



Accelerating Cloud Security to enable AI:

How security teams can adopt a new operating model to enable agile AI adoption



Matt Preswick
Principal Solutions Engineer, APJ



The cloud has changed
everything

Cloud changed everything



New
environment

How do I get visibility
into my environment?



New risks

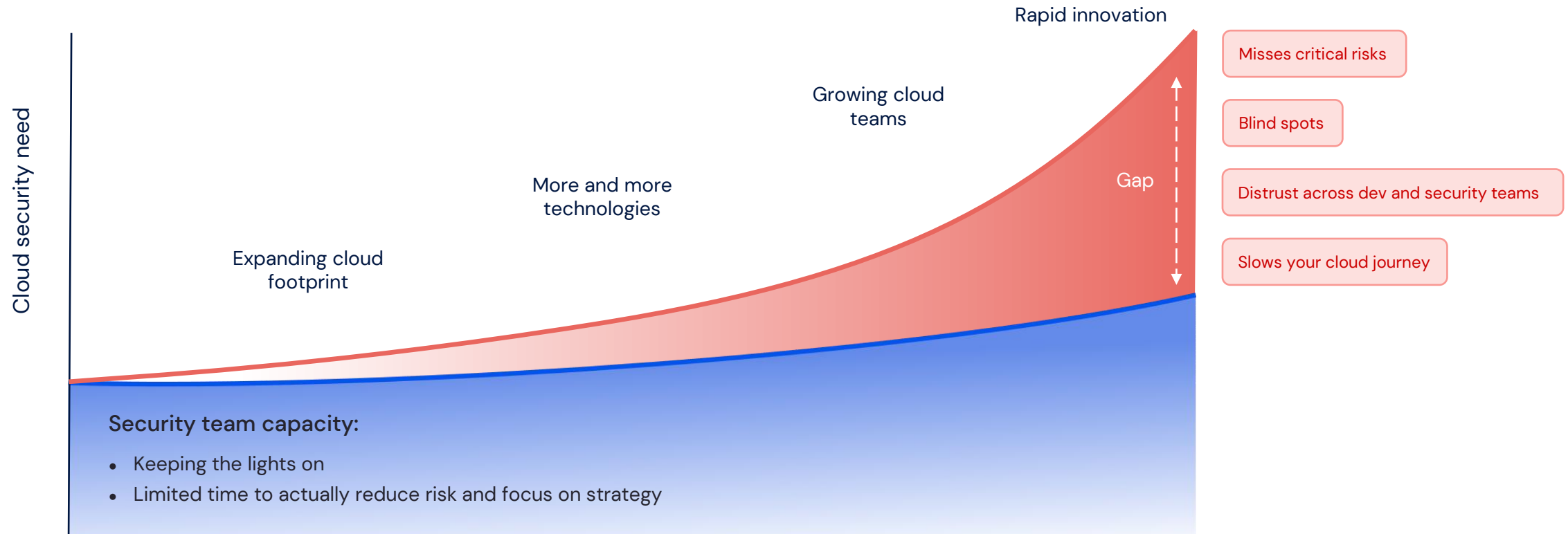
How do I prioritize the real
risks and eliminate the noise?



New ownership model

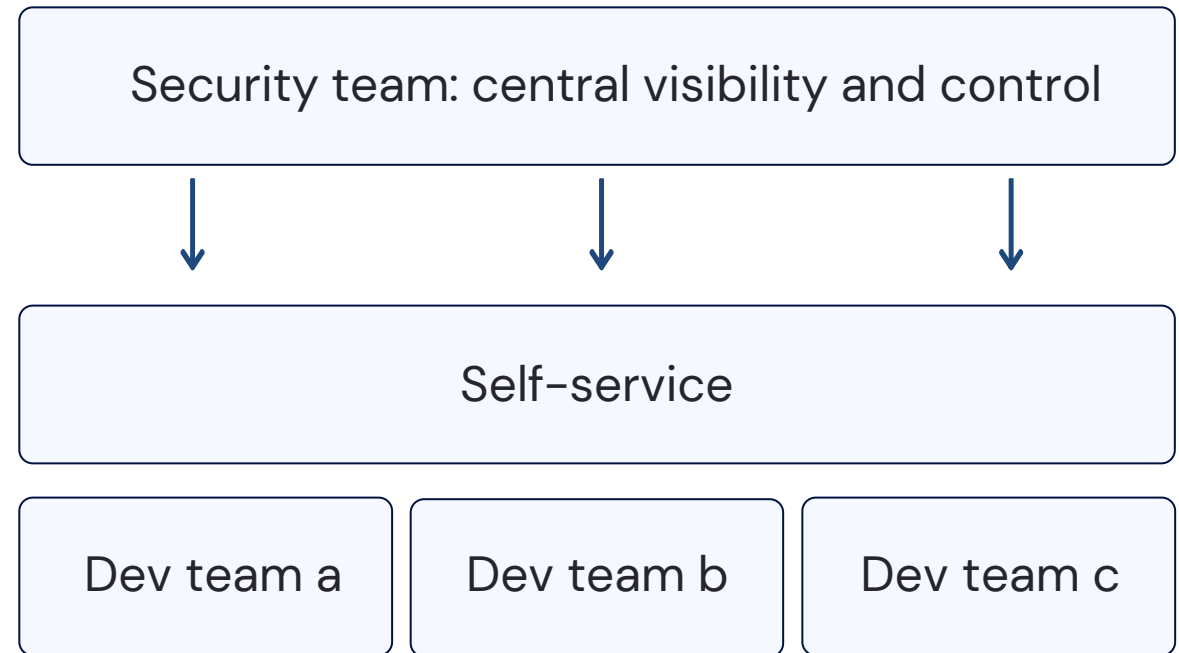
How do I ingrain
security into our teams?

