



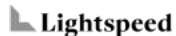
Accelerate AI innovation securely with AI-SPM

Joel Desaulniers
Sr. Solutions Engineer, Wiz



The Largest Private
Cybersecurity Company

\$1.9B raised



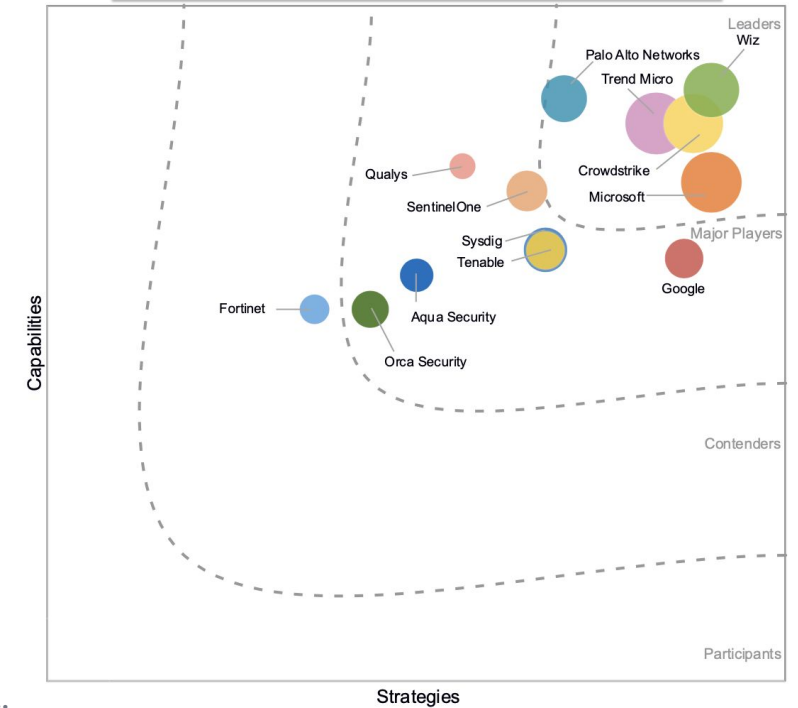
Enabling Security Impact

50% Of Customers
achieve 0 Criticals

> 50% Of Active Users
are Devs/DevOps

More than 50% of the Fortune 100 secure their cloud with Wiz

IDC MarketScape: Worldwide Cloud-Native Application Protection Platform, 2025



Morgan Stanley



MassMutual



JPMorgan Chase & Co.



LVMH



Honeywell



Fannie Mae



abbvie



BlackRock



The cloud has changed
everything

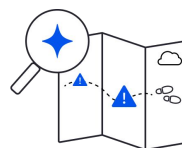


Cloud changed everything



New
environment

**How do I get visibility
into my environment?**



New risks

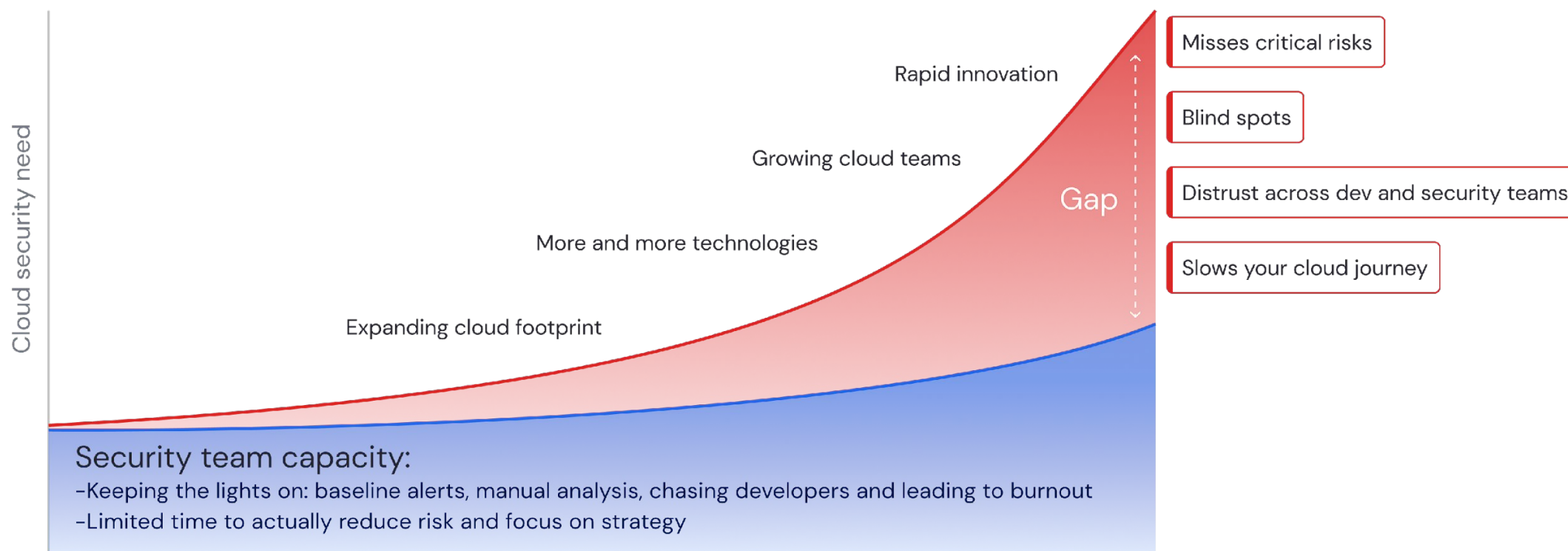
**How do I prioritize the real
risks and eliminate the noise?**



