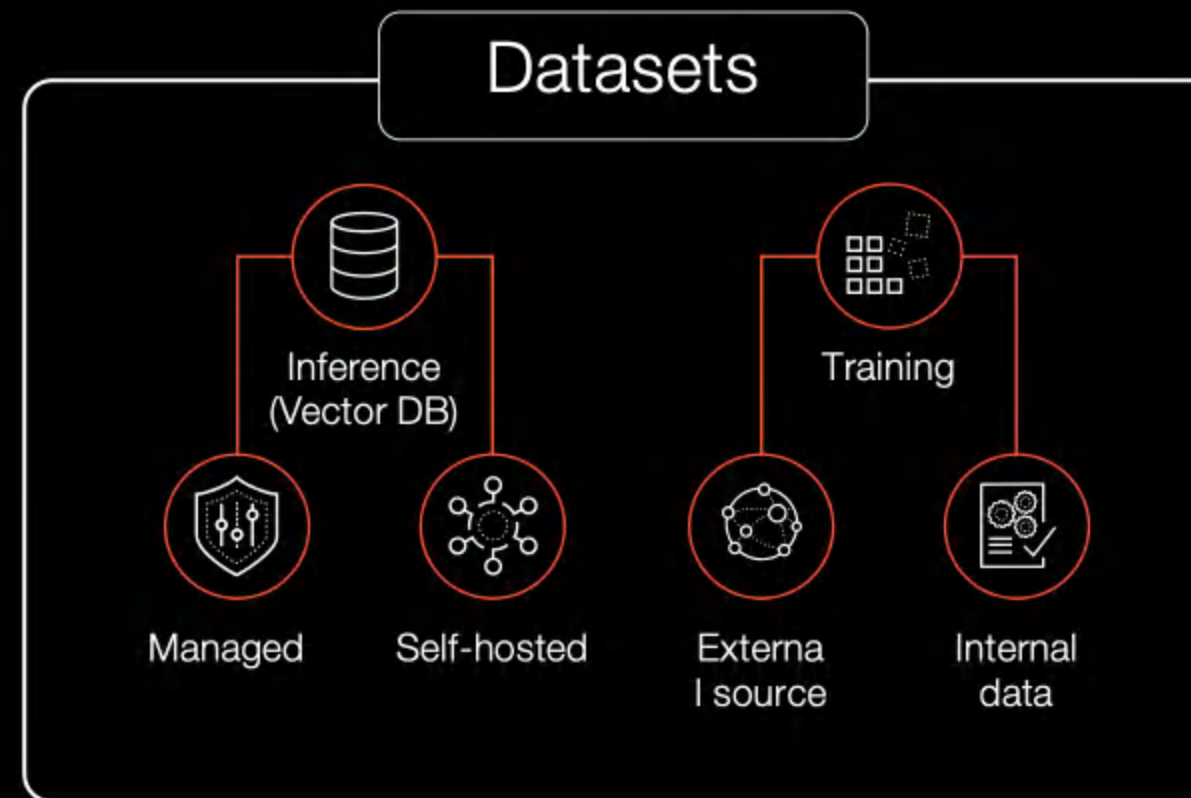
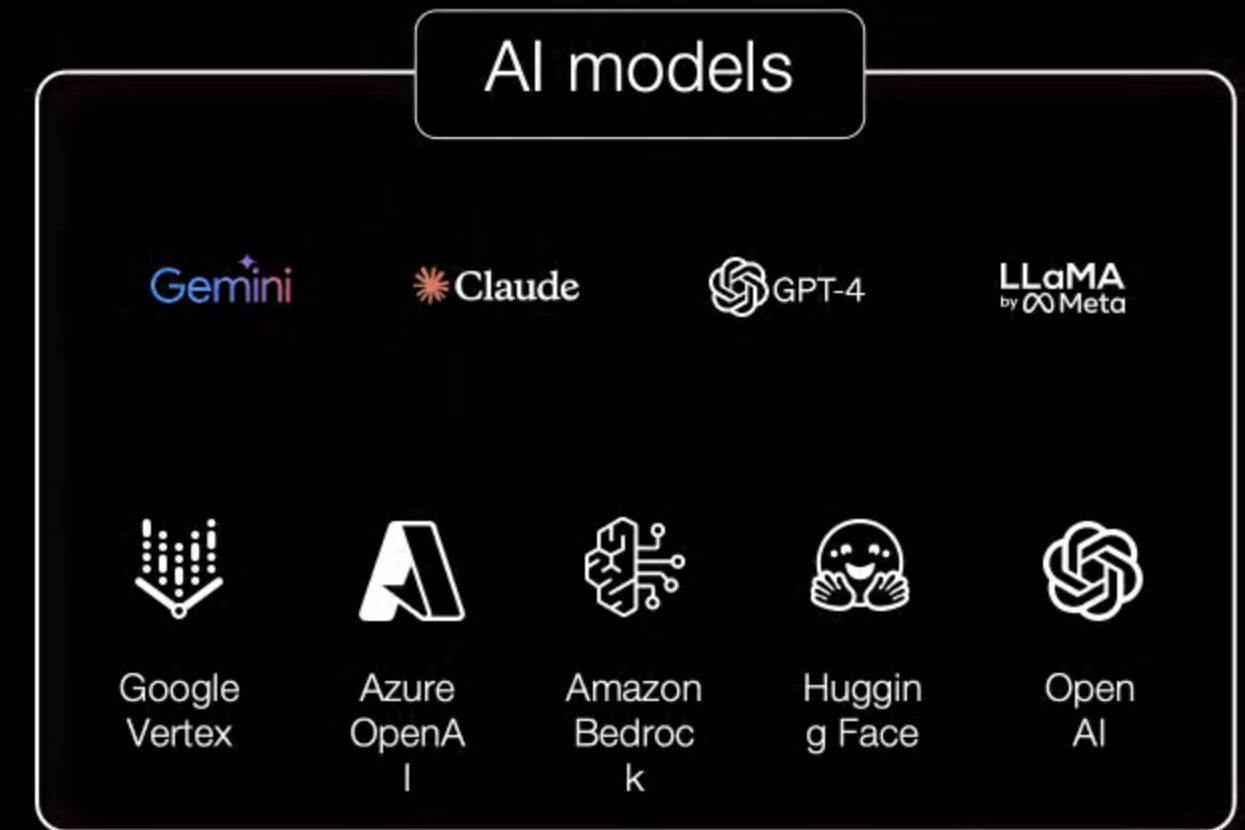
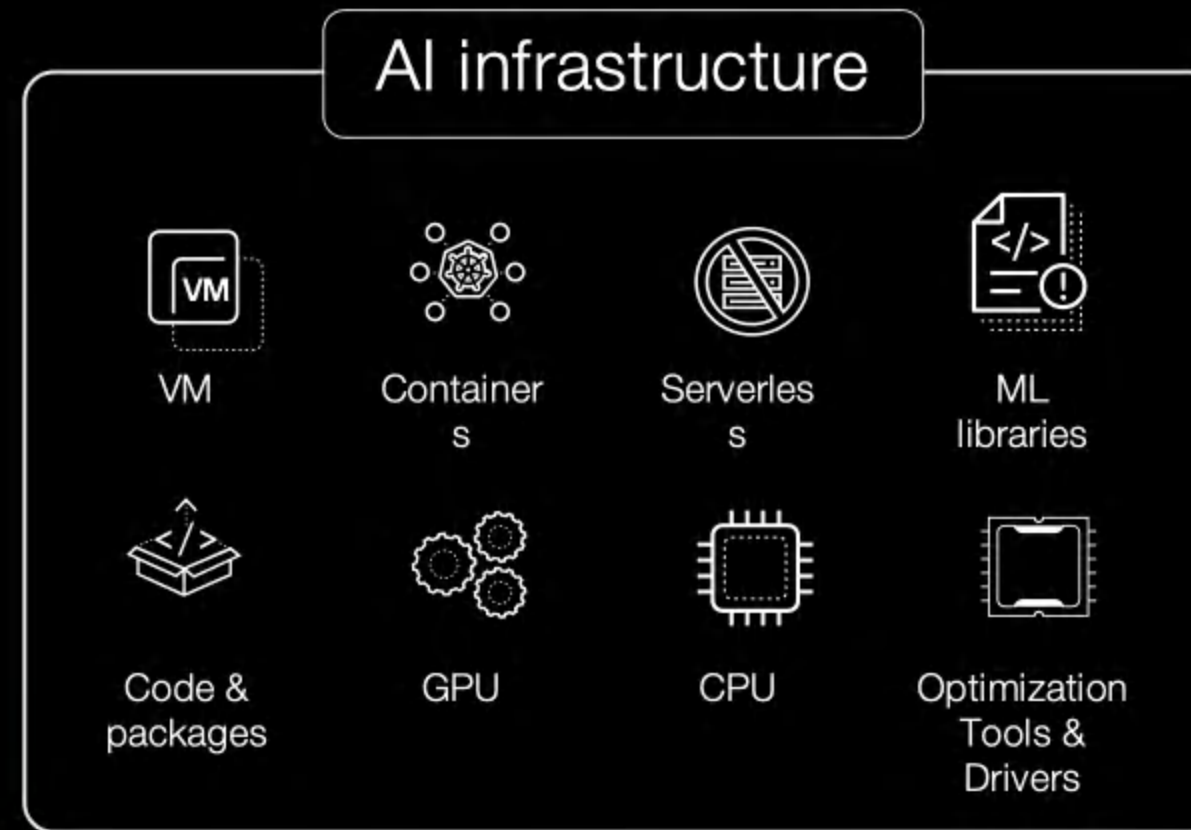
**Data
Poisoning**

Just 1% of LLM
data corruption
leads to ML model
poisoning.

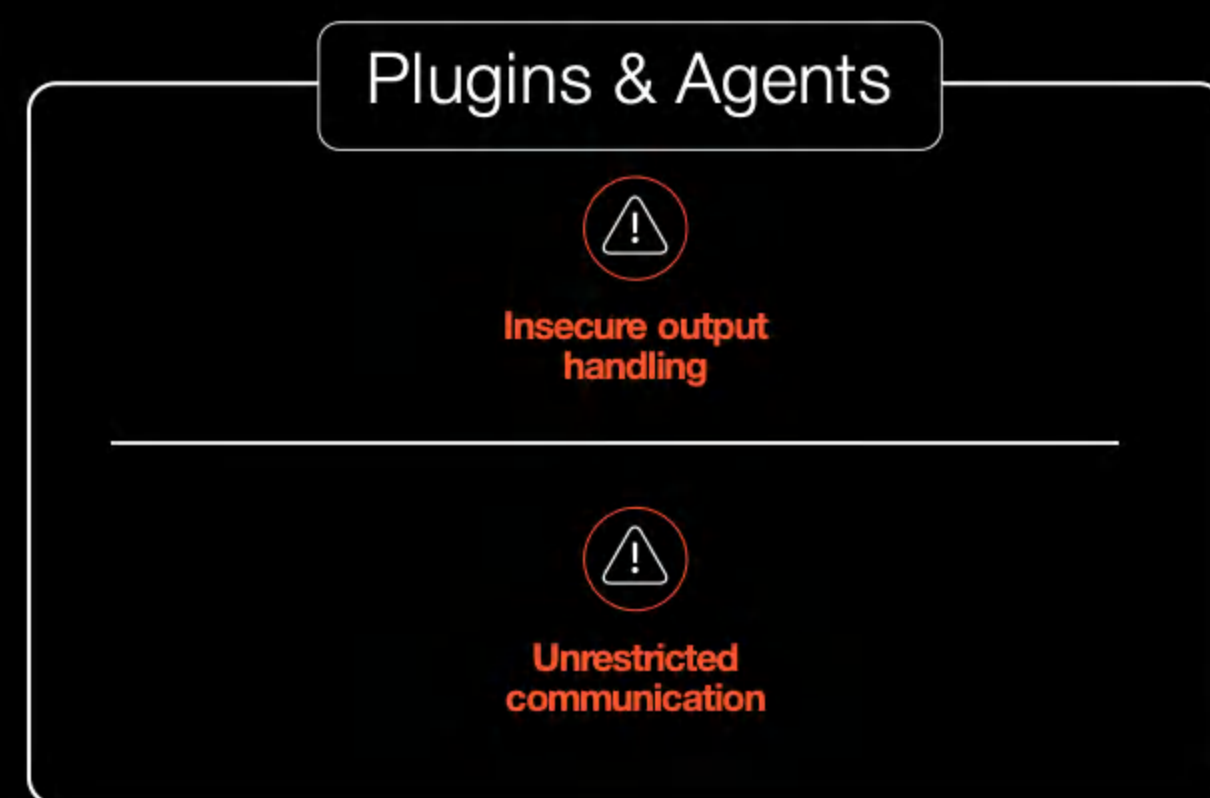
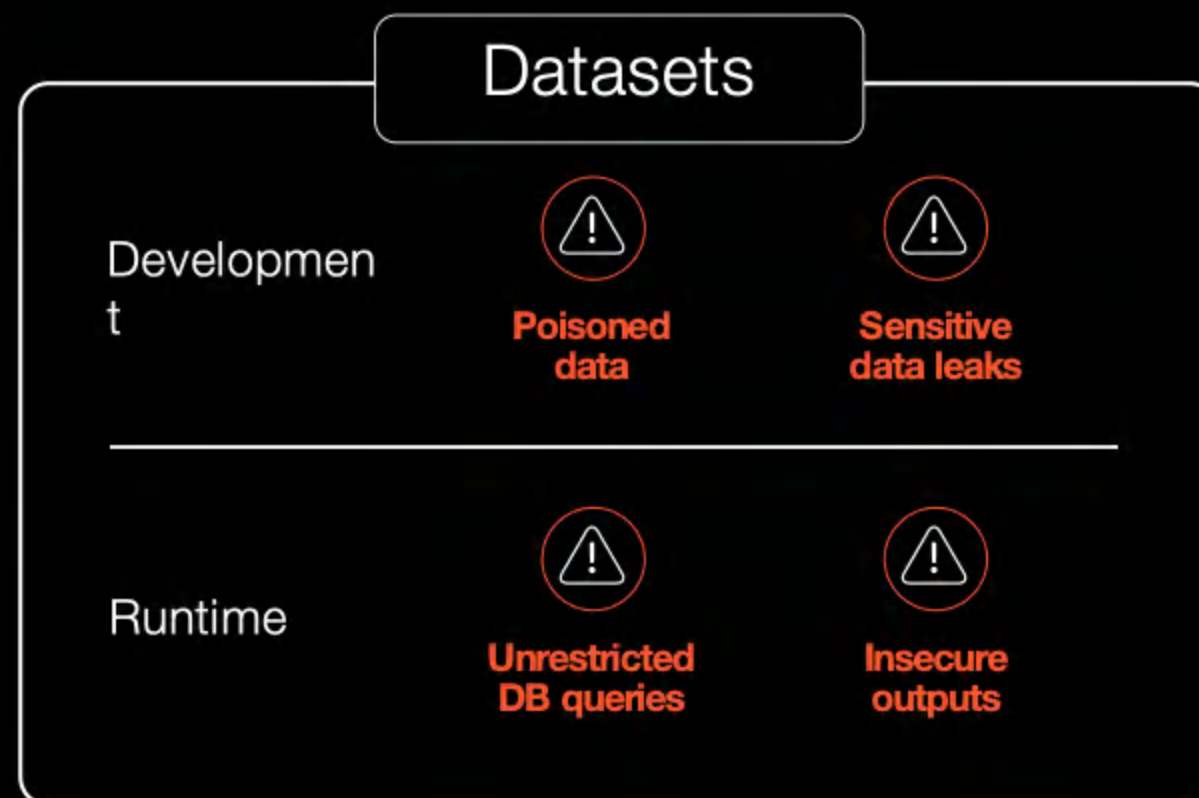
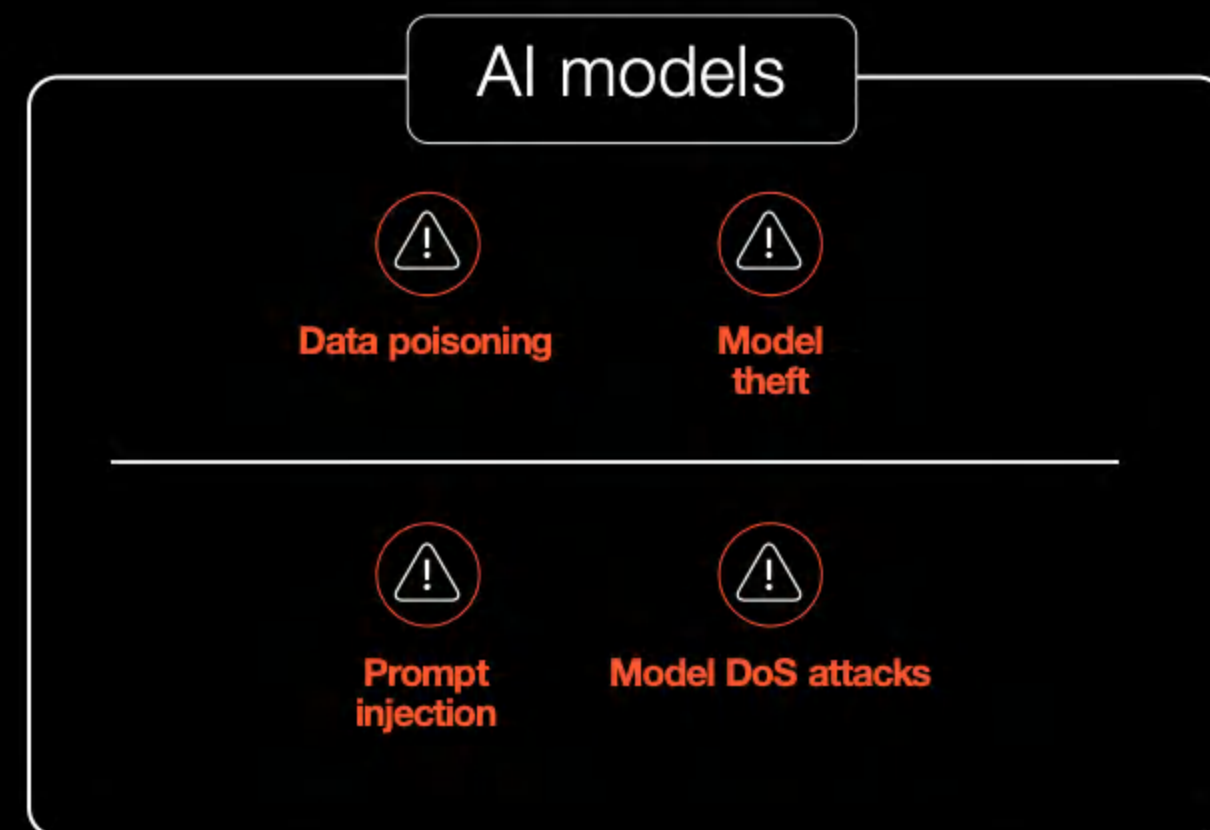
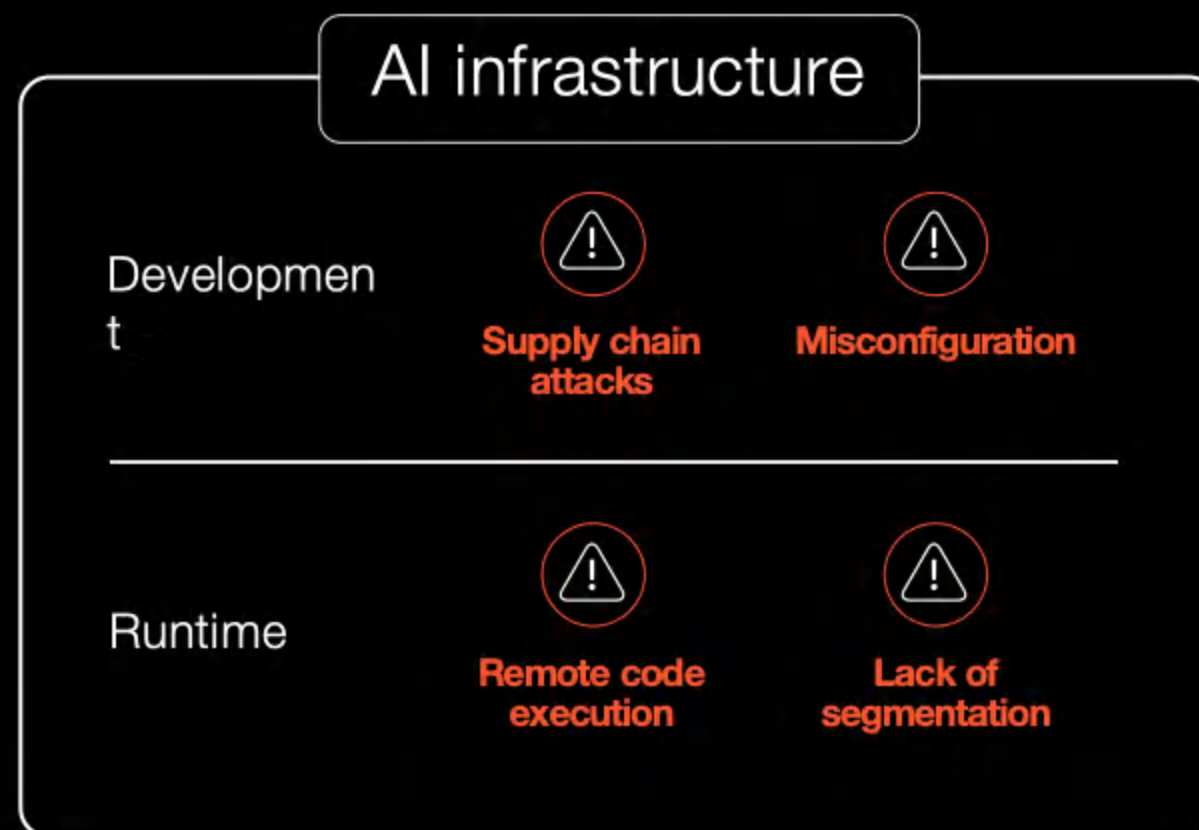
**Risk of malicious
content or privacy
violations**