Security teams are struggling to keep up with pace of cloud



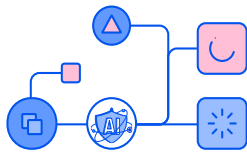
Cloud
security
needs
a new
operating
model

Cloud security is a team sport



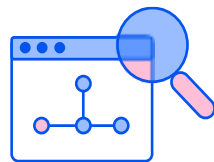
AI changes everything
again!

AI Adoption adds a new layer of complexity



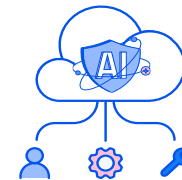
More new
environments

Complex system and data
pipelines



More new
risks

Data leakage, model
vulnerabilities



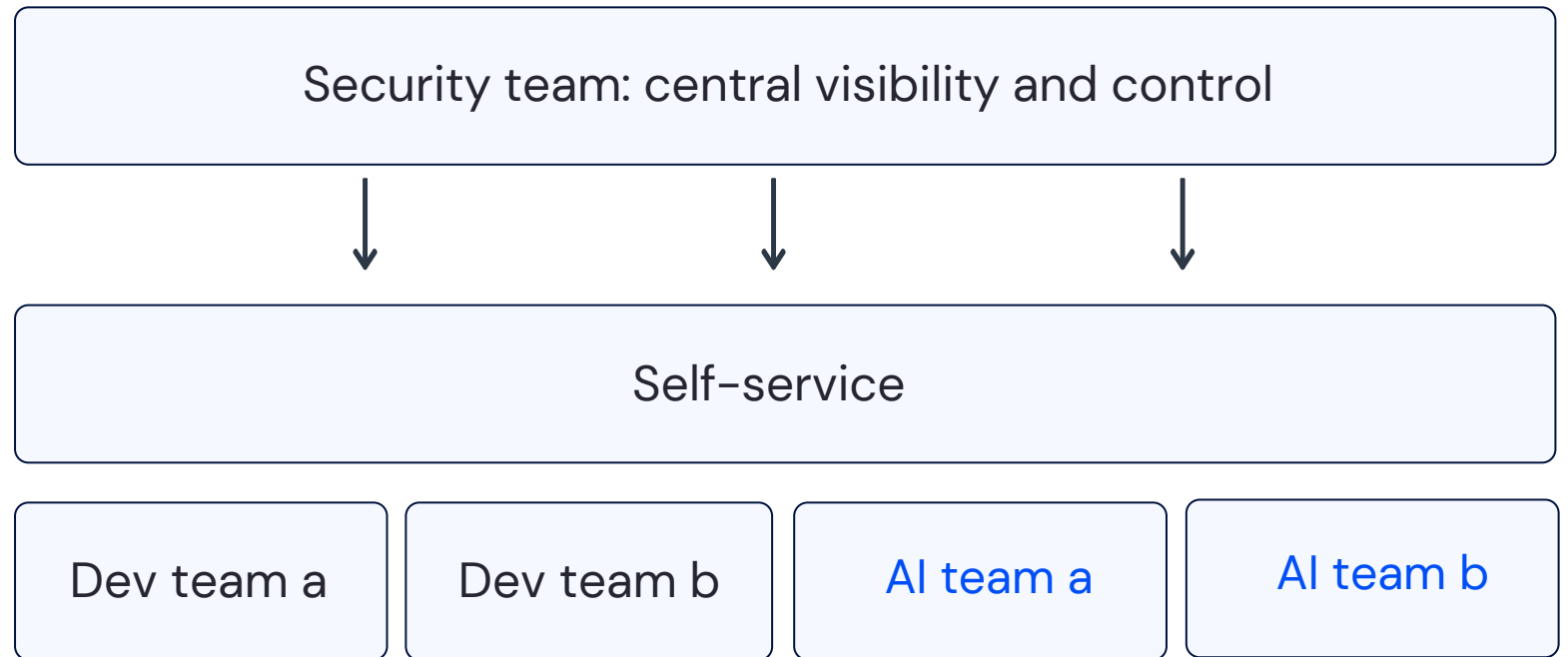
More new
Ownerships

AI researchers, data
engineers

AI introduces new teams to the security operating model

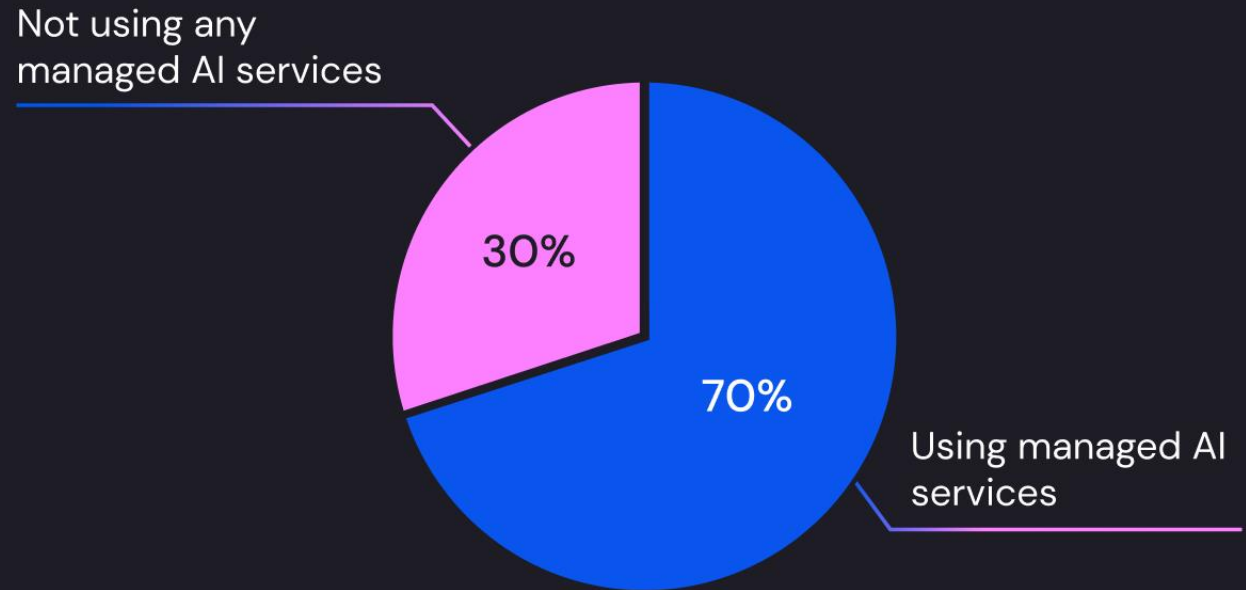


Extend the cloud security operating model to AI

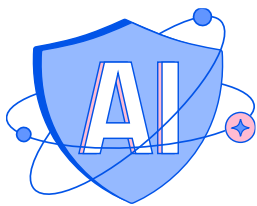


AI has taken
over the cloud:
Cloud-based
managed AI
services can
already be found
in over 70% of
environments

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 respondents¹



¹Asked only of respondents whose organizations have adopted AI in at least 1 function. For both risks considered relevant and risks mitigated, n = 913.
Source: McKinsey Global Survey on AI, 1,684 participants at all levels of the organization, April 11–21, 2023



Security is a main AI adoption blocker.



AI security knowledge gap

Lack of knowledge in AI

Security teams lack experience in AI systems and pipelines

AI pipelines are complex

AI system design is fragmented across multiple tools and steps. Requires a new approach to assess holistically.

AI teams lack security awareness

AI researchers tend to focus on delivery rather than a security-first mindset



New & unknown risks

Data leakage

What data might leak from the model? Is the training data exposed or sensitive?

Vulnerabilities in AI models

What makes an AI model vulnerable? Can an attacker manipulate it?

Lateral movement

How can attackers escalate via direct model interaction? Via training data poisoning? Via cloud tokens and permissions?