New ownership model

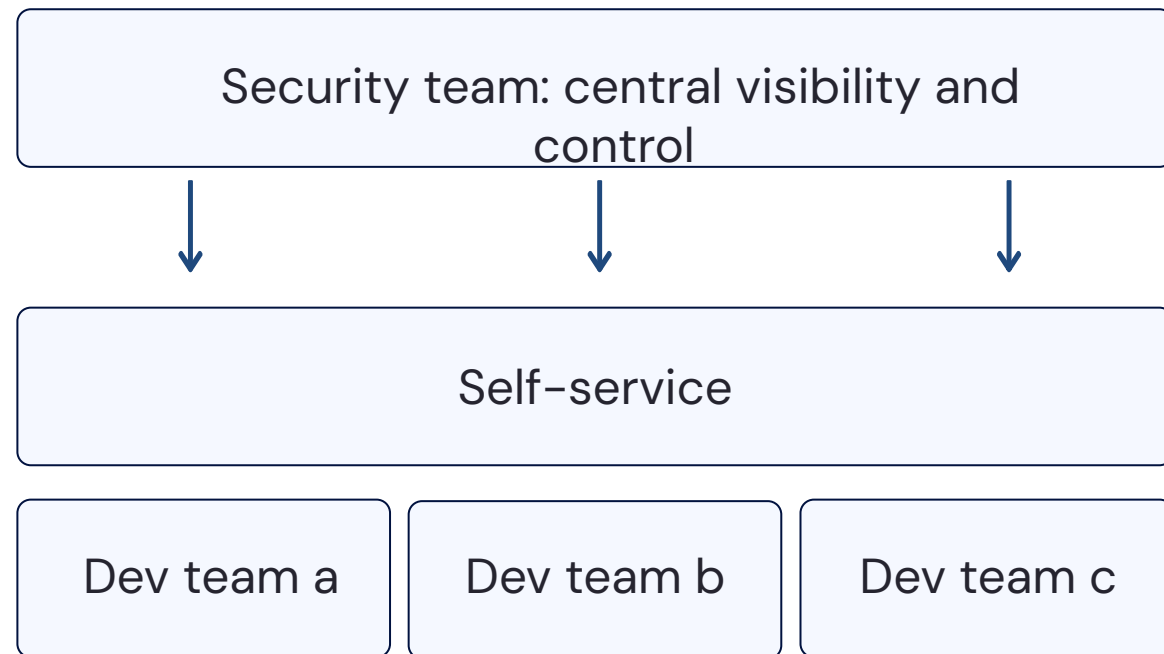
**How do I ingrain
security into our teams?**

Security teams could not keep up with the cloud



Cloud
security
needed
a new
operating
model

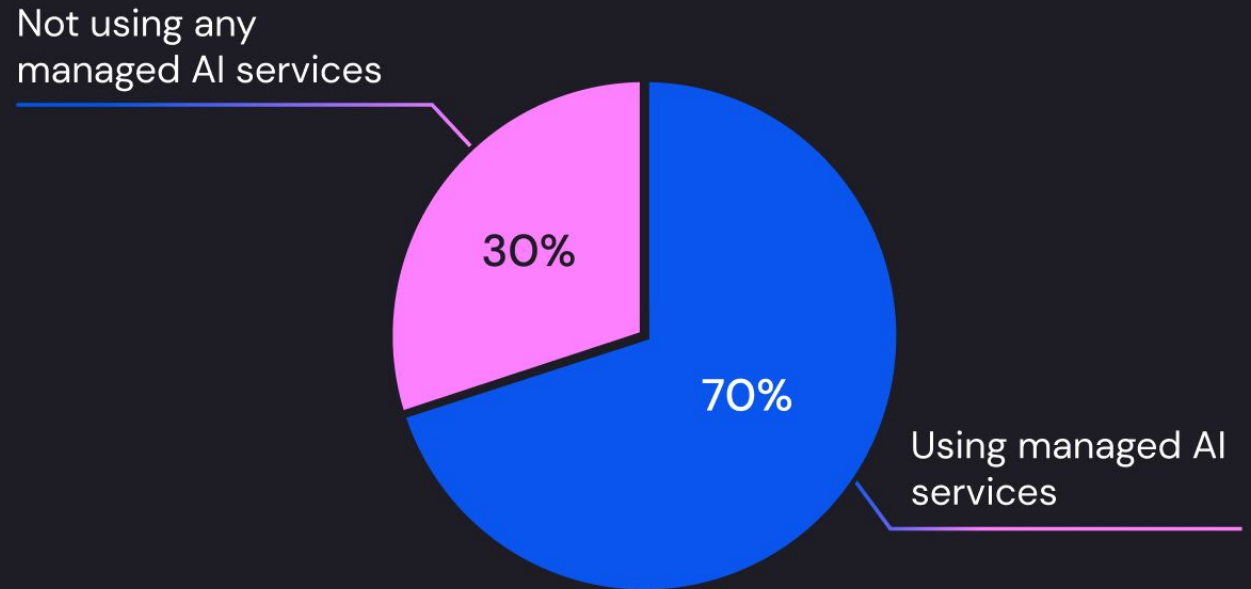
Cloud security is a team sport



AI changes everything
again!

AI has taken
over the cloud:
Cloud-based
managed AI
services can
already be found
in over 70% of
environments

Percent of cloud environments
using managed AI services



Inaccuracy, cybersecurity, and intellectual-property infringement are the most-cited risks of generative AI adoption.