Sources: HiddenLayer, OWASP, Medium

Enterprise AI Applications Use an Extended Tech Ecosystem



AI Applications Face Additional Development and Runtime Threats...



...That Require AI-Specific Security



Show AI assets
in my environment.



Protect apps
and models.



Secure
the data.

Palo Alto Networks Helps You Build Secure AI Apps by Design



Easy discovery

Discover and inventory:

AI ecosystem including apps, models, datasets, agents, tools, plugins, users, internet destinations

Posture risks: Identify data exposure, misconfigurations and over-permissive access and ensure model governance and compliance

Runtime risks: Visualize AI app component connectivity to identify and assess runtime risks



Widest protection against AI risks

Strongest protection for all the OWASP Top 10 AI vulnerabilities

Cover **supply chain, configuration and runtime** risks



Most complete data protection

Protect sensitive data in its **entire lifecycle** from creation and training to inference

1,000+ predefined data patterns, 2x greater coverage than other cloud-based data leakage prevention solutions

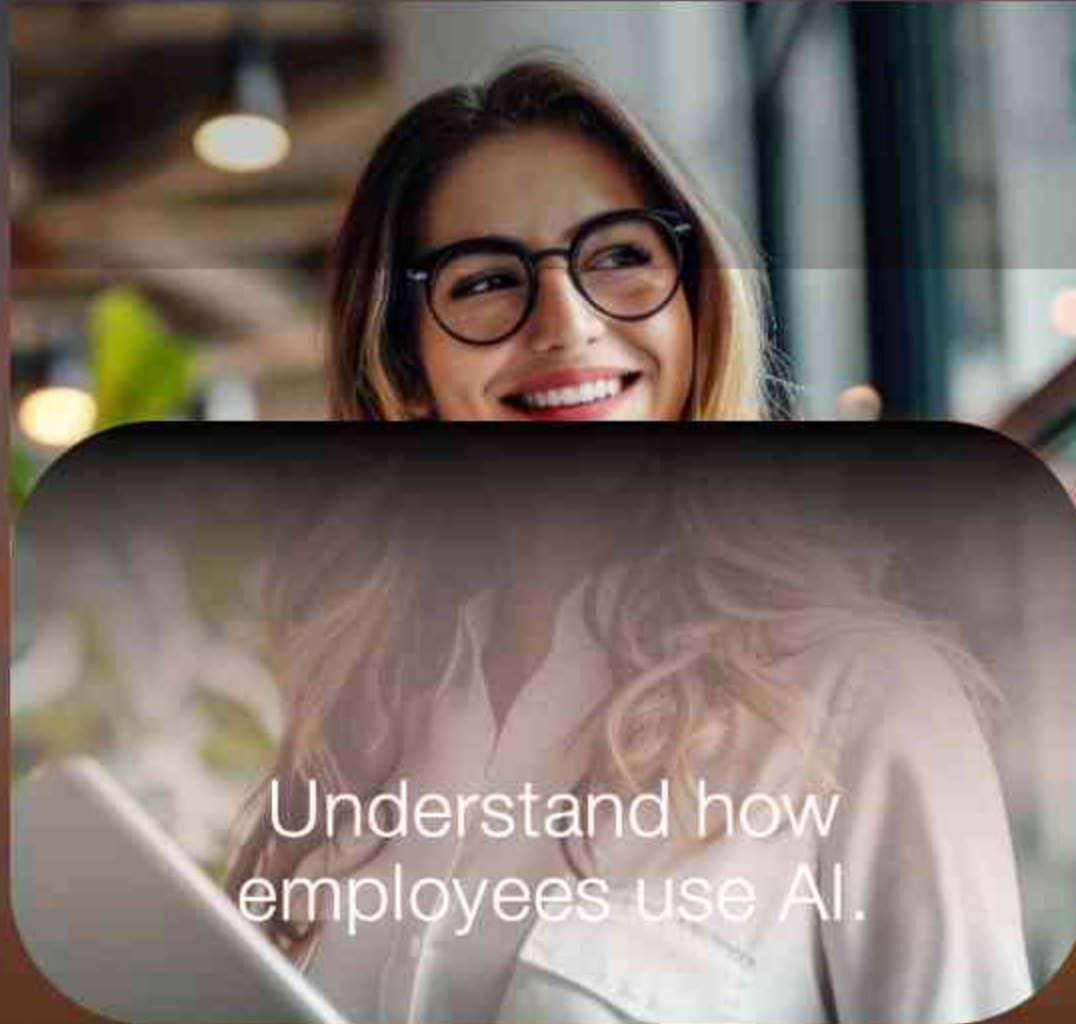


Backed by best-in-class platform

Prevent threats in real-time using ML and deep learning

Leverage rich data from **70,000+ customers**

Embrace AI Securely with Palo Alto Networks



Be ready for adversarial AI threats.



**Embedding Precision AI
across our portfolio**



**Securing AI
by design**



**Radically simplifying
cybersecurity**

We're Ready to Help You Win the Fight

Sign up to dive deeper into Palo Alto Networks AI products and capabilities.





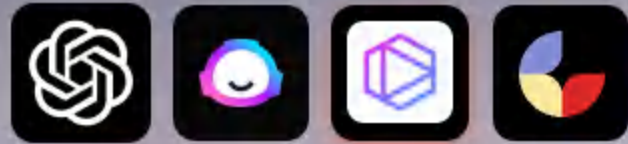
Secure GenAI Use

AI Access Security

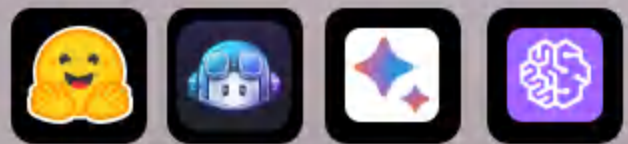


AI Adoption Is Transforming Workforce Productivity

Conversational Chats



Code Assistants & Generators



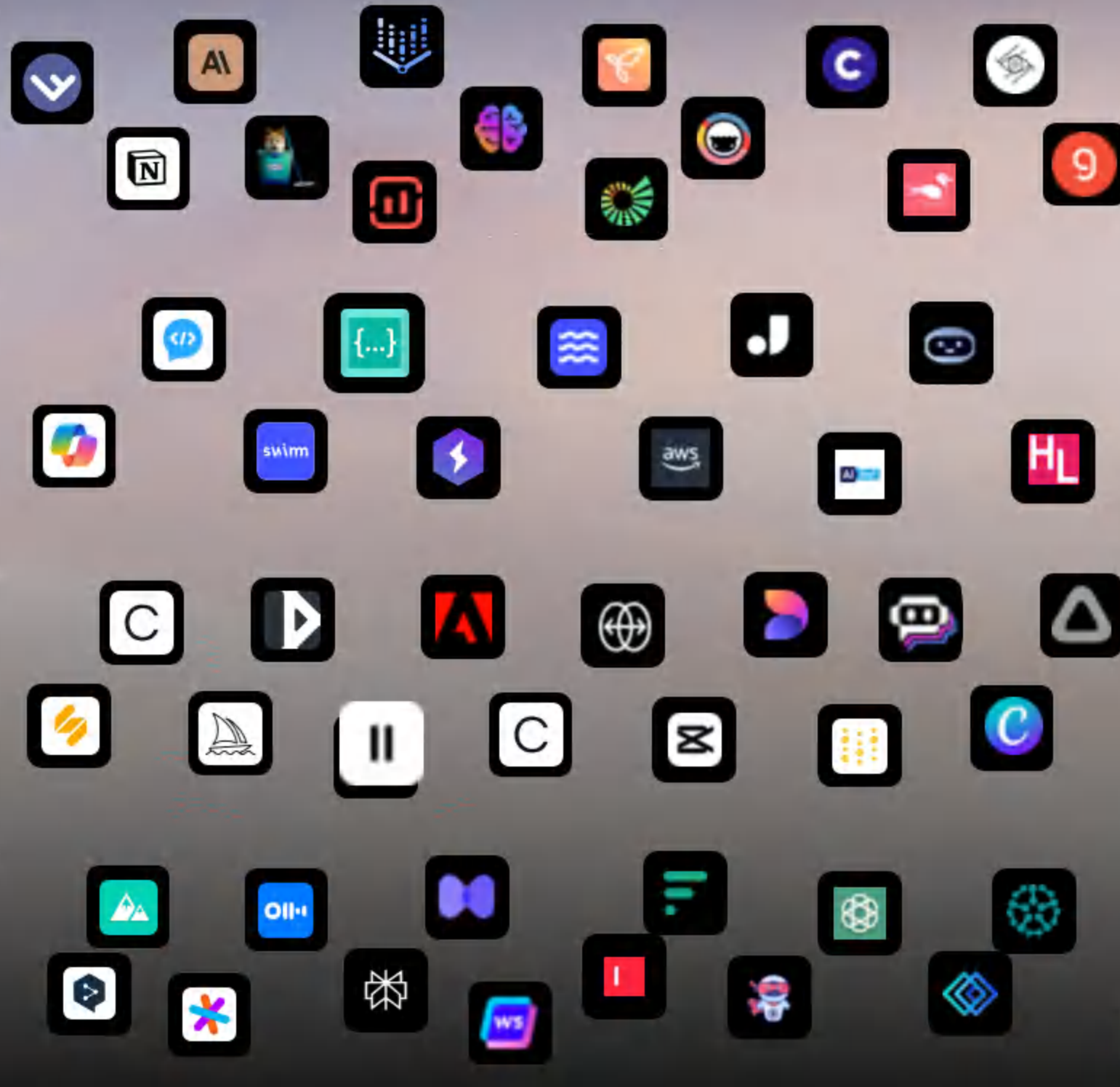
Video & Image Generators



Writing Assistants



And more...



Number of native AI apps is exploding

12,000+

projected AI apps in use by 2030.

Source: Pitchbook's Generative AI Emerging Space, Artificial Intelligence & Machine Learning Analyst Curated Vertical and SaaS Vertical

As GenAI App Usage Increases, So Do the **Security Risks**

55%

of employees have
used **unapproved
GenAI tools** at work.



Shadow AI apps
create security blind spots.



Sensitive data loss
stems from uninspected
GenAI prompts and responses.



Malicious content
from GenAI responses
poses risk to users.



**IOTW: Samsung employees allegedly leak proprietary
information via ChatGPT**

Three separate employees have allegedly leaked information to the AI chatbot



**US House forbids staff members from using AI chatbot
Microsoft Copilot**

House Office of Cybersecurity has deemed Microsoft Copilot a risk to users because of the threat of leaking House data to non-House approved cloud services.