Rapidly evolving technology

Explosion in usage of AI services

Multiple AI projects are started in every team, impossible to track

Complex architectures

Dynamic and diverse set of AI build options, each with different risks

Thousands of technologies

Growing # of services, applications, libraries

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

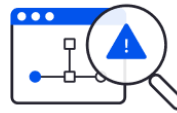


1



Visibility is the foundation

2



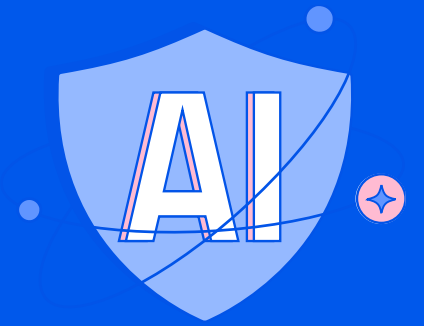
Risk-based approach is critical

3



Secure across the AI-pipeline with context

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

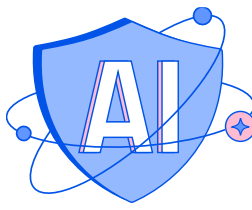


AI-SPM: The four questions security organizations need to ask

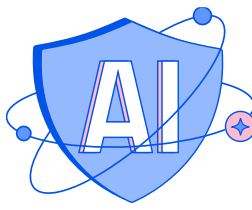


AI-SPM: The four questions security org s need to ask

- ☐ Do I know what AI services and technologies are running in my environment?
- ☐ Do I know what risks exist in my AI pipeline?
- ☐ Can I prioritize the critical risks across the AI pipeline?
- ☐ Can I detect a misuse in my AI pipelines?



1. Do I know what AI services and technologies are running in my environment?



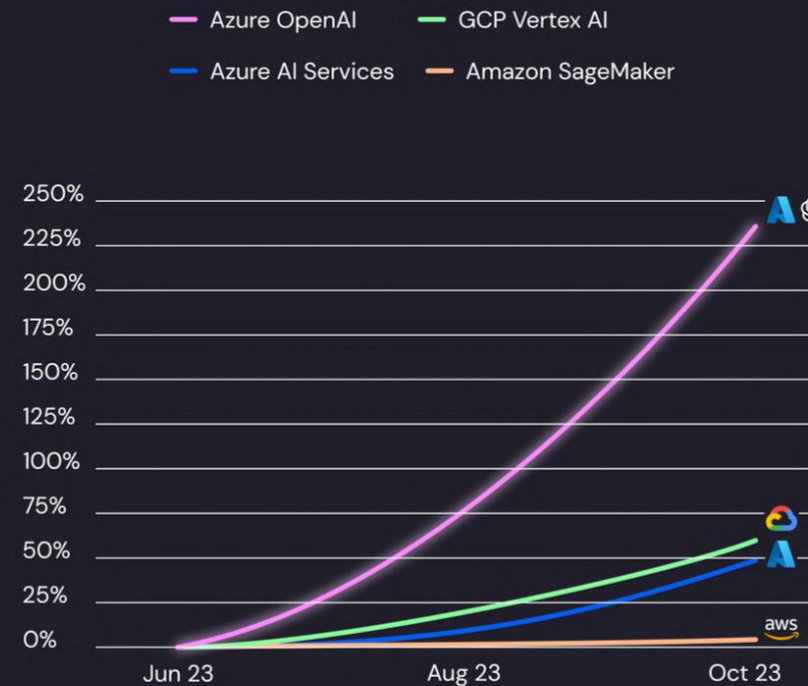
Massive adoption of AI services

Azure OpenAI is seeing explosive growth:

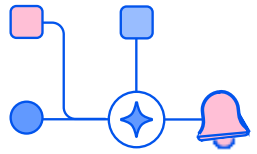
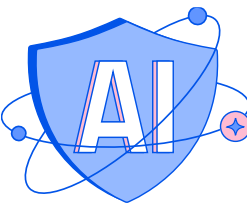
Organizations have recently more than tripled their use of Azure OpenAI instances