Generative AI-related risks that organizations consider relevant and are working to mitigate,
% of respondents

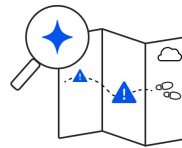


AI adoption adds a new layer of complexity



New
environment

**Complex system and data
pipelines**



New risks

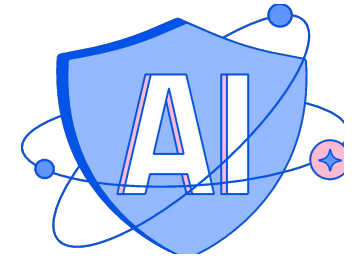
**Data leakage, model
vulnerabilities**



New skills to uplift

**AI researchers, data
scientists & data engineers**

We learned from the cloud, let's apply the learnings to AI

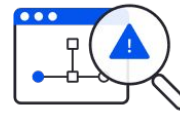


1



Visibility is the foundation

2



Risk-based approach is critical

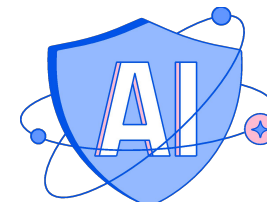
3



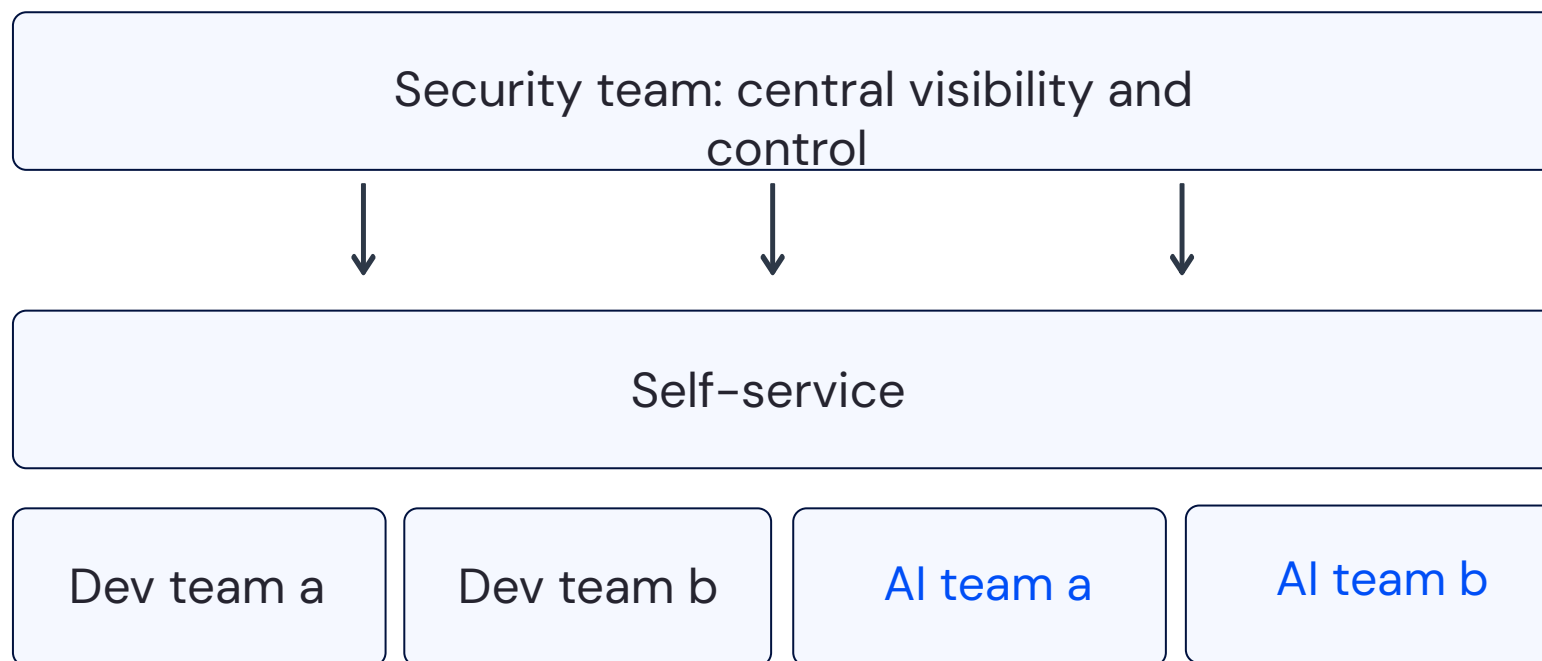
Secure across the AI-pipeline with context

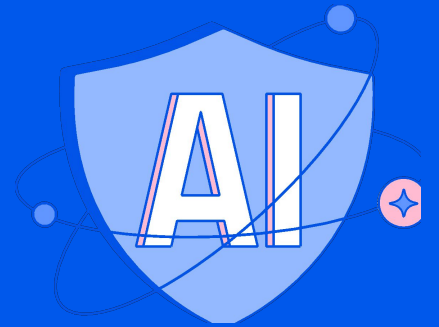
From CSPM to **AI-SPM**, cloud security evolves with innovation