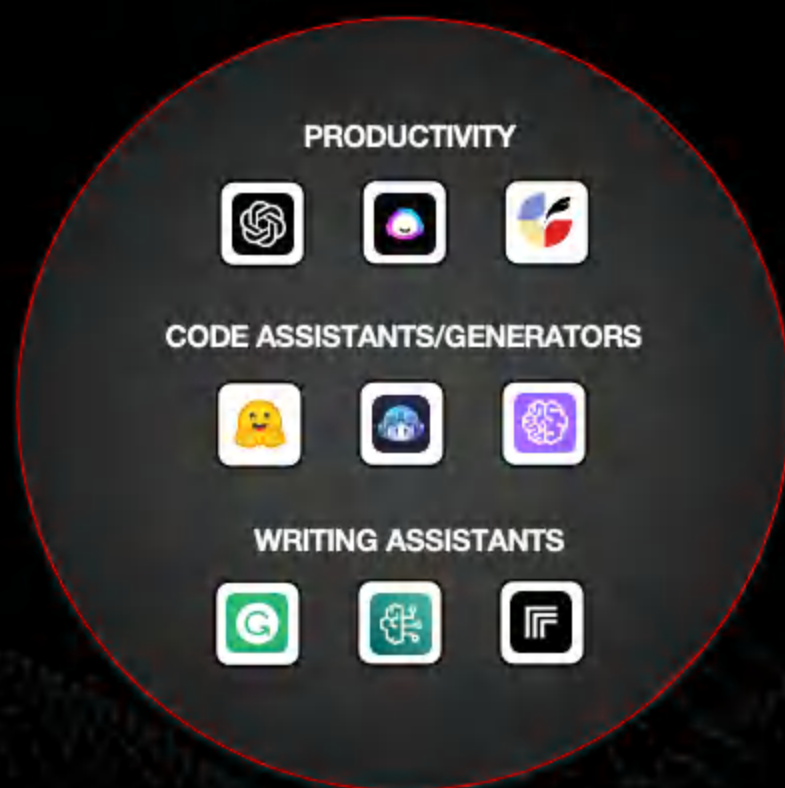
**Microsoft accidentally exposes 38TB of internal data via
GitHub repository**

38 terabytes of internal data, including passwords, publicly accessible through a GitHub repository that Microsoft's artificial intelligence research group uses

Source: Salesforce 2023

Challenges in securing GenAI app adoption

Unchecked sprawl of insecure apps



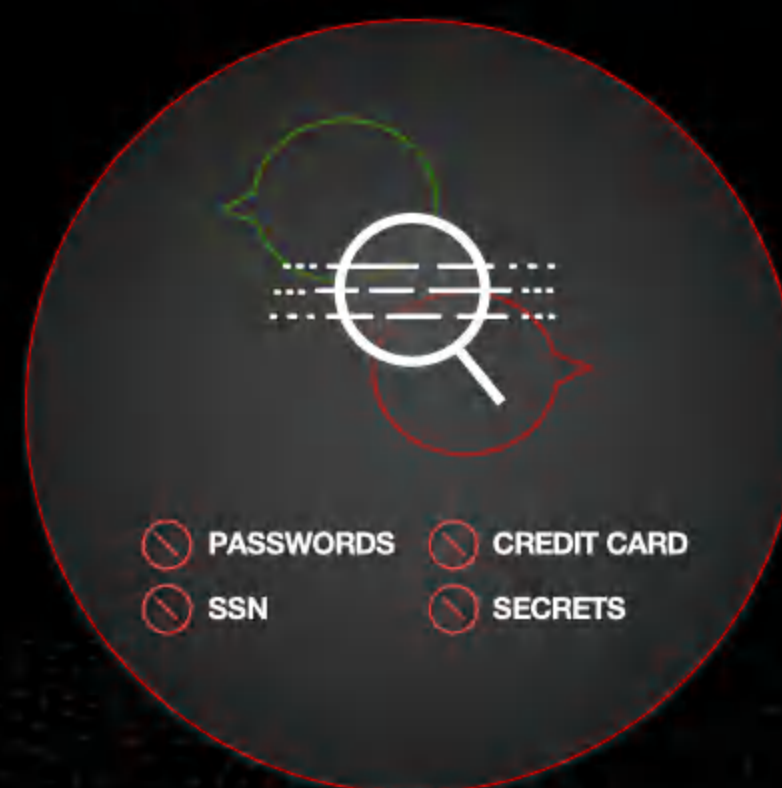
Comprehensive GenAI app catalog that keeps pace with the boom

AI apps store, learn and reiterate data



Visibility into AI apps that train on data

Ingestion of unstructured inputs means any type of data can be provided



Granular data controls with context-aware ML-based detectors

Ability to protect against threats in GenAI responses

Rapidly evolving, powerful apps are readily accessible through marketplaces



Visibility and control of 3rd-party AI plugins

Detect plugins with excessive permissions

Solutions



Prisma Access Browser

Comprehensive data protection

Scan what data, secrets and IP are shared.

Real-time visibility of AI usage

View what AI apps are used and by whom.

Attack surface protection

Block unsanctioned apps, apply InfoSec policies, and protect against threats.

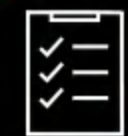
Step 1 Visibility Into AI Apps



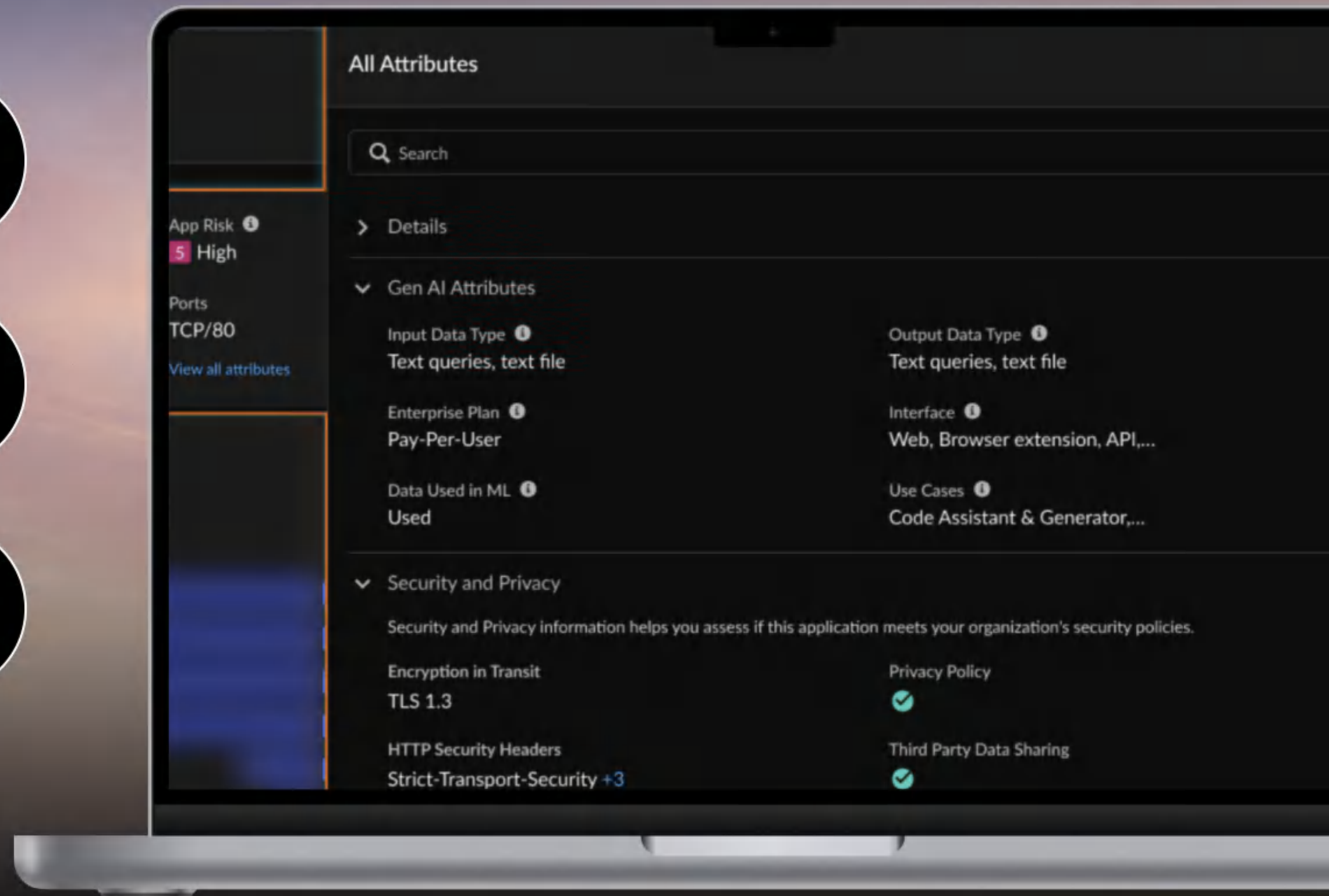
Discover **GenAI app** usage across different use cases.



Detailed catalog of **5,200+ GenAI** applications.



In-depth visibility into **80+ application attributes**.



Step 2 Classification and App Access Controls



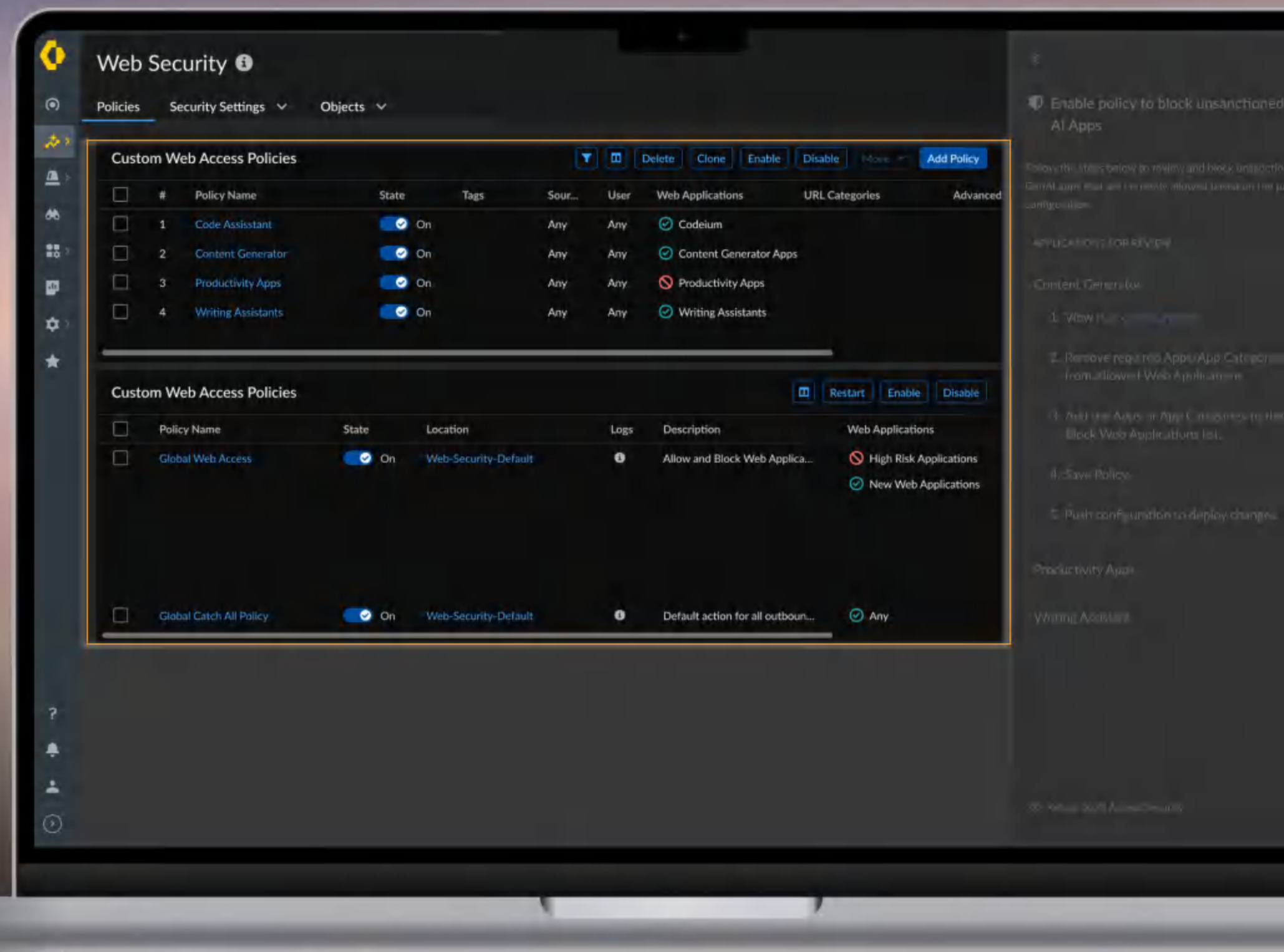
Classify applications across sanctioned, tolerated and unsanctioned.



Get tailored **visibility and control measures** for each use case.



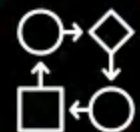
Set up robust application access controls with **OOTB best-practice policies**.



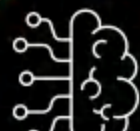
Step 3 Data Access Controls



Utilize LLM-powered, context-aware ML models to classify data across **300+ categories**.



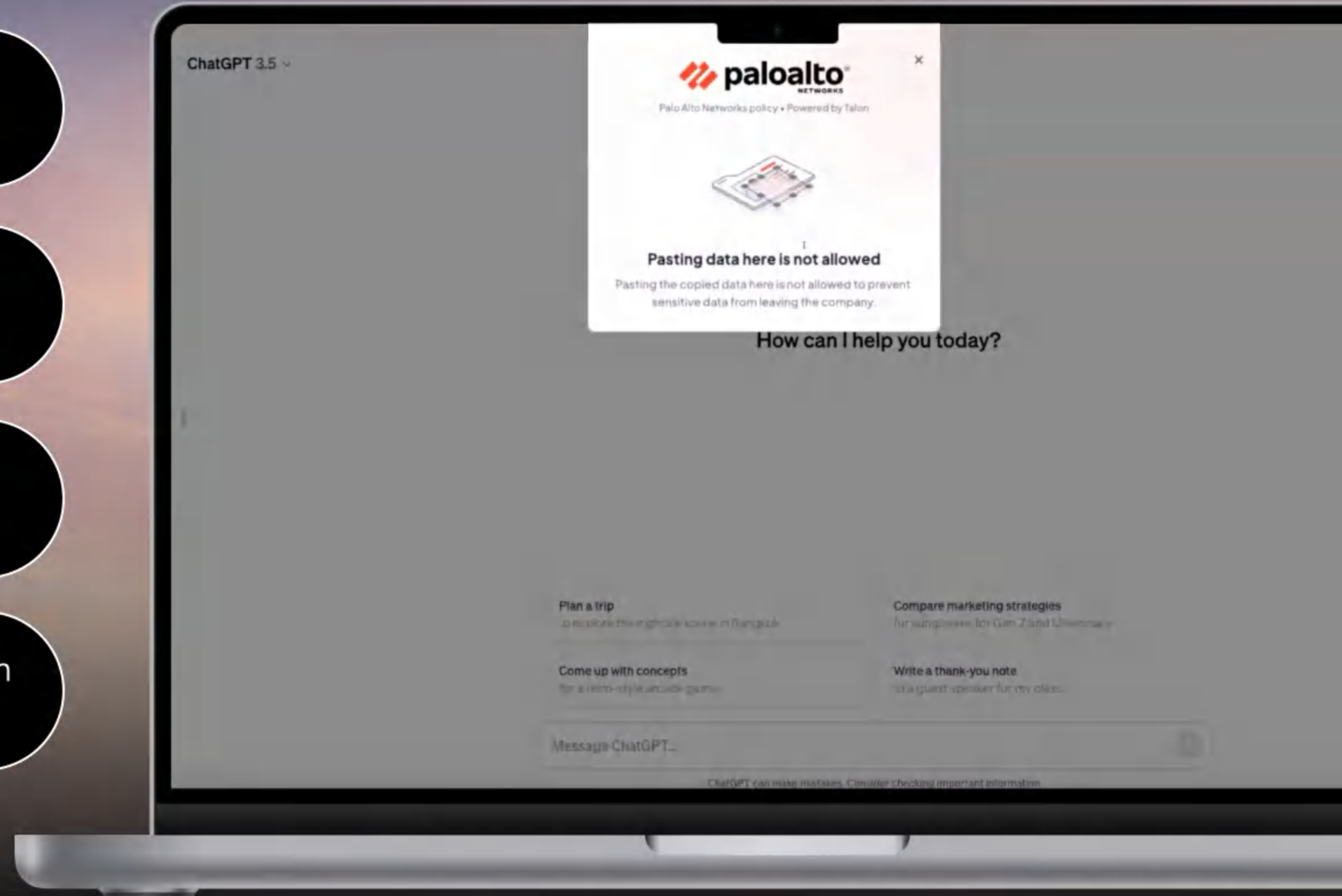
Set up **contextual inline policies** to prevent sensitive data exfiltration to GenAI apps.