WIZ⁺ Research

Growth of cloud AI service instances

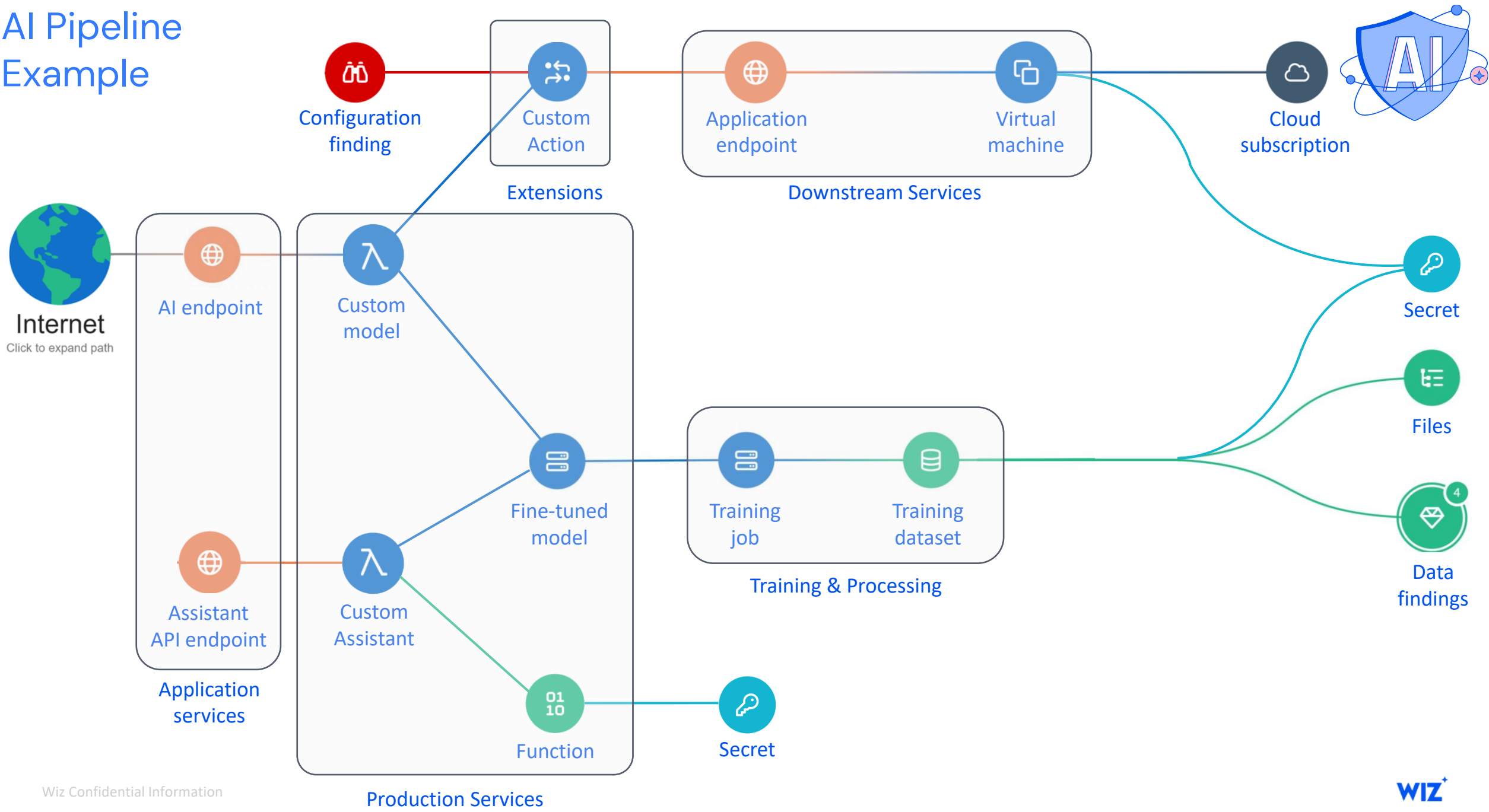


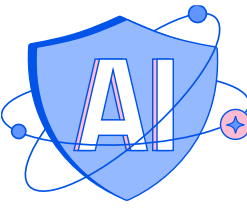
Source: [State of AI in the Cloud 2024](#)



2. Do I know what risks exist in my AI pipeline?

AI Pipeline Example





3. Can I prioritize the critical risks across the AI pipeline?

Real-life example of an AI toxic combination



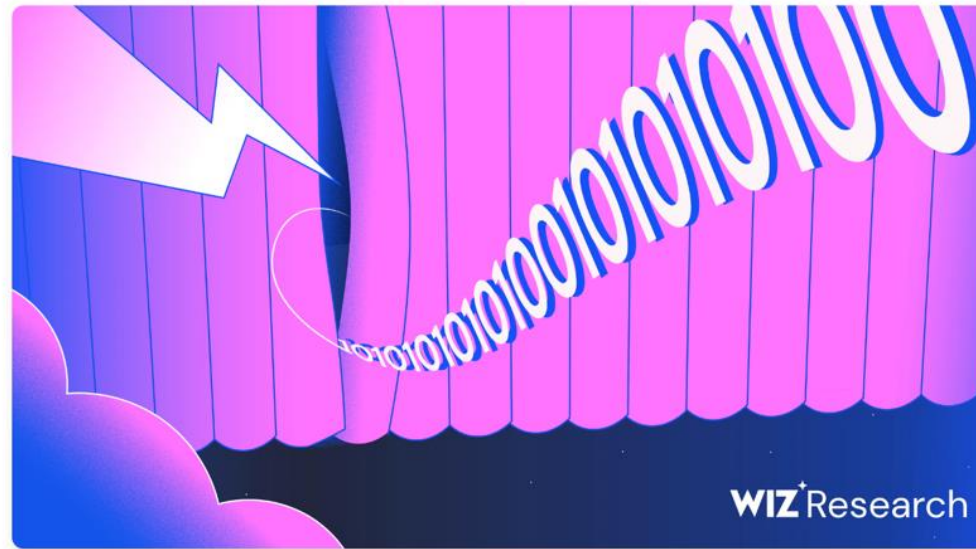
38TB of data accidentally exposed by Microsoft AI researchers