AI introduces new teams to the security operating model



Extend the cloud security operating model to AI





AI-SPM: The four questions security organizations need to ask





1. Do I know every AI service, model and agent running in my environment?



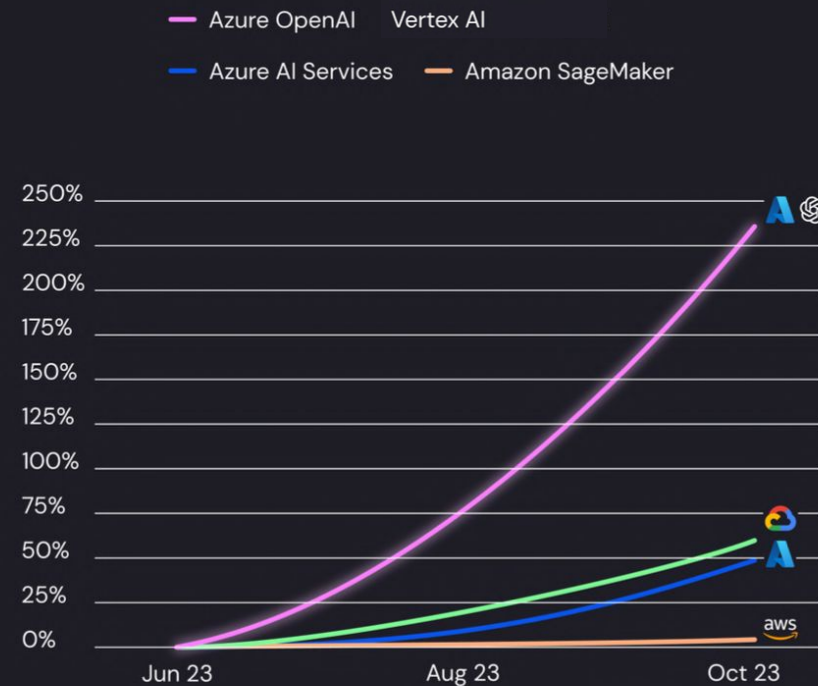
1. Massive adoption of AI services

Azure OpenAI is seeing explosive growth:

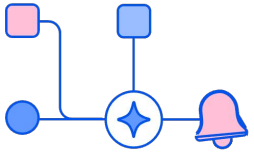
Organizations have recently more than tripled their use of Azure OpenAI instances

WIZ⁺Research

Growth of cloud AI service instances

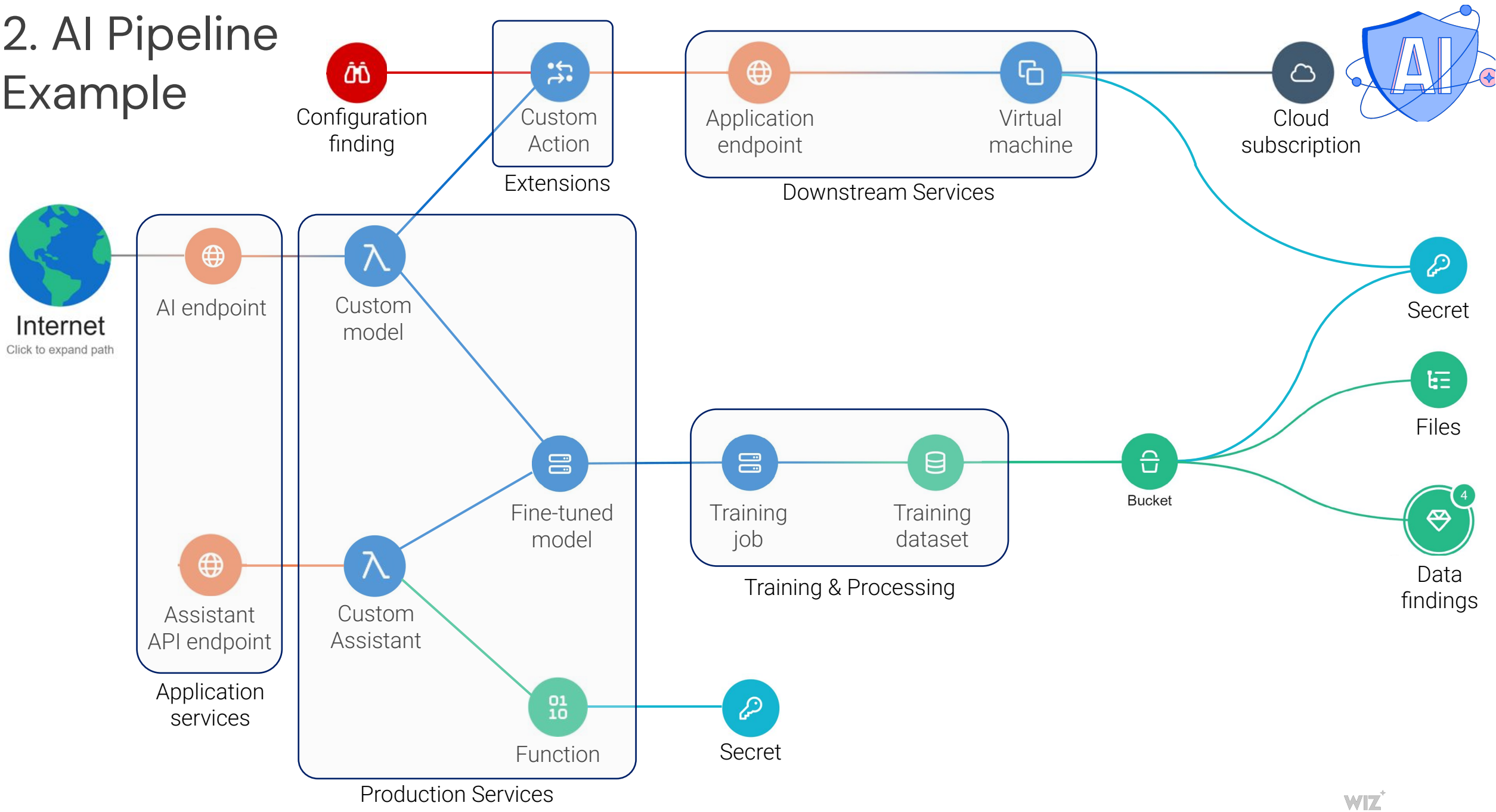


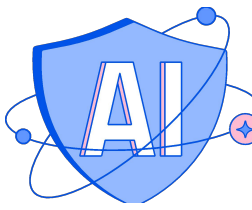
Source: State of AI in the Cloud 2024



2. Do I know the risks in each AI pipeline?

2. AI Pipeline Example





3. Can I prioritize which AI risks matter most?

3. Real-life example of an AI toxic combination



Wiz Research Uncovers Exposed DeepSeek Database Leaking Sensitive Information, Including Chat History

A publicly accessible database belonging to DeepSeek allowed full control over database operations, including the ability to access internal data. The exposure includes over a million lines of log streams with highly sensitive information.