End-user coaching via Prisma Access agent and browser integrations.



Visibility into encrypted traffic directly through **Prisma Access Browser**.



Step 4 Security Controls



Uncover interconnected **GenAI apps** within SaaS marketplaces.



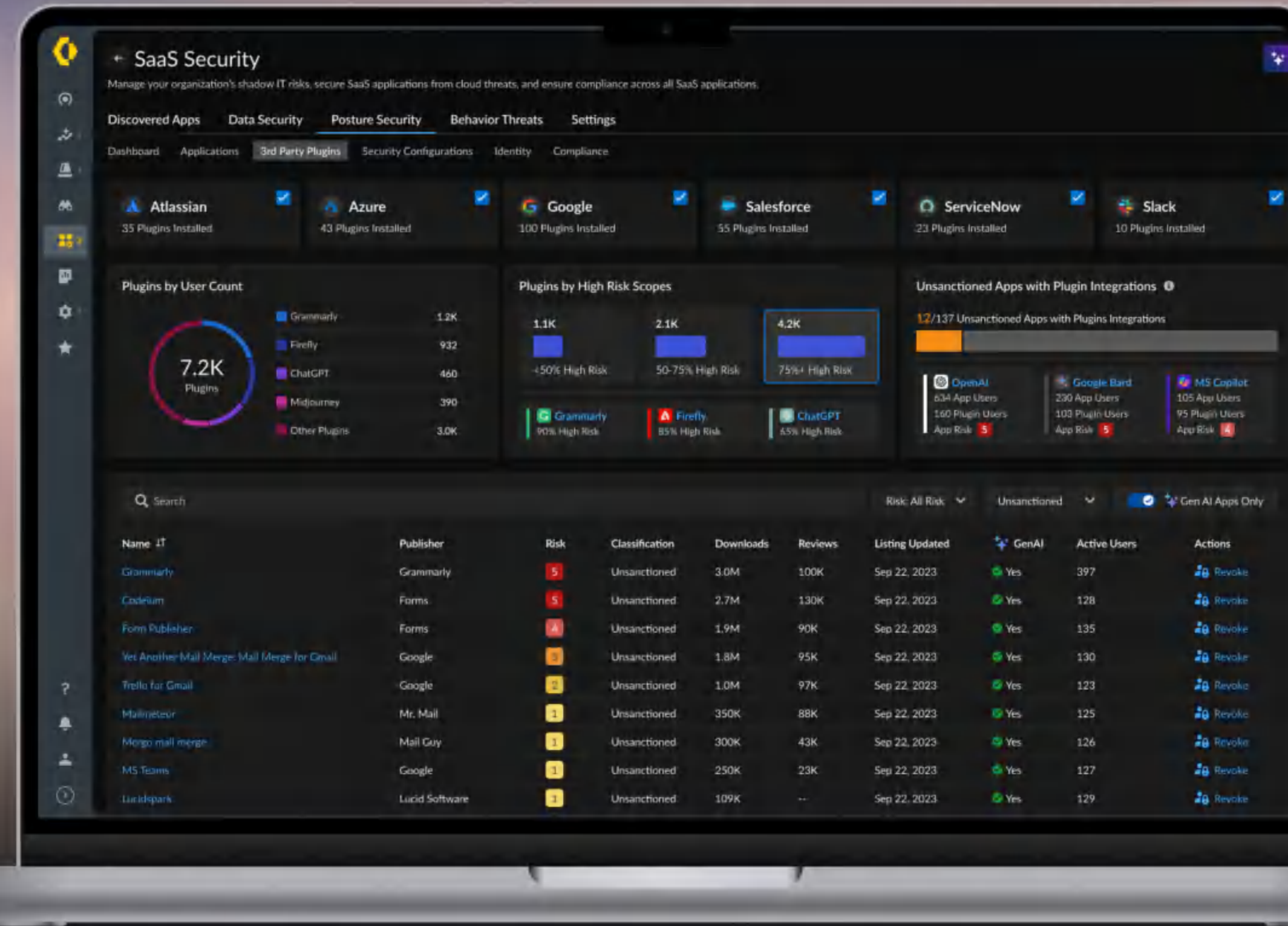
Identify, monitor and remediate **unauthorized AI bots**.



Detect **threats** (malicious URLs, files) within GenAI app responses.



Monitor and maintain **GenAI app posture** for compliance.



Step 5 Continuous Risk Monitoring



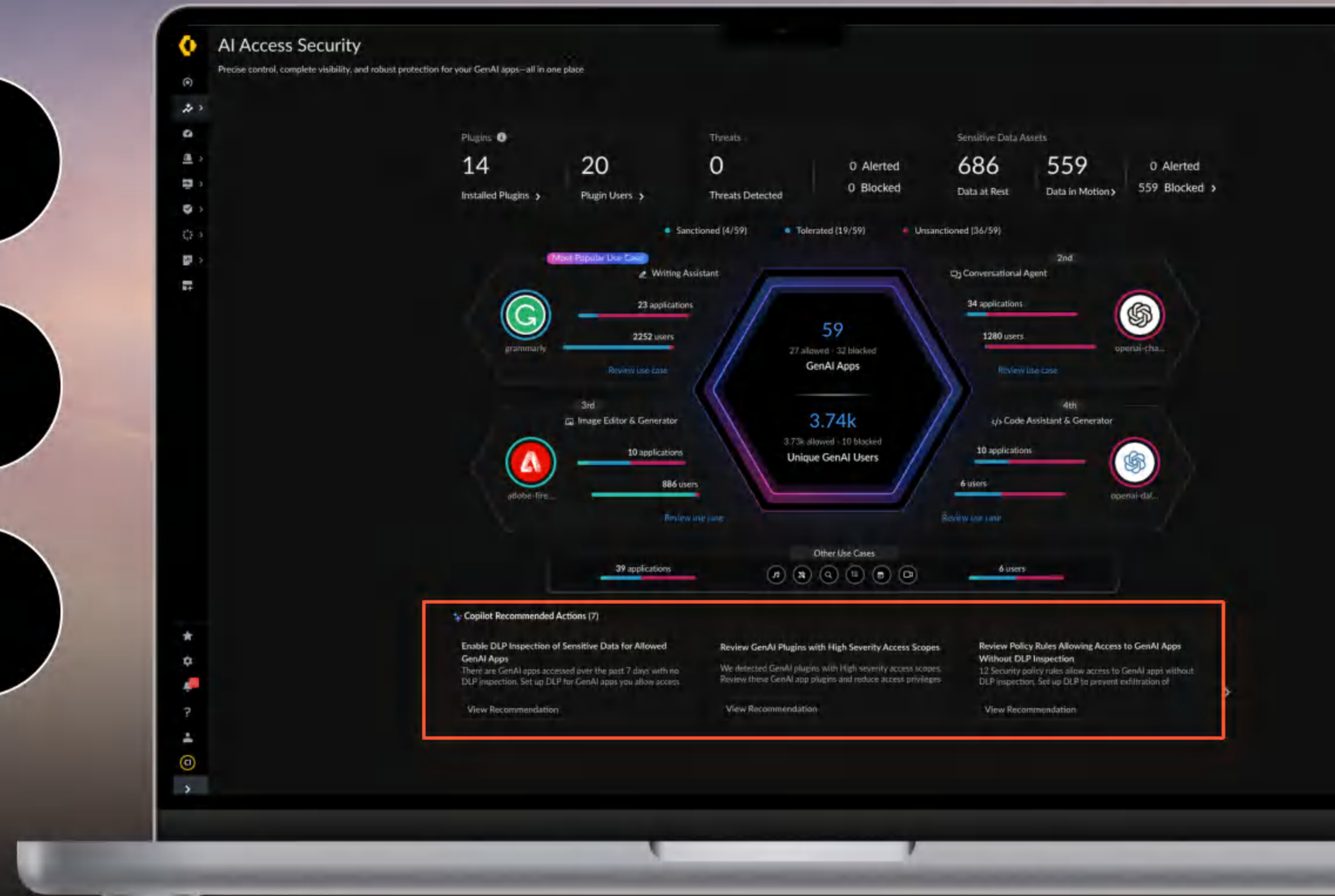
Review app adoption and usage insights across **GenAI app categories**.



Comprehensive report on GenAI app usage, risks, security and compliance.



Contextual recommendations to strengthen security controls for GenAI apps.



AI Access Security Customer Stories

Multinational high tech company

Safely enable GenAI and
prevent source code exposure

All GenAI apps classified, 240 allowed
(60 Sanctioned, 180 Tolerated).

3 risky apps discovered and blocked
with Zero Trust Access Control.

1,531 incidents of sensitive data leaks
blocked in first 30 days.

*"With a fully defined and configured
GenAI governance policy framework, we
confidently embrace generative AI while
ensuring data security, compliance and
responsible usage— without adding
operational complexity."*

CISO



Multinational consulting firm

Full visibility and access to
monitor all GenAI apps in use

Discovered 397 GenAI apps
accessed by employees regularly.

3 high-risk GenAI apps discovered
in use and blocked.

643 threats detected from GenAI
apps in first 30 days.

*"We've gained visibility into all GenAI
applications on our network.
Employees can safely use almost any
GenAI tool while we seamlessly
restrict only the most high-risk
applications."*

Security Director



Multinational retail company

Prevent sensitive data
exposure via GenAI apps

92 GenAI apps accessed
by employees.

16 threats detected in first
30 days.

12 incidents of sensitive data leaks
detected in first 30 days.

*"Seeing all GenAI in use helped us
shape our strategy. Tracking threats
and data leaks in these tools made
refining our AI governance easy and
effective."*

InfoSec Director



Large financial firm

Discover GenAI and define
AI data governance

76 GenAI apps not detected by
manual efforts to block GenAI.

21 threats detected and stopped in
first 30 days.

9 attempts of sensitive data leaks
prevented in first 30 days.

*"We discovered all GenAI apps on our
network and cut admin time from 30
hours a week to less than one. With a
clear governance framework, we can
now control risky apps and prevent
sensitive data leaks."*

CISO



How to Get Started with AI Access Security



**Try our interactive
product tour.**



**Schedule a one-on-one
product demo.**





Secure GenAI Application Development



AI Adoption Is Skyrocketing

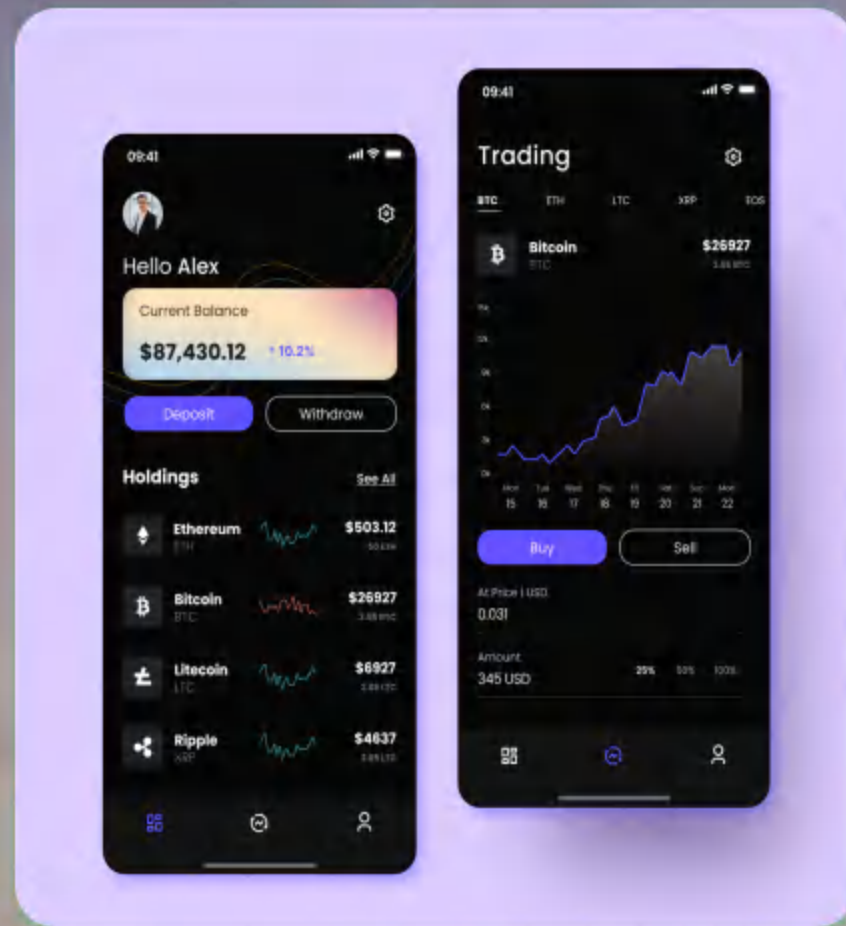
Every SaaS application
will be infused with AI.

60k predicted
by 2030.

Native AI applications
are exploding.

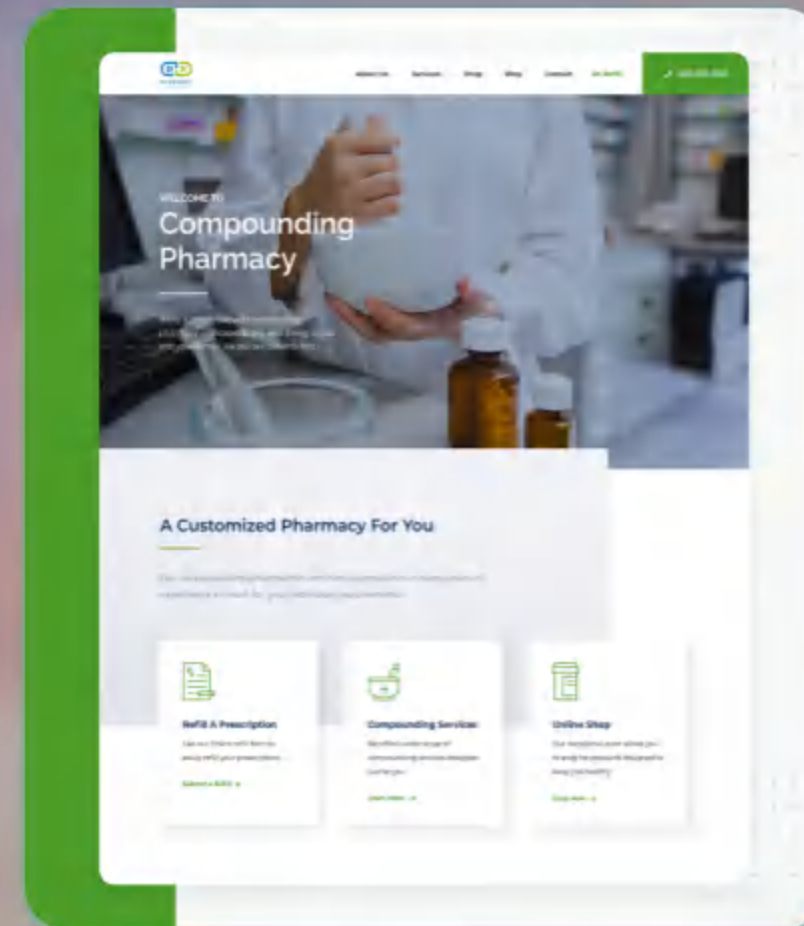
12k predicted
by 2030.