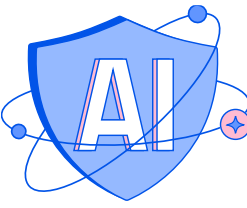
Wiz Research found a data exposure incident on Microsoft's AI GitHub repository, including over 30,000 internal Microsoft Teams messages – all caused by one misconfigured SAS token



Hillai Ben-Sasson, Ronny Greenberg
September 18, 2023

10 minutes read





4. Can I detect a misuse in my AI pipelines?

Can I detect a misuse in my AI Pipelines?

Threat detection to respond to AI threats in real time



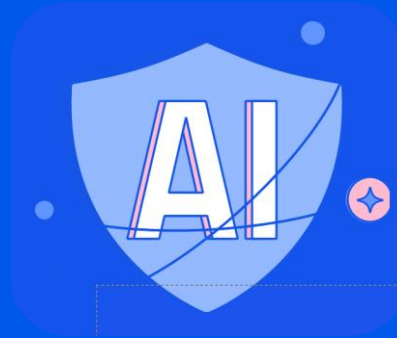
Real-time Threat detection

Anomaly Detection

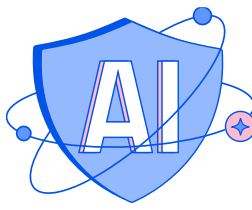
Detect Attack Paths

The image shows a security dashboard with three overlapping alert panels. The top panel, titled 'Malicious AI Model detected', shows a 'Detected events' list with an entry for 'Fileless execution was detected' on Nov 26th. The middle panel, titled 'Anomalous activity detected in AI Model execution engine', shows 'Raw Event Details' with Stdin and Stderr paths, and a 'Process Tree' showing a hierarchy of processes. The bottom panel, titled 'AI Model escape detected', shows a detailed description of a process reading user information files, along with a 'Subscription' section, 'Severity' (High), 'Type' (Threat Detection Issue), and 'Related Frameworks' (TA0001-T1078.001 Valid Accounts: Default Accounts). The dashboard also includes various action buttons like 'Comment', 'Run an Action', 'Create a Ticket', and 'Give Feedback', as well as status and due date dropdowns.