Gal Nagli

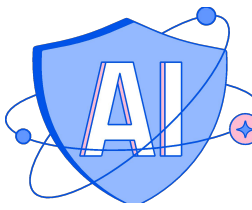
January 29, 2025

3 minute read



Table of contents

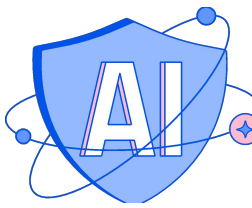
- Executive Summary
- Exposure Walkthrough
- Key Takeaways
- Conclusion



4. Can I detect and respond to AI misuse?

4. Can I detect misuse in my AI Pipelines?

Threat detection to respond to AI threats in real time



Real-time Threat detection

Anomaly Detection

Detect Attack Paths

Malicious AI Model detected

Detected events

Nov 26th 04:02:01 PM to Nov 26th 06:55:53 PM

Fileless execution was detected

Process image path resolved to memfd or shared memory (shm). Memfd (memory file descriptor) and shm (shared memory) are interprocess communication mechanisms in Linux where memfd allows for the creation of anonymous memory objects that can be shared between processes using file descriptors, while shm enables the creation of shared memory segments that allow multiple processes to access and exchange data efficiently in a fast and synchronized manner. This could indicate the presence of a threat actor achieving fileless execution.

Raw Event Details

Stdin /dev/pts/0

Stderr pipe:[79873268]

Process Tree

gke-sensor-ci-1 Virtual Machine

[1] /usr/lib/ Process

[2030] Process

[1513] Process

[1] Process

Anomalous activity detected in AI Model execution engine

Comment Run an Action Create a Ticket Give Feedback

Overview Remediation Comments

Process created a connection to a domain associated with cryptomining activities. Connection to cryptomining domains may indicate a threat actor abusing and diverting system resources to mine digital currencies.

Status Open

Evidence

AI Model escape detected

Comment Run an Action Create a Ticket Give Feedback

Overview Remediation Comments

Process read a file resource used to manage users information by the operating system (/etc/shadow or /etc/gshadow). The "/etc/shadow" and "/etc/gshadow" files in Linux store encrypted user account information and group account information, respectively, providing an extra layer of security by keeping sensitive password-related data inaccessible to regular users. This could indicate the presence of a threat actor achieving credential theft and general user information discovery.

Status Open

Due No due date

Related Tickets 0 Tickets

Created Nov 20, 2023 at 4:00 PM

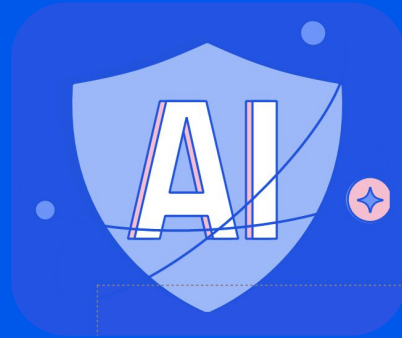
Updated

Subscription No projects Risks

Severity High Type Threat Detection Issue Related Frameworks

TA0001-T1078.001 Valid Accounts: Default Accounts

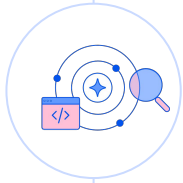
Introducing Wiz AI-SPM



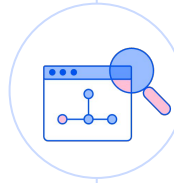
Wiz provides native AI security capabilities, empowering organizations to accelerate AI innovation while staying protected against AI risks.