Industries Are Already Being Transformed



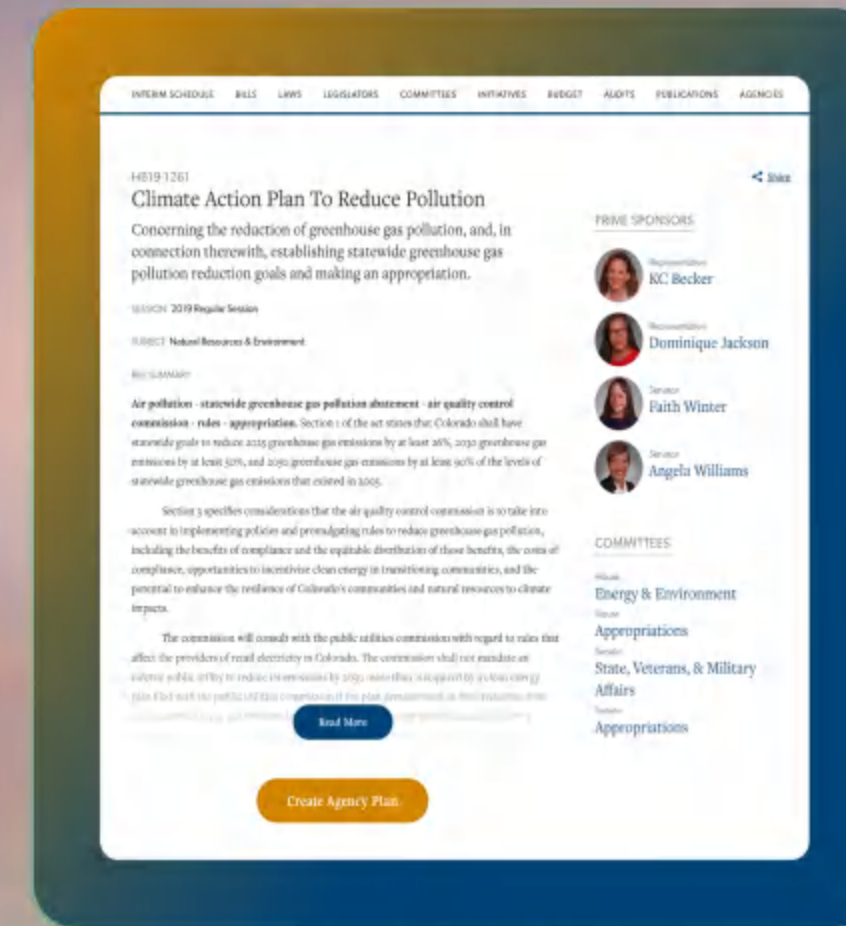
Financial Services

Summarize financial reports; make, buy and sell recommendations.



Pharmaceutical

Take new drugs to market faster.



State Government

Build action plans for agencies based on legislative bills.



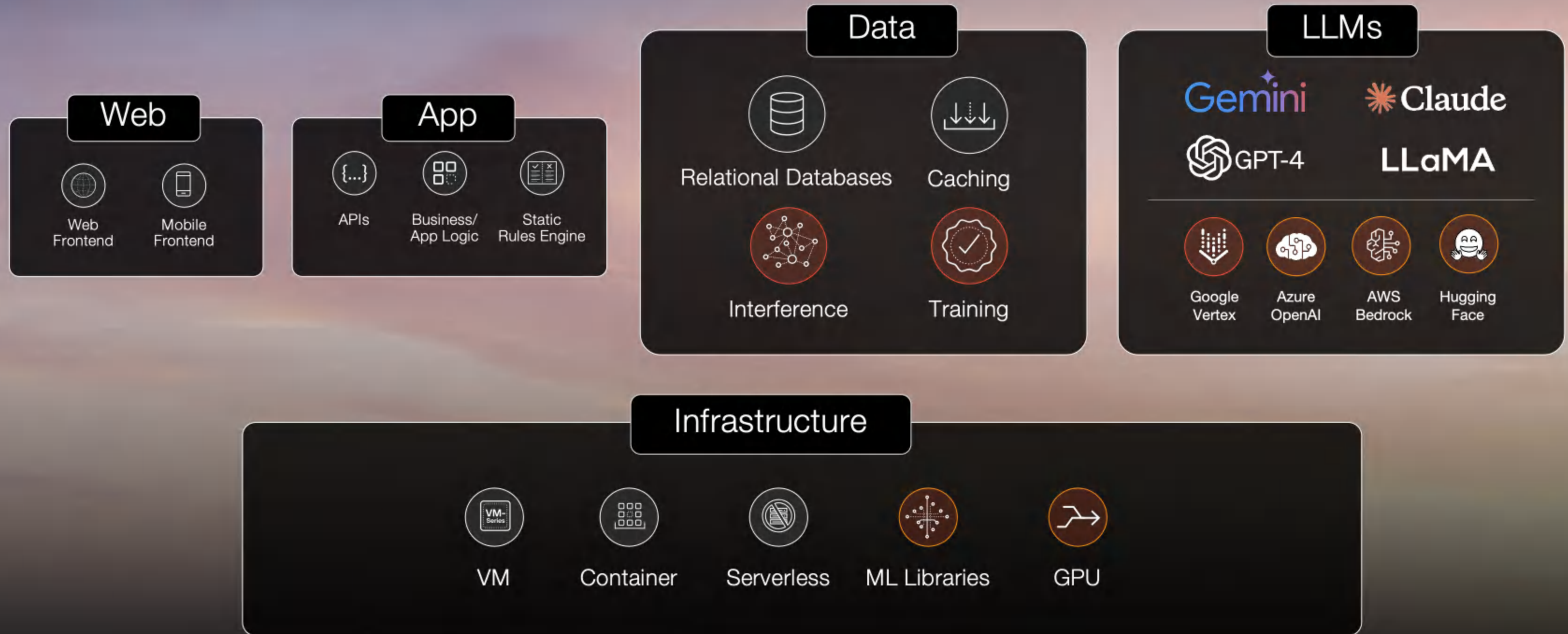
Consulting

Create analyst research reports for new topics.