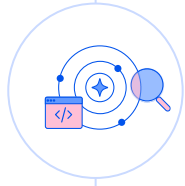
Introducing Wiz AI-SPM



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 easy-to-understand UI

Agentless visibility with AI-BOM

Detect every AI technology with AI-BOM

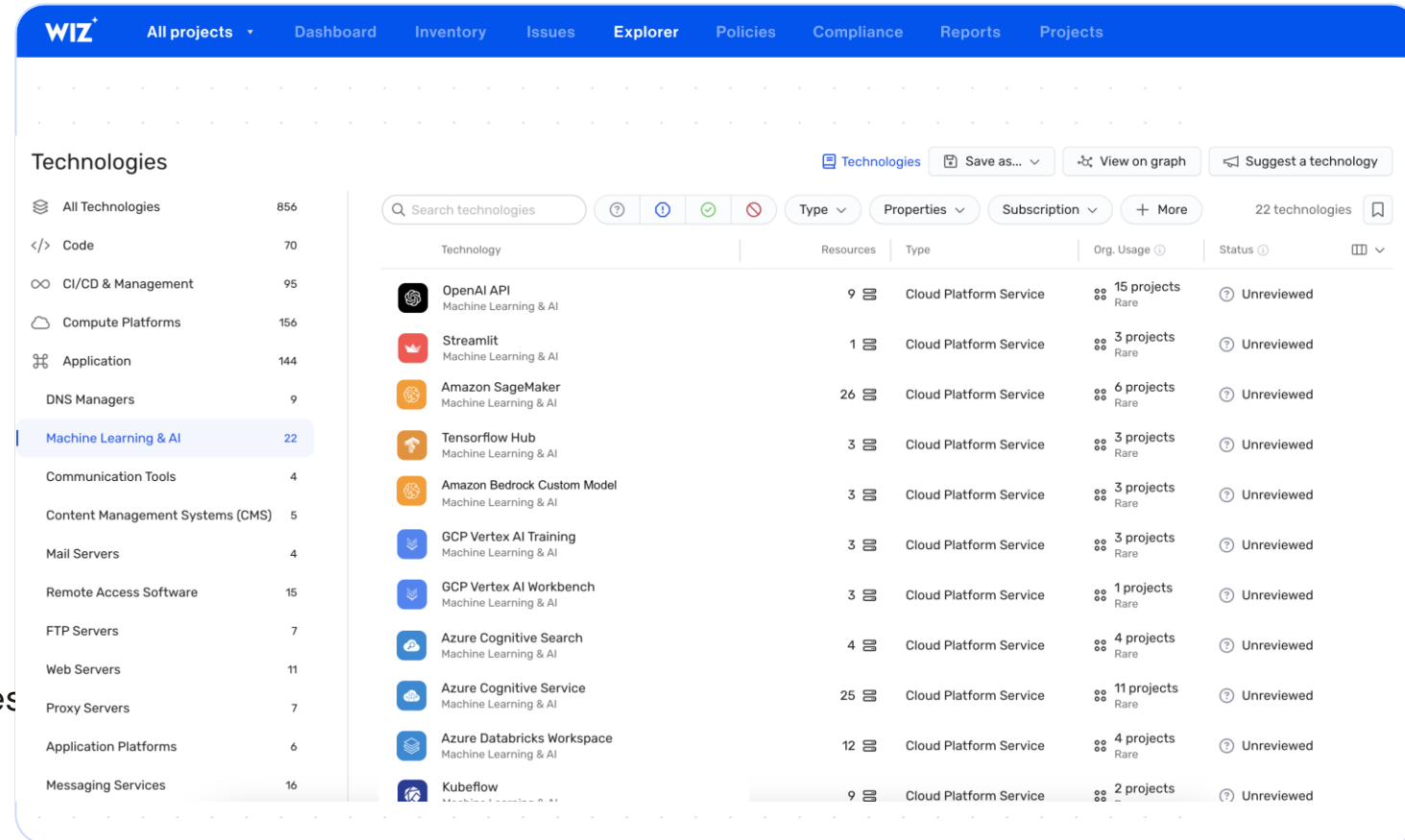
AI Services, SDKs, etc all without agents.

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 Technologies Explorer 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 search bar, filters for Type, Properties, and Subscription, and a 'Suggest a technology' button. A sidebar on the left lists various technology categories with their counts. The main table lists specific technologies, their resources, types, usage across projects, and their review status.