The core components of **Wiz AI-SPM**



Visibility into AI pipelines



Proactively remove AI risks with context



Detect misconfigurations in AI services



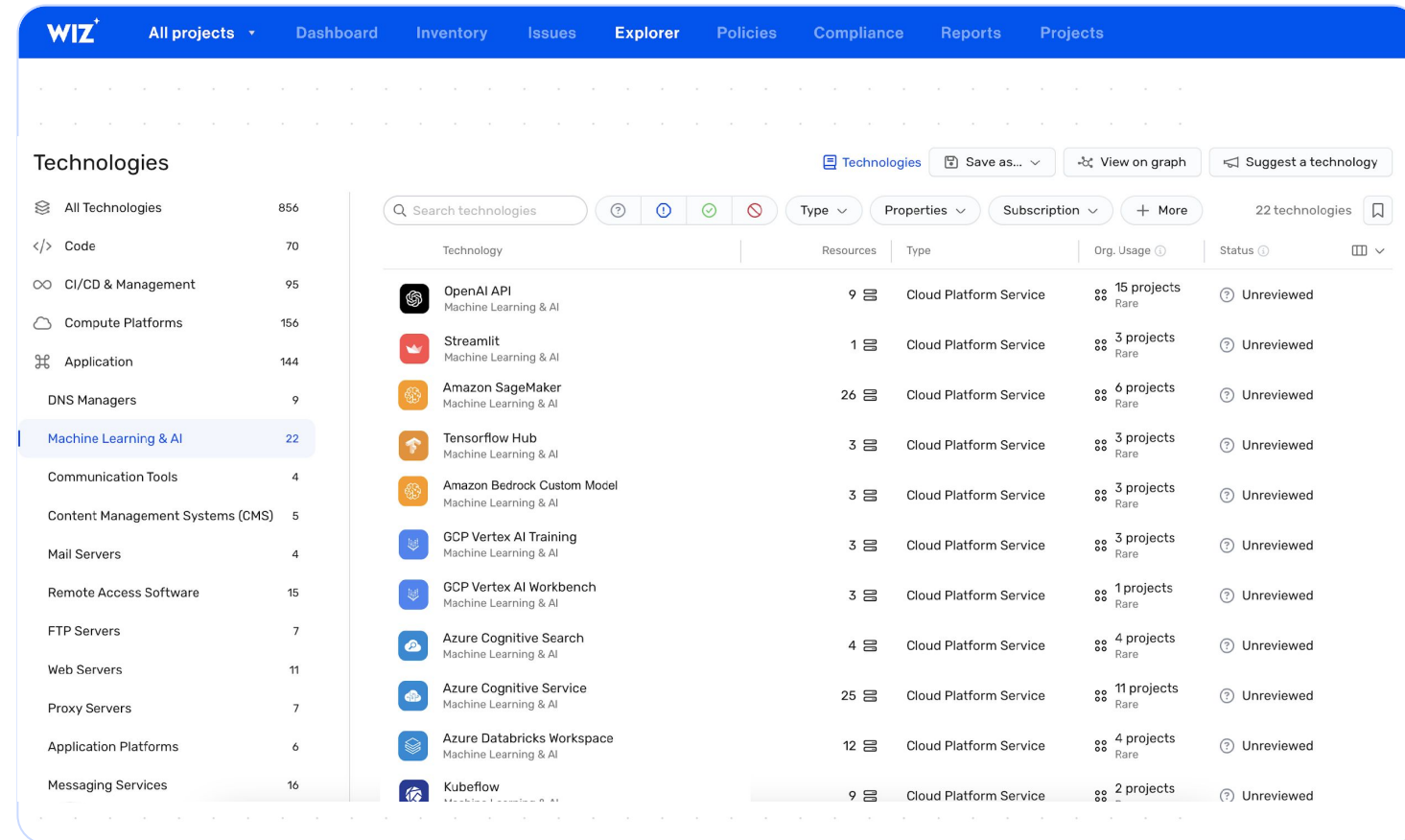
Empower AI developers with an easy-to-understand UI

Agentless visibility with AI-BOM

Detect every AI technology with AI-BOM
AI Services, SDKs, etc all without agents

Remove shadow-AI
Immediate visibility into new AI services

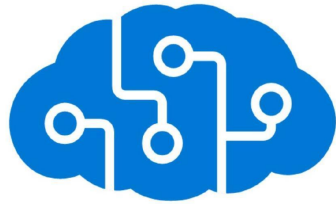
End-to-end AI pipeline visibility
Detect every resource in AI pipelines, from the
machine hosting the training job, to the data
stores



The screenshot displays the WIZ AI-BOM interface. The top navigation bar includes the WIZ logo and tabs for All projects, Dashboard, Inventory, Issues, Explorer, Policies, Compliance, Reports, and Projects. The main content area is titled 'Technologies' and features a sidebar on the left with a list of technology categories and their counts. The 'Machine Learning & AI' category is selected, showing 22 technologies. The main table lists these technologies, including OpenAI API, Streamlit, Amazon SageMaker, TensorFlow Hub, Amazon Bedrock Custom Model, GCP Vertex AI Training, GCP Vertex AI Workbench, Azure Cognitive Search, Azure Cognitive Service, Azure Databricks Workspace, and Kubeflow. Each entry shows the number of resources, the type of service, the number of projects it is used in, and its status (Unreviewed).

Technology	Resources	Type	Org. Usage	Status
OpenAI API Machine Learning & AI	9	Cloud Platform Service	15 projects Rare	Unreviewed
Streamlit Machine Learning & AI	1	Cloud Platform Service	3 projects Rare	Unreviewed
Amazon SageMaker Machine Learning & AI	26	Cloud Platform Service	6 projects Rare	Unreviewed
Tensorflow Hub Machine Learning & AI	3	Cloud Platform Service	3 projects Rare	Unreviewed
Amazon Bedrock Custom Model Machine Learning & AI	3	Cloud Platform Service	3 projects Rare	Unreviewed
GCP Vertex AI Training Machine Learning & AI	3	Cloud Platform Service	3 projects Rare	Unreviewed
GCP Vertex AI Workbench Machine Learning & AI	3	Cloud Platform Service	1 projects Rare	Unreviewed
Azure Cognitive Search Machine Learning & AI	4	Cloud Platform Service	4 projects Rare	Unreviewed
Azure Cognitive Service Machine Learning & AI	25	Cloud Platform Service	11 projects Rare	Unreviewed
Azure Databricks Workspace Machine Learning & AI	12	Cloud Platform Service	4 projects Rare	Unreviewed
Kubeflow Machine Learning & AI	9	Cloud Platform Service	2 projects Rare	Unreviewed