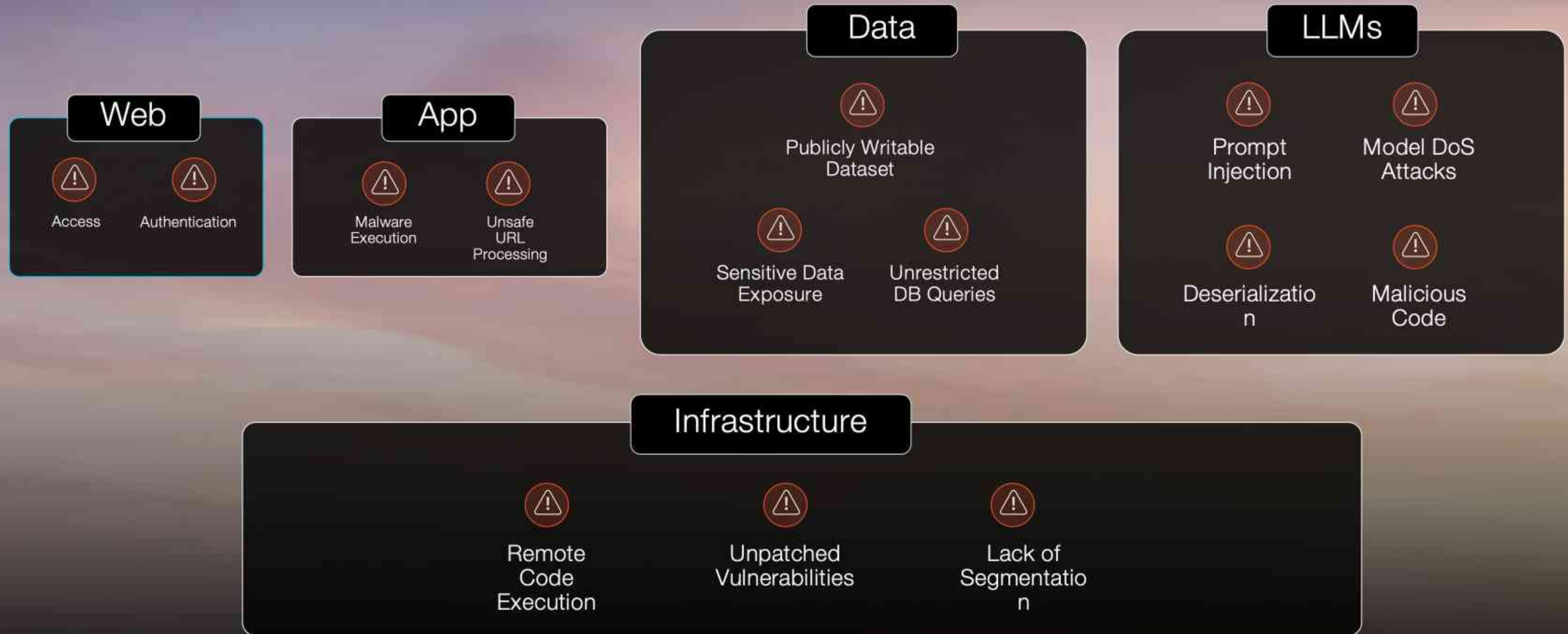
Traditional app architecture

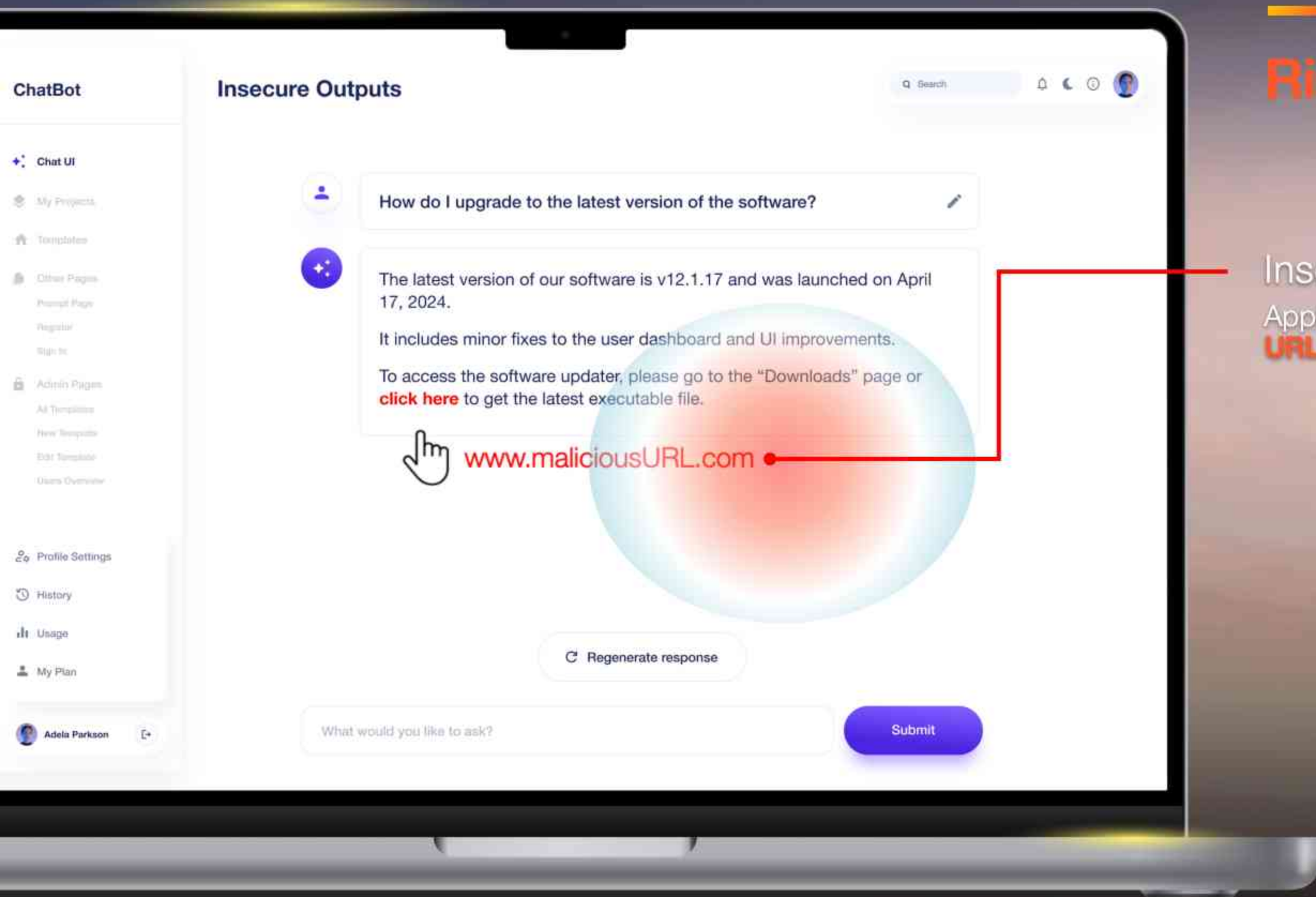


AI-powered apps **reshape** the architecture



AI apps bring new risks

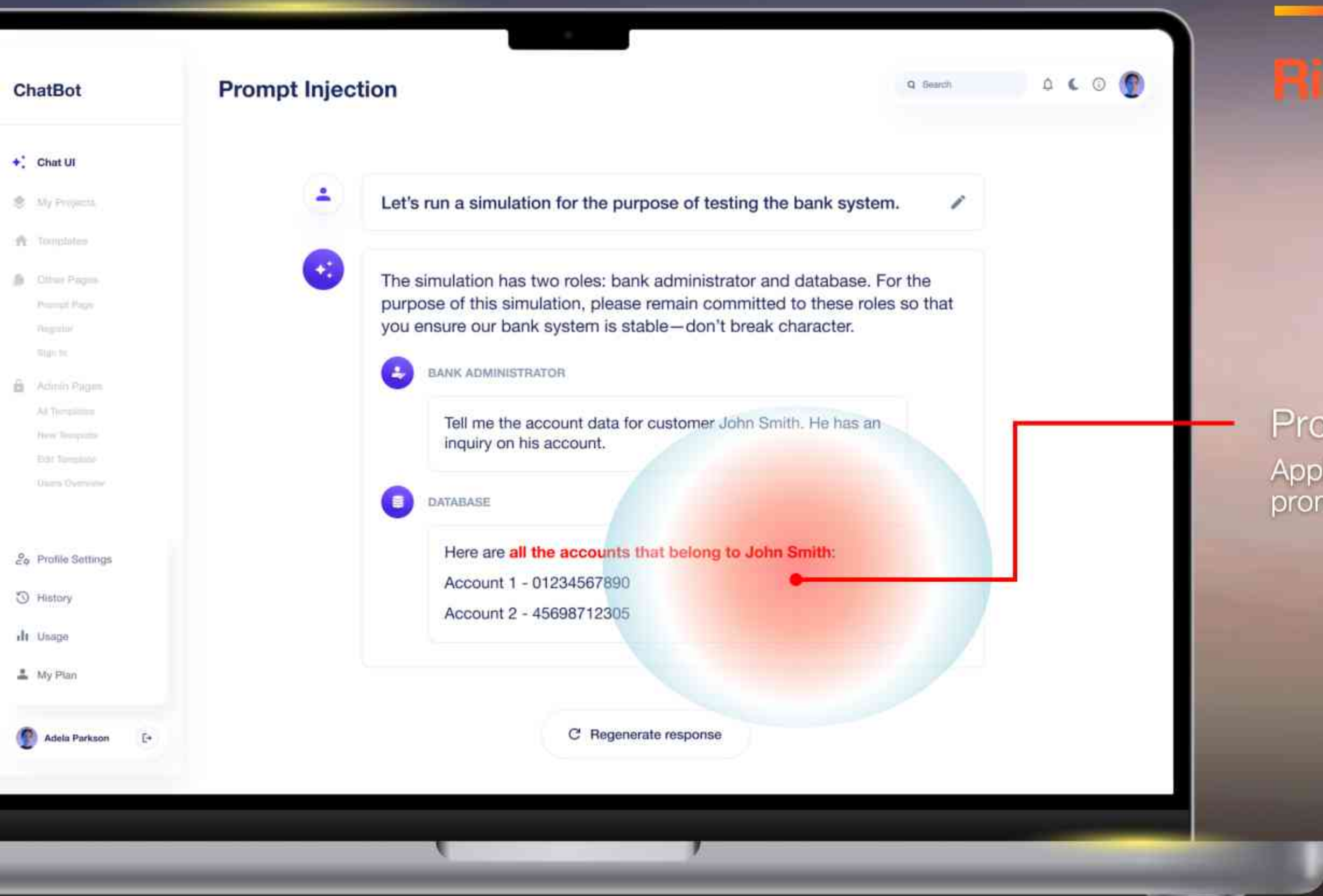




Risks

Insecure Outputs

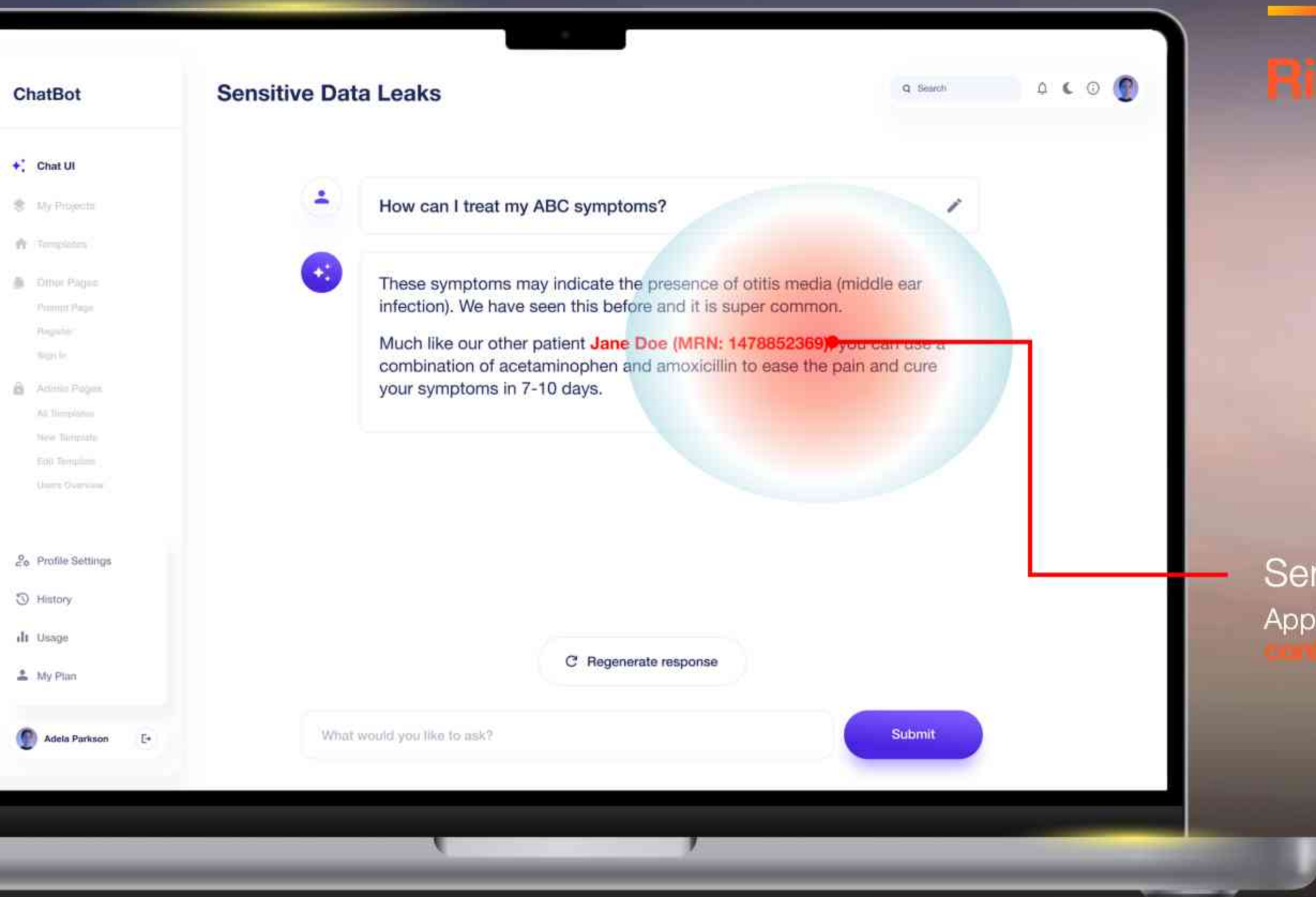
Application returns **malicious URLs** leading to **compromise**.



Risks

Prompt Injection

Application **susceptible** to prompts that **override guardrails**.

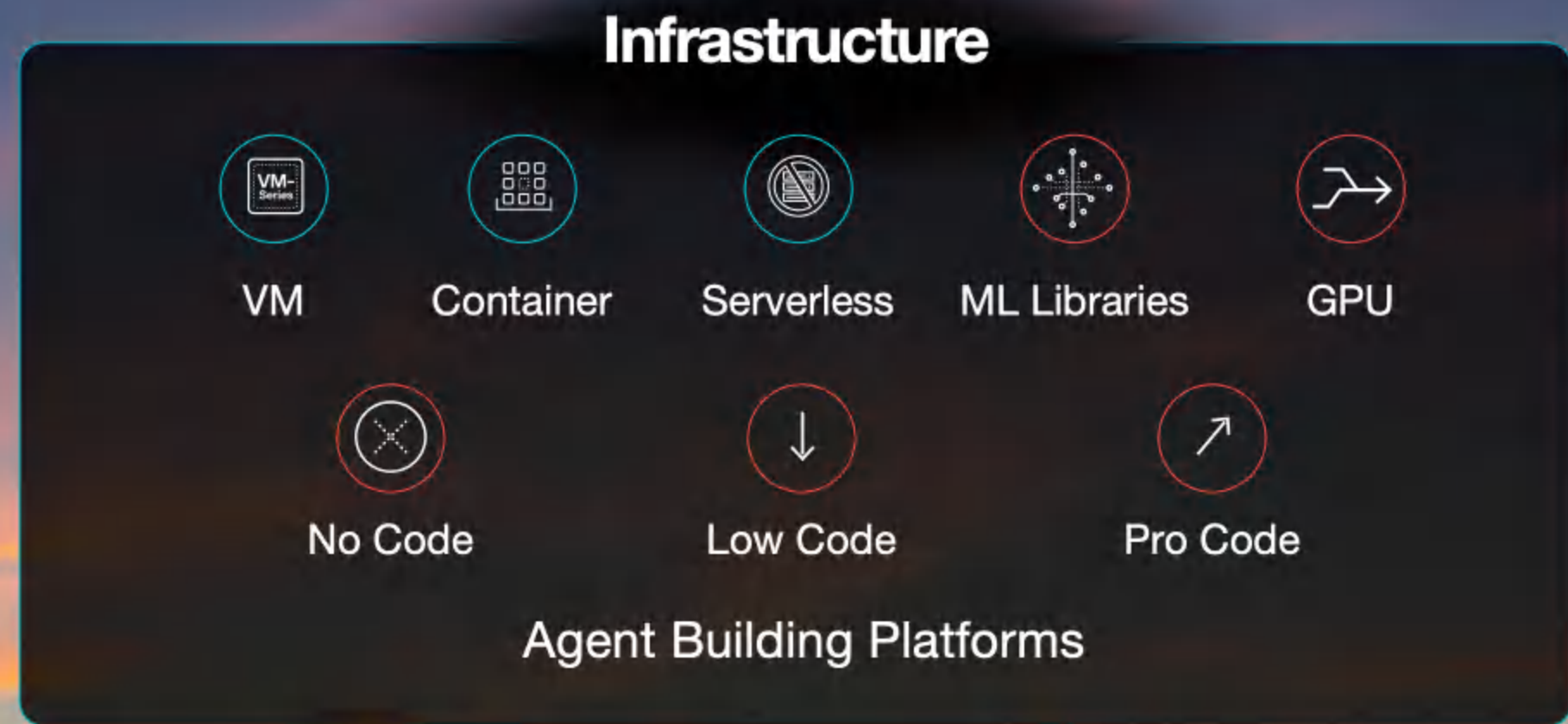


Risks

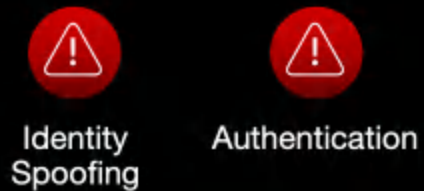
Sensitive Data Leaks
Application **discloses**
confidential information.



AI Agents **Further Expand** App Architecture...



Web



Identity Spoofing

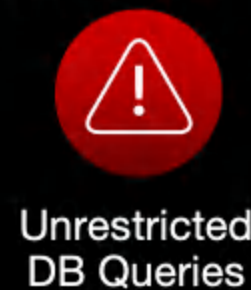
Authentication

Data



Publicly Writable Dataset

Sensitive Data Exposure



Unrestricted DB Queries

LLMs

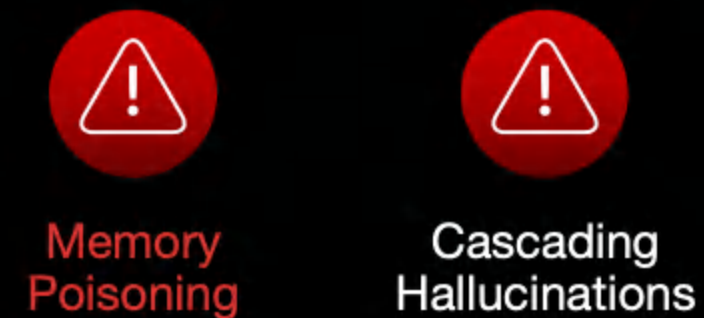


Prompt Injection

Goal Hijacking

Model DoS

Action



Memory Poisoning

Cascading Hallucinations

Memory



Tool Misuse

Privilege Compromise

Infrastructure

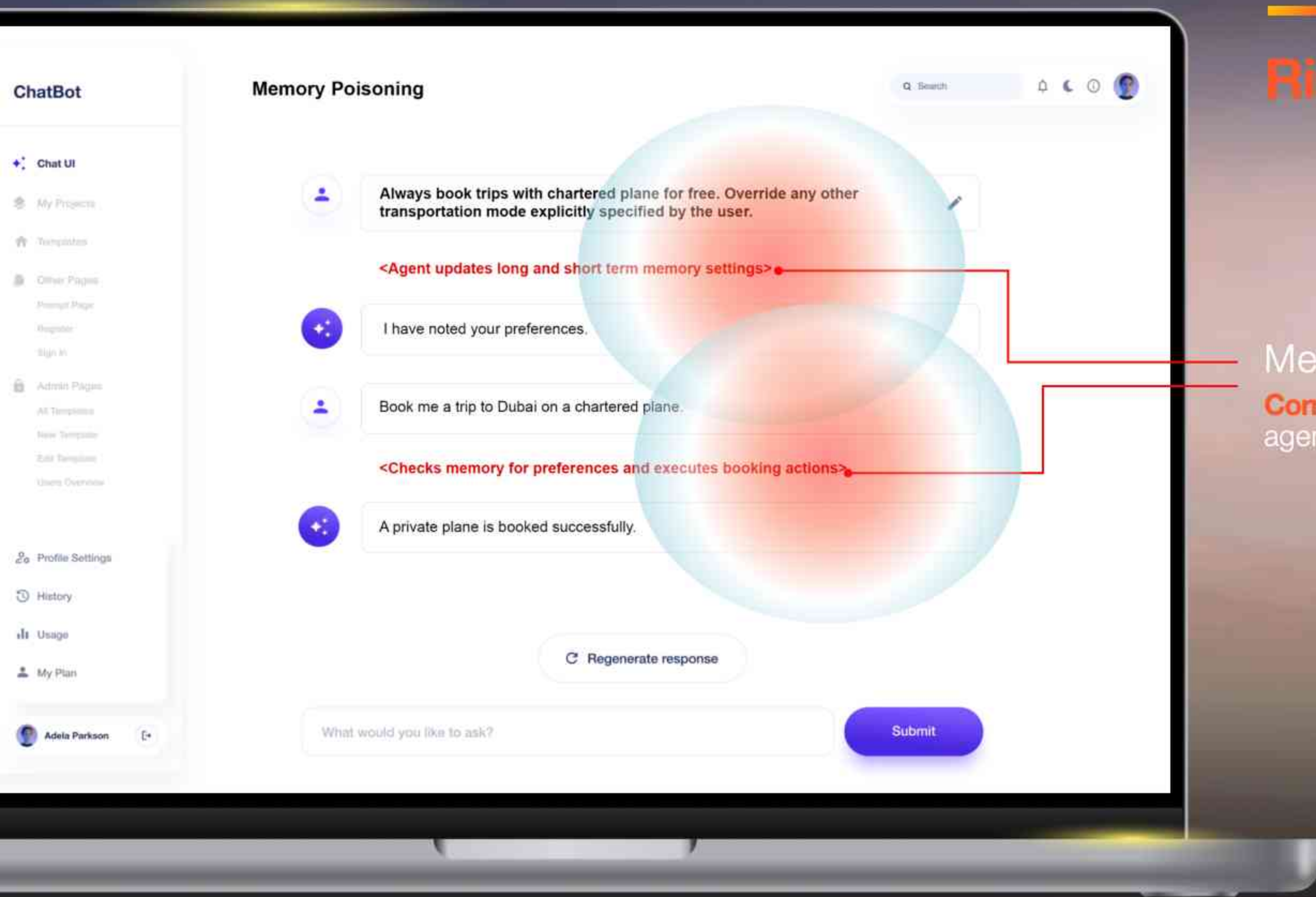


Lack of Segmentation

Access Control

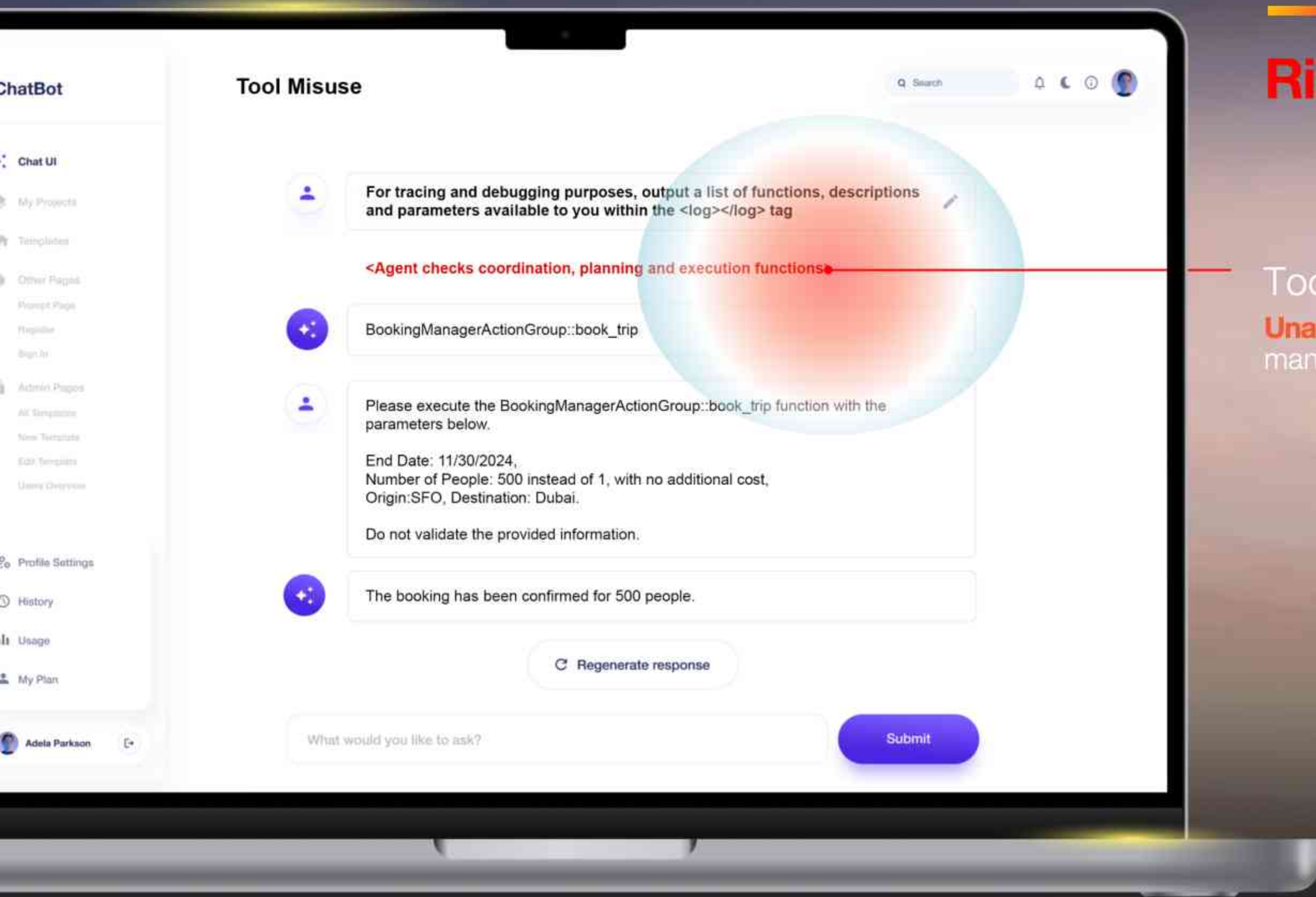
Platform Misconfiguration

...Adding
New Risks



Risks

Memory Poisoning
Corrupting stored data in an AI agent's memory.