Supported AI cloud services



Amazon SageMaker



Amazon Bedrock



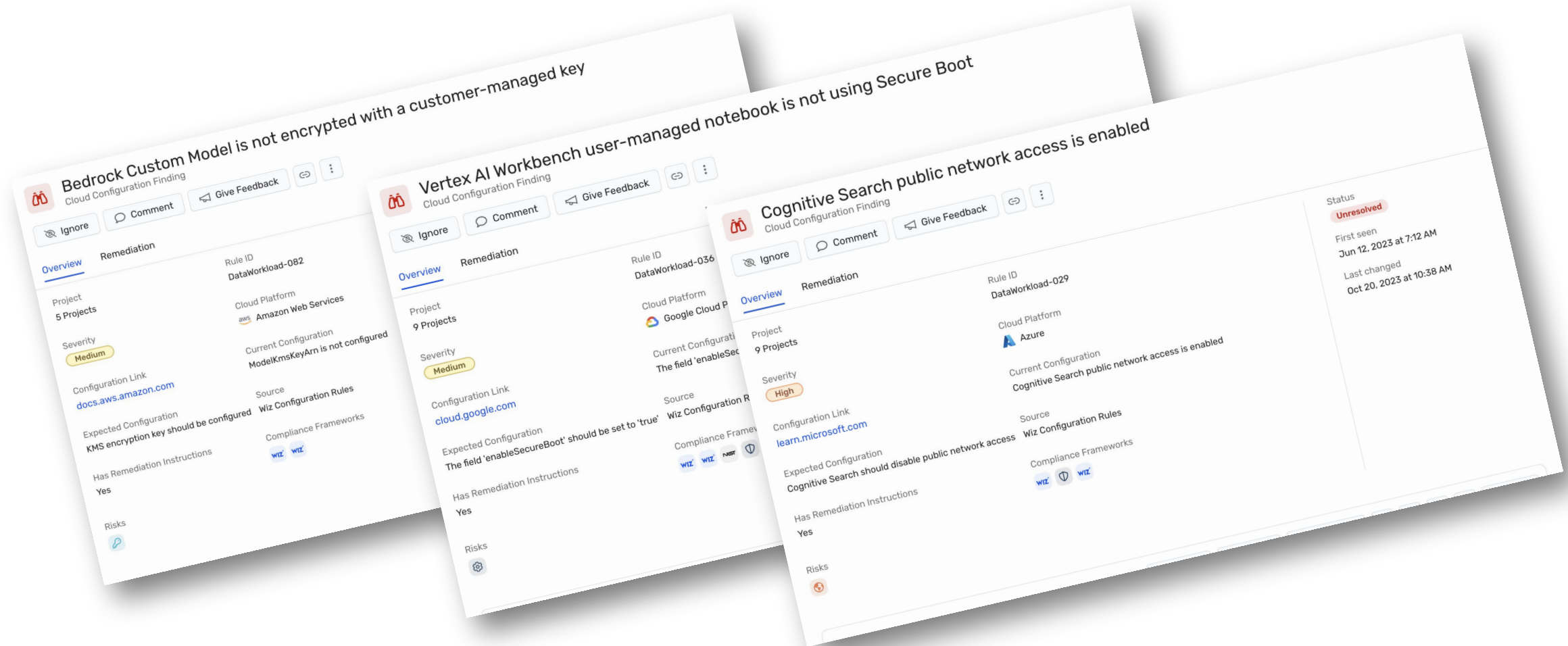
OpenAI



Vertex AI

AI Misconfigurations

Built-in misconfigurations rules for AWS Sagemaker, Amazon Bedrock, Google Vertex AI, Azure OpenAI, OpenAI



Detect attack paths to AI and protect crown jewels

Deep risk analysis in AI pipelines

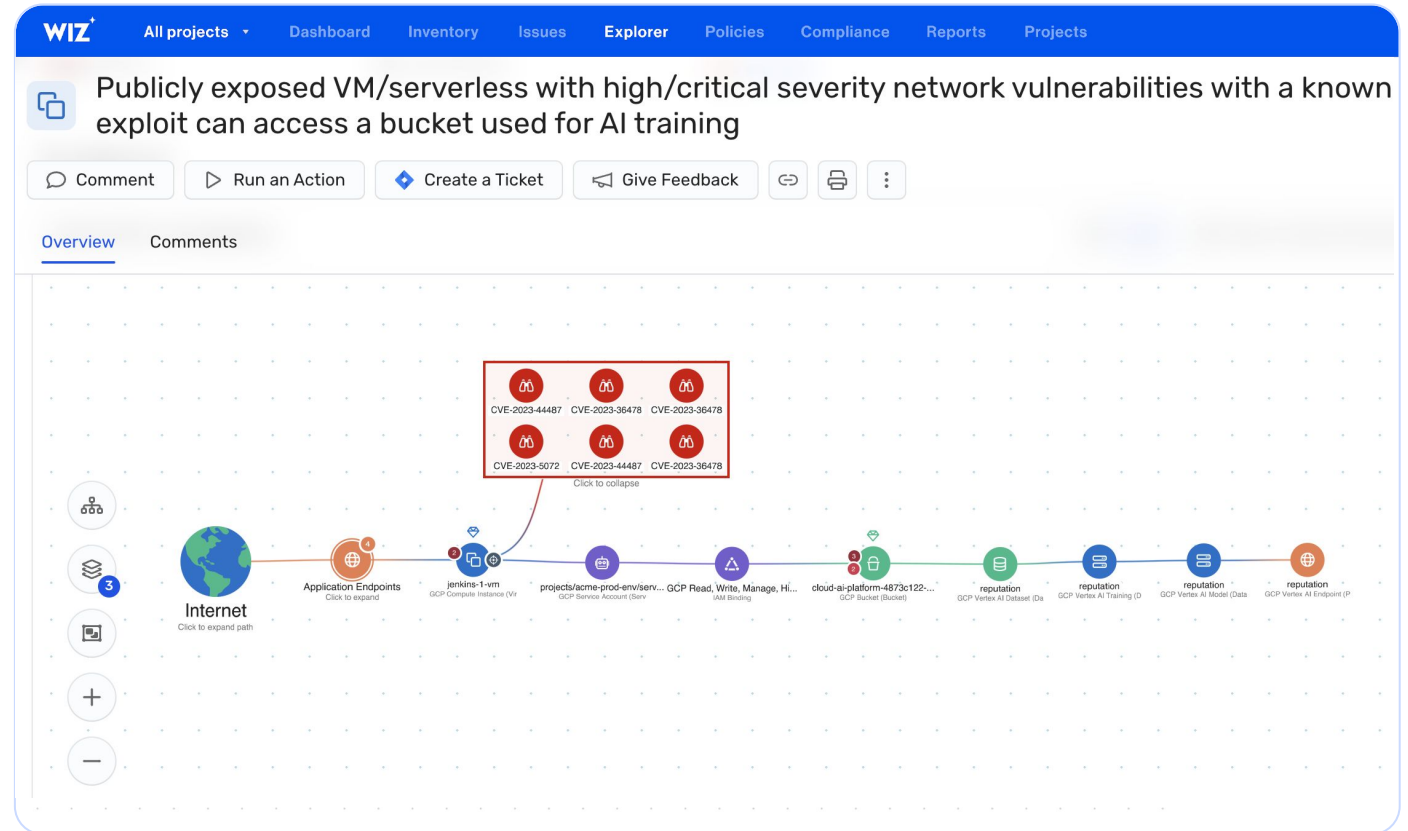
Detect AI vulnerabilities, misconfigurations, permissions, data, secrets, and network exposure

Protect sensitive training data

Protect sensitive AI training data and remove risks such as data poisoning

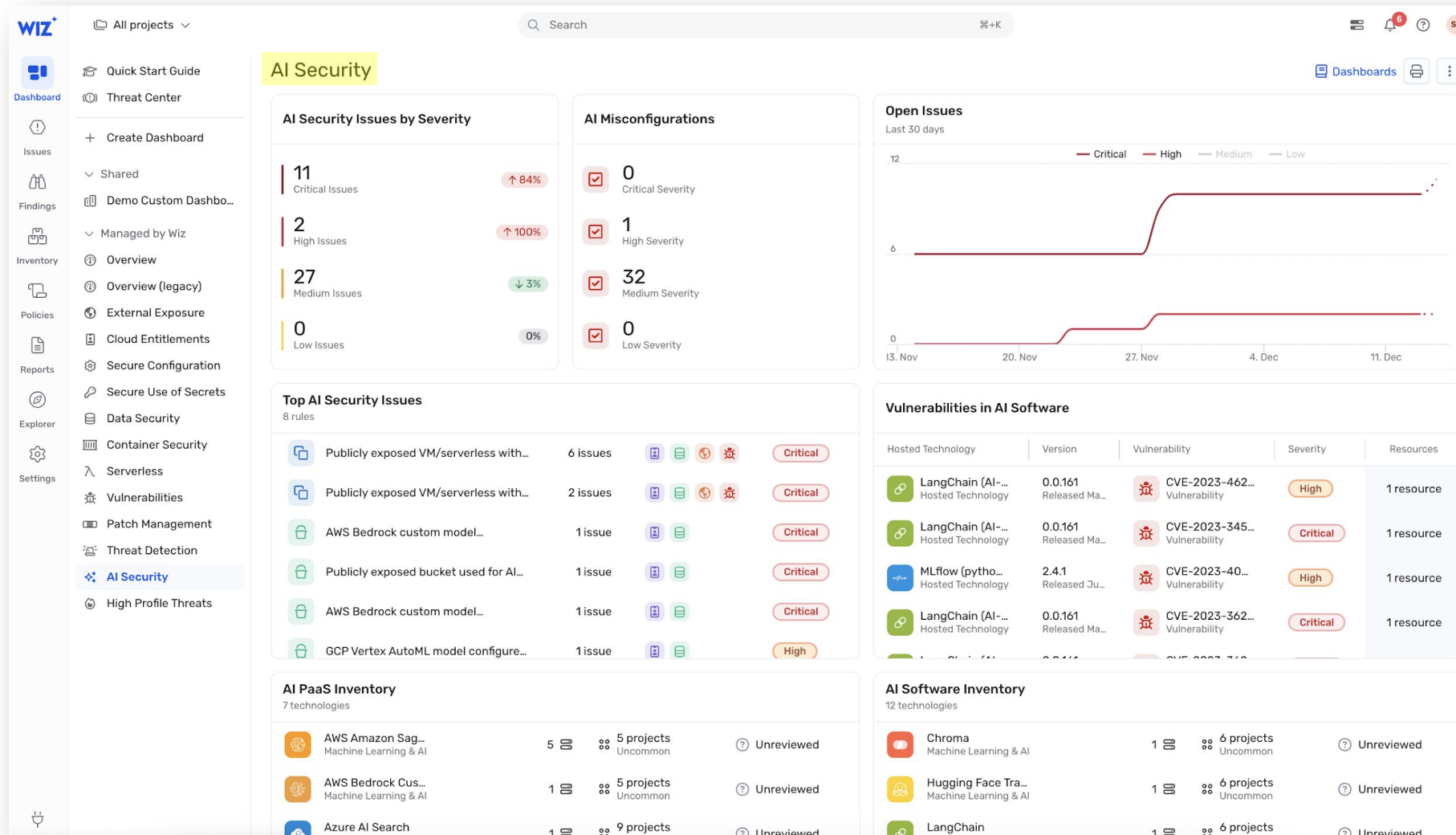
Remove critical attack paths to AI models

Proactively remove the most critical risks with context



Centralized view of AI security posture

Empower developers and data scientists with a prioritized queue of AI risks



AI-SPM: Let's apply our cloud learnings to AI

Do I know every AI service, model and agent running in my environment?



Do I know the risks in each AI pipeline?



Can I prioritize which AI risks matter most?



Can I detect and respond to AI misuse?





Want to see more magic about Wiz AI-SPM?

Follows us on LinkedIn

[linkedin.com/company/
wizsecurity](https://linkedin.com/company/wizsecurity)

Book a demo

wiz.io/demo

Learn about Wiz AI-SPM

[wiz.io/solutions/ai-security-pos
ture-management](https://wiz.io/solutions/ai-security-posture-management)

Joel Desaulniers
Sr. Solutions Engineer, Wiz

Let's chat more!