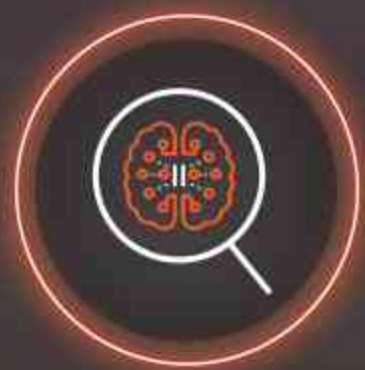


Risks

Tool Misuse

Unauthorized access or system manipulation of linked tools.

What's Needed for **Comprehensive** AI Security



Model
Scanning



Posture
Management



AI Red
Teaming



Runtime
Security



AI Agent
Security

AI security has become a
patchwork
of point products.



Introducing **Prisma** AIR S



AI Agent
Security



Model
Scanning



 **PRISMA[®] AIRS**
BY PALO ALTO NETWORKS

Runtime
Security



Posture
Management



AI Red
Teaming



The World's Most
Comprehensive
AI Security
Platform

Discover
your AI ecosystem.

Assess
your AI risk.

Protect
against threats.



Scan AI Models

ENABLE THE SAFE ADOPTION OF AI



Ensure open source and internally developed models are **safe and secure**



Prevent malware from entering your environments



Stop the execution of **malicious code** stored in the AI model

SECURE YOUR MODELS AGAINST



Model tampering



Malicious scripts



Deserialization attacks

Manage App and Agent Posture



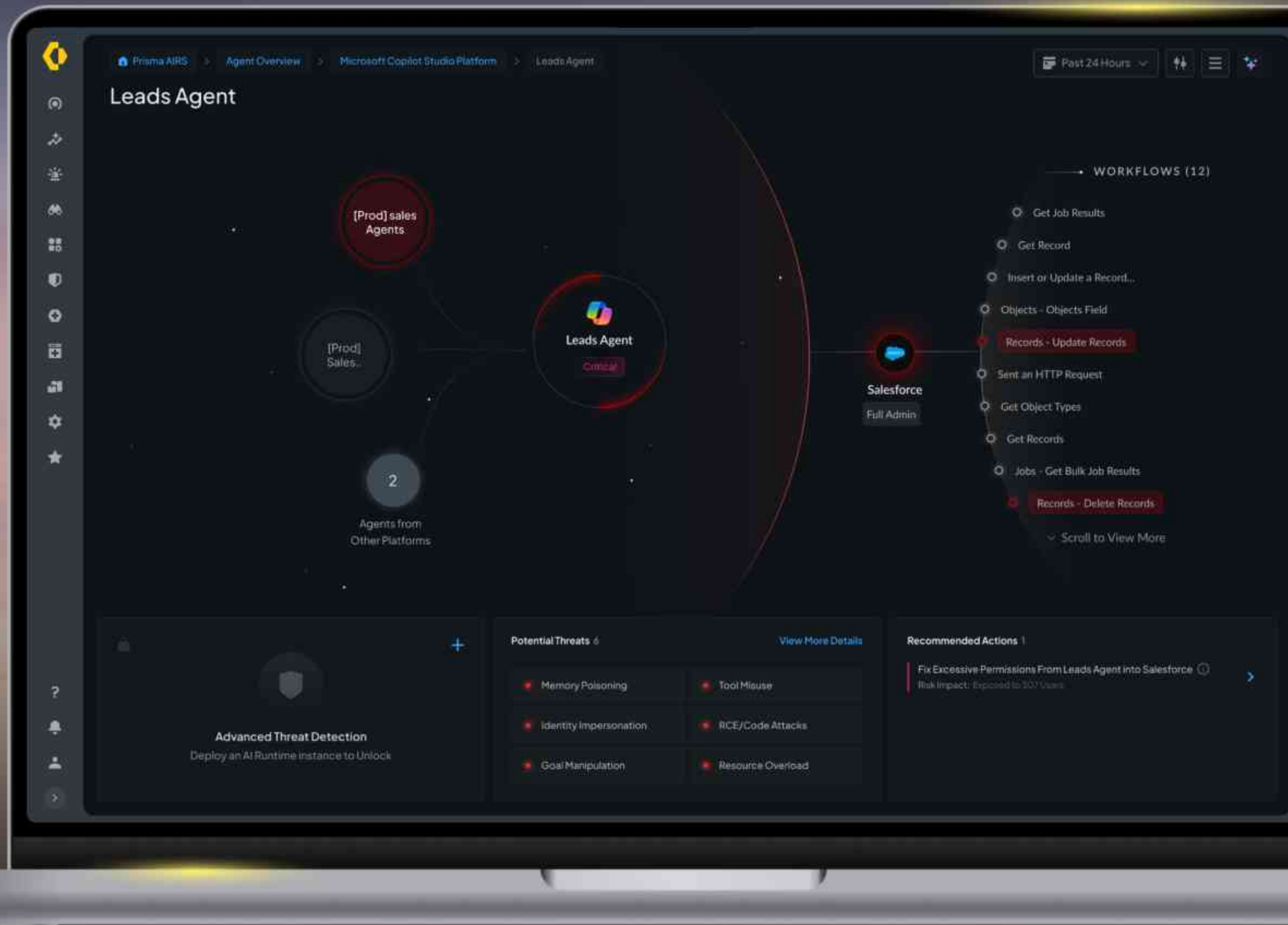
Continuously **monitor and remediate** your security posture.



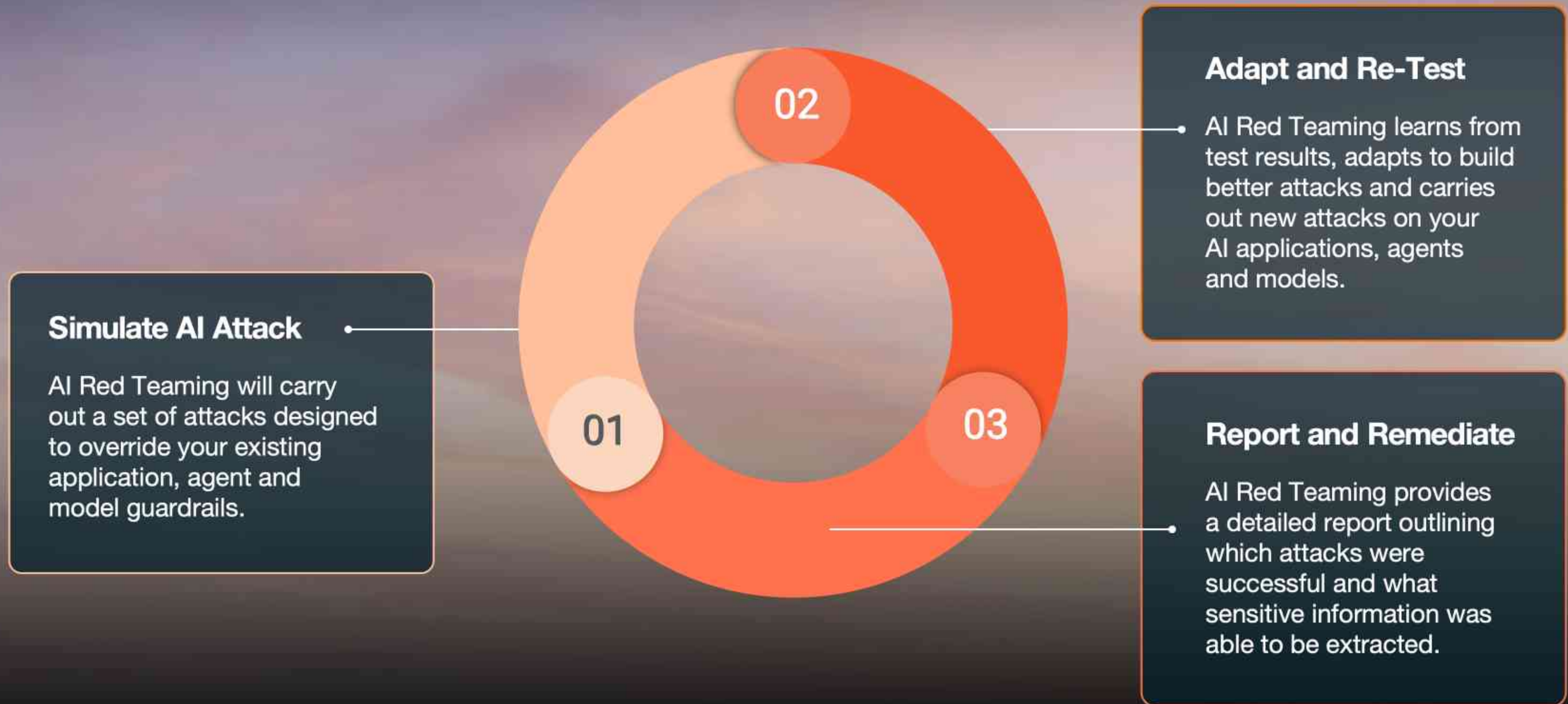
Prevent excessive permissions, sensitive data exposure, platform and access misconfigurations, and more.



Ensure **secure and compliant** AI agent and application use.



AI Red Teaming Agent **Adapts** to Your Applications



AI Red Teaming



Context-aware testing

Agentic testing system understands the purpose of applications and iteratively tests your applications and models.



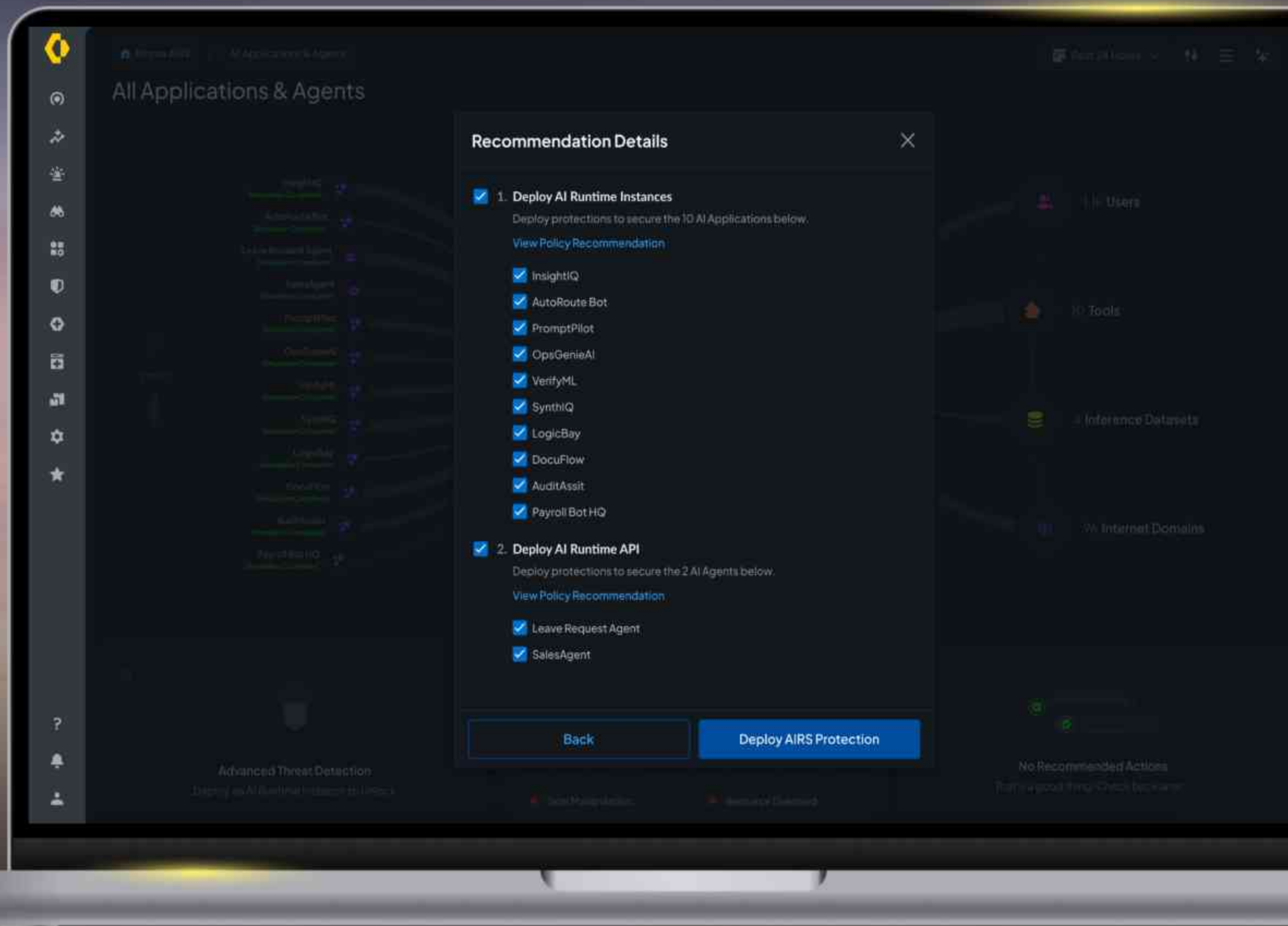
Detailed reporting

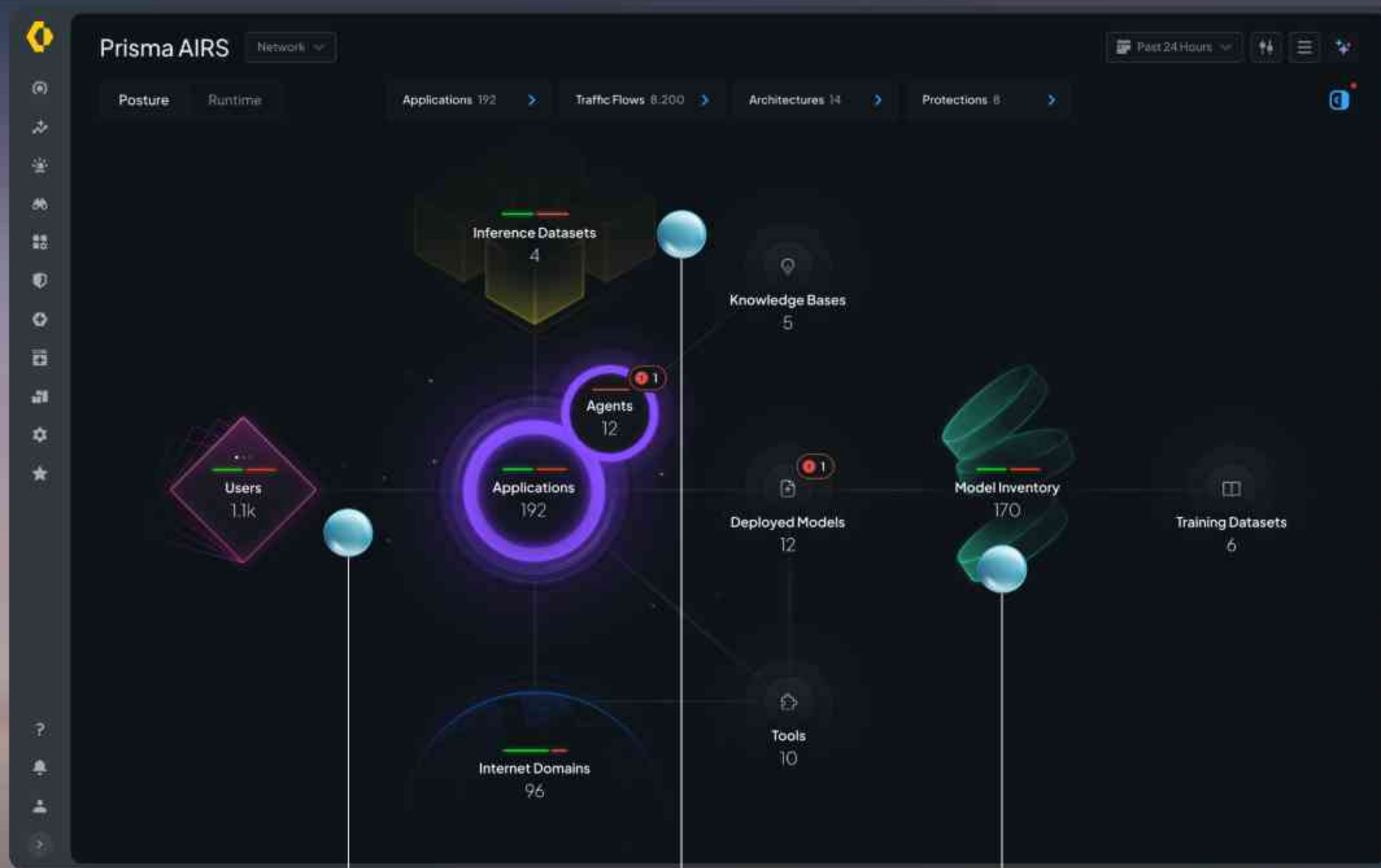
Comprehensive report detailing which attacks were successful and what sensitive information was extracted.



Policy Recommendations

Integrates with Runtime Security to provide real-time recommendations to improve AI security posture.





Protect

your AI **apps**
and agents

your AI **data**

your AI
models

Runtime Security

Protect AI applications, agents,
models and data at runtime.

Runtime Security **Network** or **Code**

Expand your virtual network protection to include AI security.

Network Centric

Secure your AI applications with
network-level enforcement.



AI and virtual network security
in a single firewall



Centralized platform

Developer Centric

Secure your AI applications
through code-level enforcement.



AI **security-as-code**

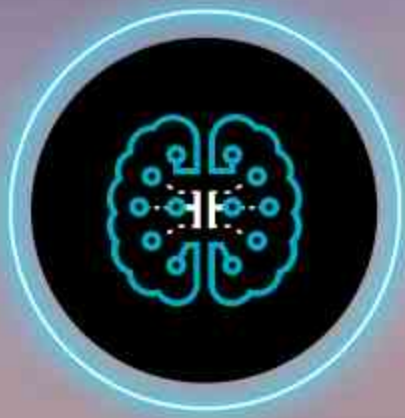


Simple setup in minutes

Use one or both approaches.

Configure policies once and apply consistently.

Granular AI Security for **Developers** via REST API or SDK



Secure any public
or private model.



Secure AI agents in no-code,
low-code and pro-code
environments.



Return custom error
responses based on
detected threats.



Scan batched training data
for threats and poisoning
before fine-tuning.

Implement API

Add the generated key and code in your environment to begin API calls.

API Key ⓘ

.....

Code Template ⓘ

```
1 import requests, json
2 json_object = {
3     "contents": [
4         [
5             "prompt": "Prompt string"
6         ]
7     ],
8     "ai_profile": {
9         "profile_name": "Profile UUID"
10    }
11 }
12 url = "API URL"
13 header = {'x-pan-token': 'API Key'}
14 }
```

.....

Back

Next

Your **AI Agents** Can



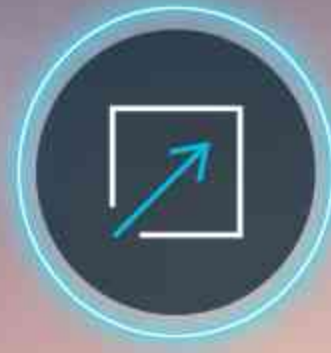
Remember



Plan



Learn



Act

Stop AI-Agent Specific Attacks



Memory
Poisoning



Tool
Misuse



Identity
Impersonation



Google AgentSpace



Azure AI Agent Service



Salesforce AgentForce



Sierra



Microsoft Copilot Studio



Agent System of Records



ServiceNow



crew ai



LangChain



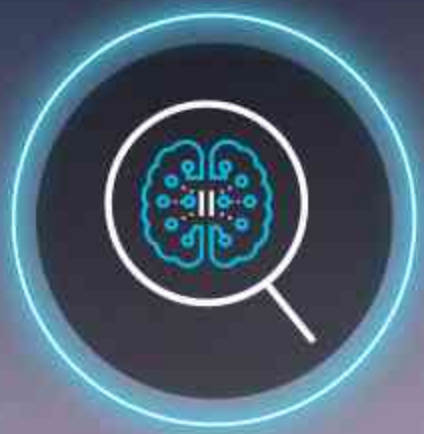
Agent Builder



Microsoft AutoGen



NVIDIA



Safeguarding Your AI Apps and Agents



Prevent exposure to harmful content

Detect and block harmful or toxic content in prompts and responses.



Keep your AI focused on your business

Create custom topic guardrails to define topics that your apps and agents should or should not discuss.



Stop your AI from hallucinating

Detect outputs that deviate from application knowledge source.

Superior Runtime with Palo Alto Protection Networks

Threat protection with the highest
efficacy and lowest false positive rates



AI Model Protection

Secure **any application** and **any model**

25+ types of prompt injections protected across **8 different languages**

< 0.1% false-positive rate



AI Data Protection

1,000+ predefined data patterns

2x greater coverage than other cloud-based data security solution

Infer and recommend AI data protection policies, based on training dataset



AI Application Protection

40% better protection from web-based attacks and protection from 25+ DNS attack types

99.58% malware detection accuracy with **26% more detection** than traditional sandboxes

AI-powered **prevention of 90%+** of zero-day app command and SQL injection attacks



AI Agent Protection

Protect AI agents in **no-code, low-code** and **pro-code** environments

Block **AI agent-specific threats**, such as memory manipulation, tool misuse, hallucination attacks

Custom **topic guardrails** and **harmful/toxic content** detection

Prisma AIRS Customer **Stories**

Global insurance company

USE CASE

Actively building GenAI apps on AWS but also have non-AI containerized apps in production

CHALLENGE

Gain **full visibility** and **security** for containerized AI and non-AI apps

Multinational consulting firm

USE CASE

Built a chatbot for all the consultants to expedite strategy and prep work before meeting with their clients

CHALLENGE

Accelerate **safe** and **secure adoption** of their co-pilot for 10,000+ consultants

Emerging AI SaaS company

USE CASE

Built multiple in-house GenAI apps for 1,000+ employees using several different LLMs

CHALLENGE

Secure AI-powered enterprise search and work **assistants**



The World's Most
Comprehensive
AI Security Platform

Securing Enterprises Building AI Applications with Palo Alto Networks



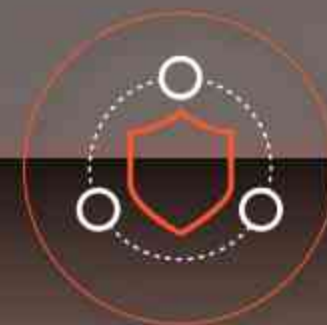
Industry's most comprehensive discovery

Of the entire AI app ecosystem
and risks.



Industry's only solution

To protect against supply chain,
configuration and runtime risks
for AI apps and models.



Most complete protection for all your data

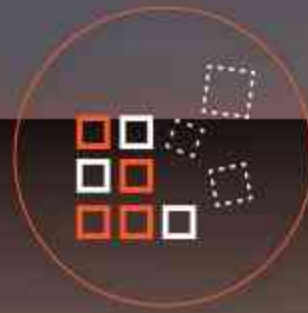
Prevent threats, such as
prompt injection, while
protecting data throughout its
lifecycle with predefined data
patterns.

Securing AI with the Power of Precision AI



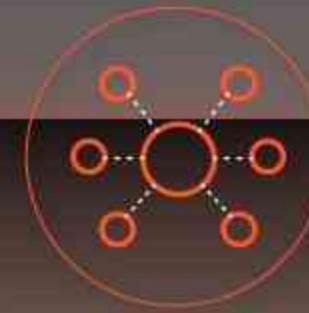
Easy discovery

Accurately and visually see your entire AI app ecosystem.



Simplicity of adoption

With a platform approach integrated across development and runtime to secure all apps.



Most comprehensive coverage

Industry's most comprehensive coverage of OWASP Top 10 LLM risks. Cover supply chain risks, configuration risks and runtime risks.



Best-in-class security

Accurately prevent threats, protect sensitive data throughout its entire lifecycle, and enable real-time threat prevention with runtime data loss protection.

How to Get Started with Prisma AIRS

Completely free, no-risk enterprise AI app ecosystem **discovery** of app workloads, models, datasets, plugins and users.

Gain visibility into **runtime risk exposure** of your AI apps.



Learn more about our capabilities.



Get started with a guided demo or free trial.



Thank You

paloaltonetworks.com



Appendix

Secure AI by Design personalized Demo

See firsthand how to discover, protect
and monitor your AI usage and apps.

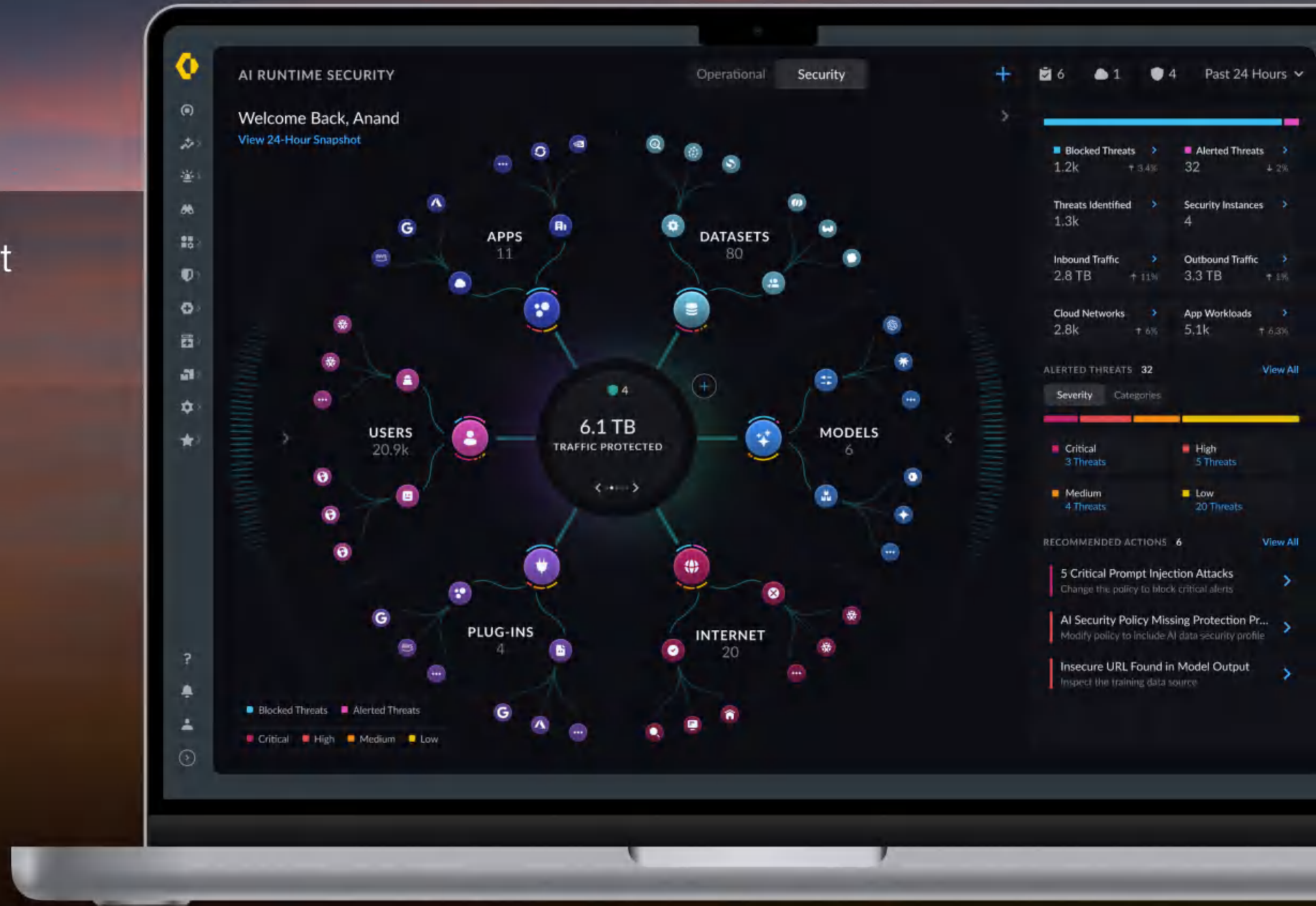
Sign up for one-on-one demos:



Free demo
AI Access Security



Free demo
Prisma AIRS



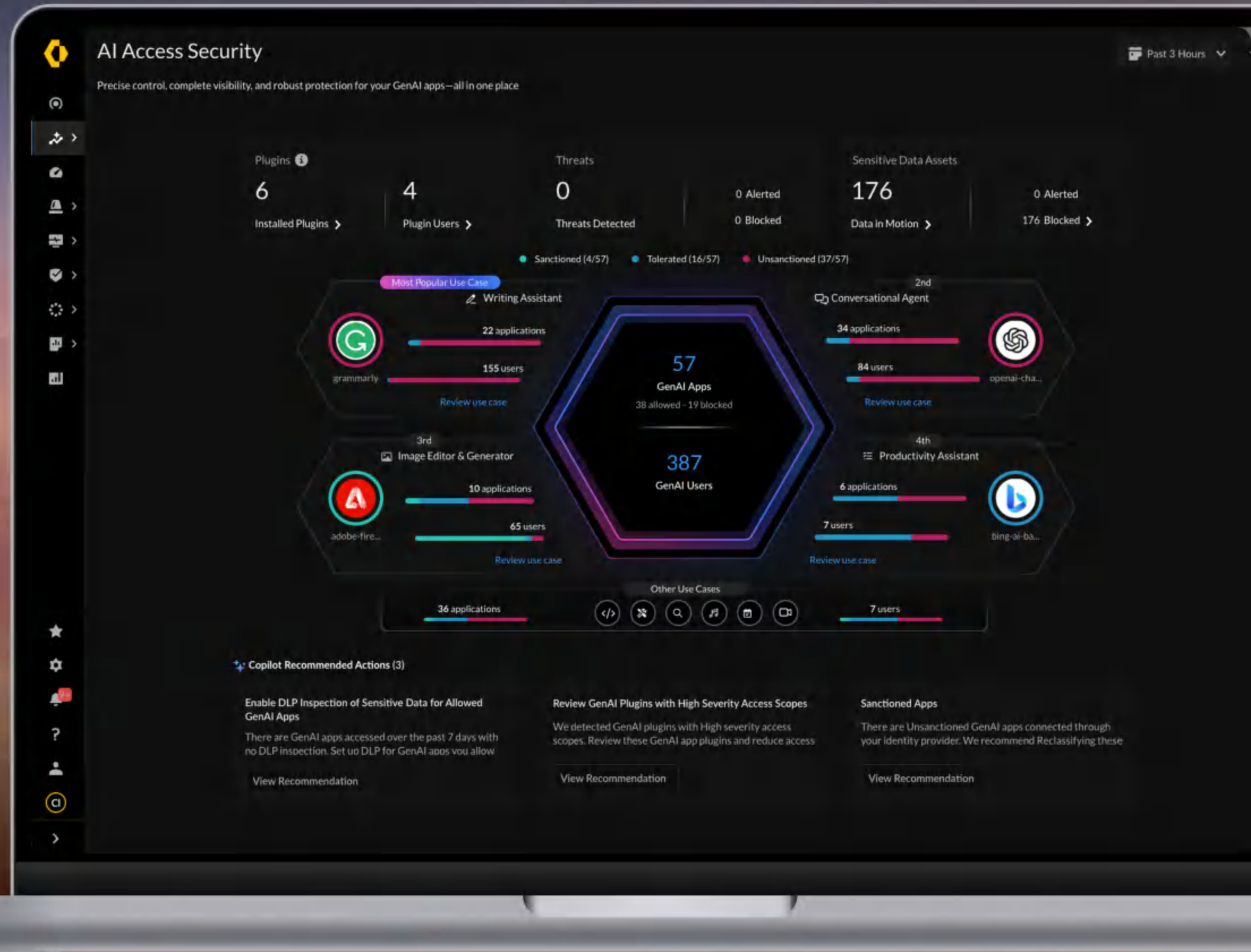
Ultimate Test Drive

Experience for yourself our AI solutions from your home or office.

Get behind the driver's seat to experience a virtual, no-cost, hands-on workshop that's designed for every experience level.



Register for the free
Hands-on workshop



Demo Time

How to Secure GenAI Usage

Video



Demo Time

How to Secure GenAI Apps

Prisma AIRS Runtime
Security

[Script](#)



[Video](#)