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



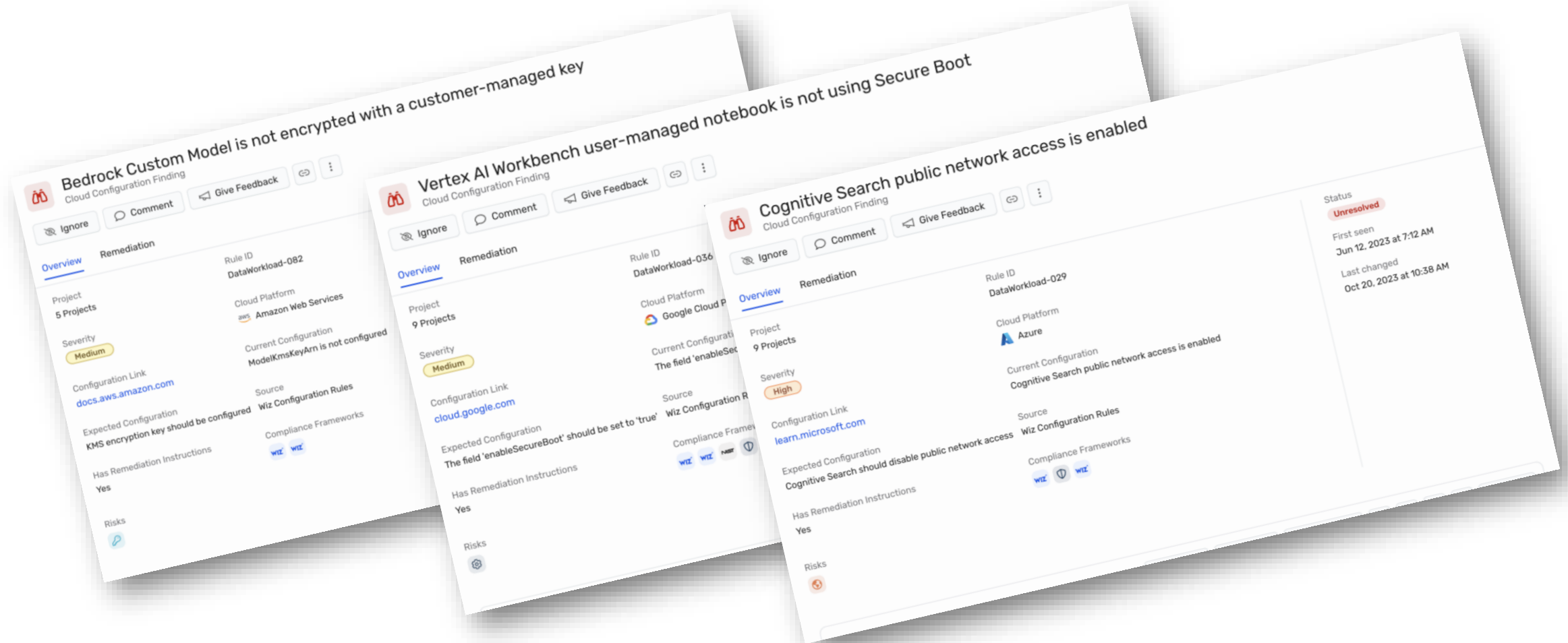
OpenAI



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

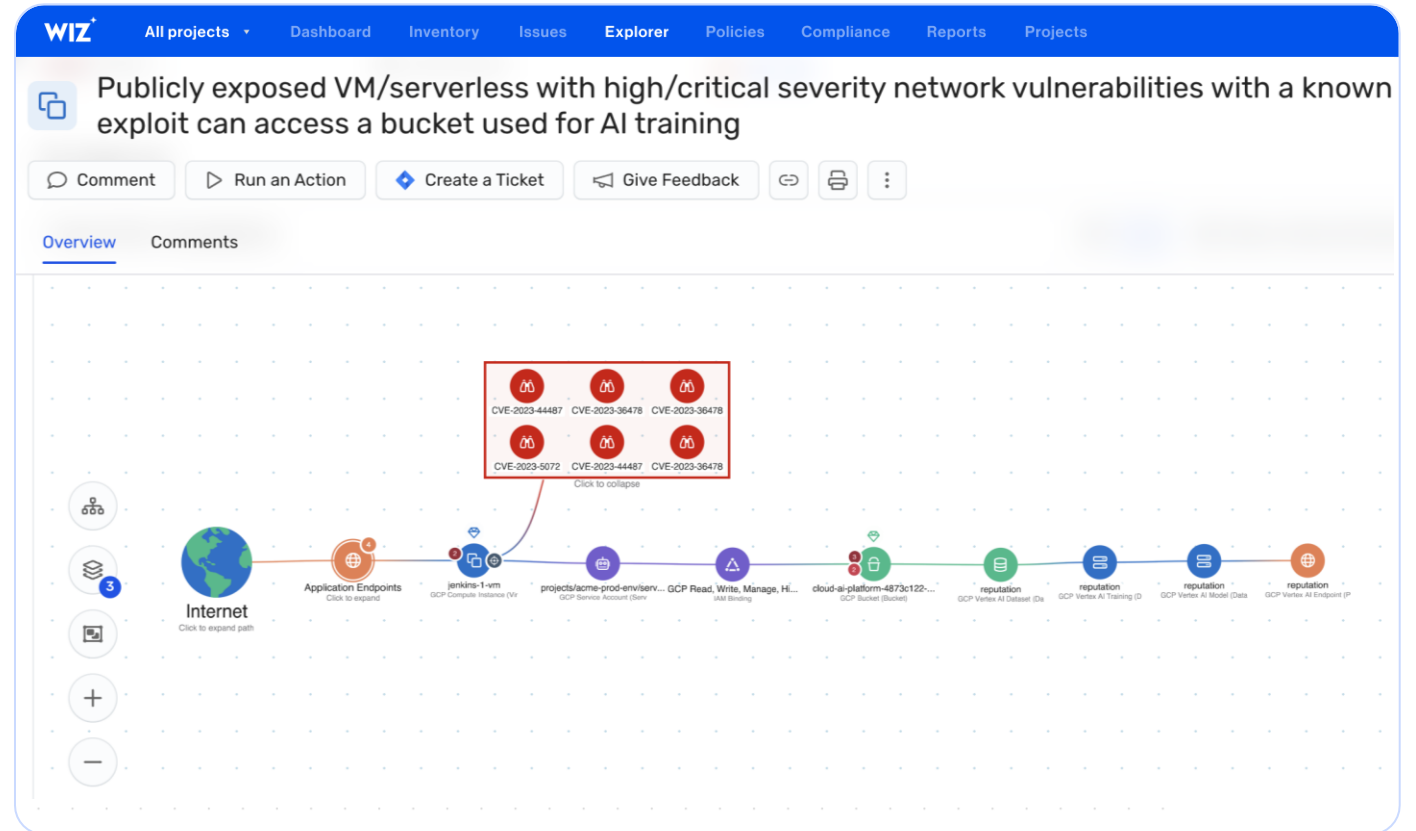
Detect AI vulnerabilities, misconfigurations, permissions, data, secrets, and network exposure

Protect sensitive training data

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

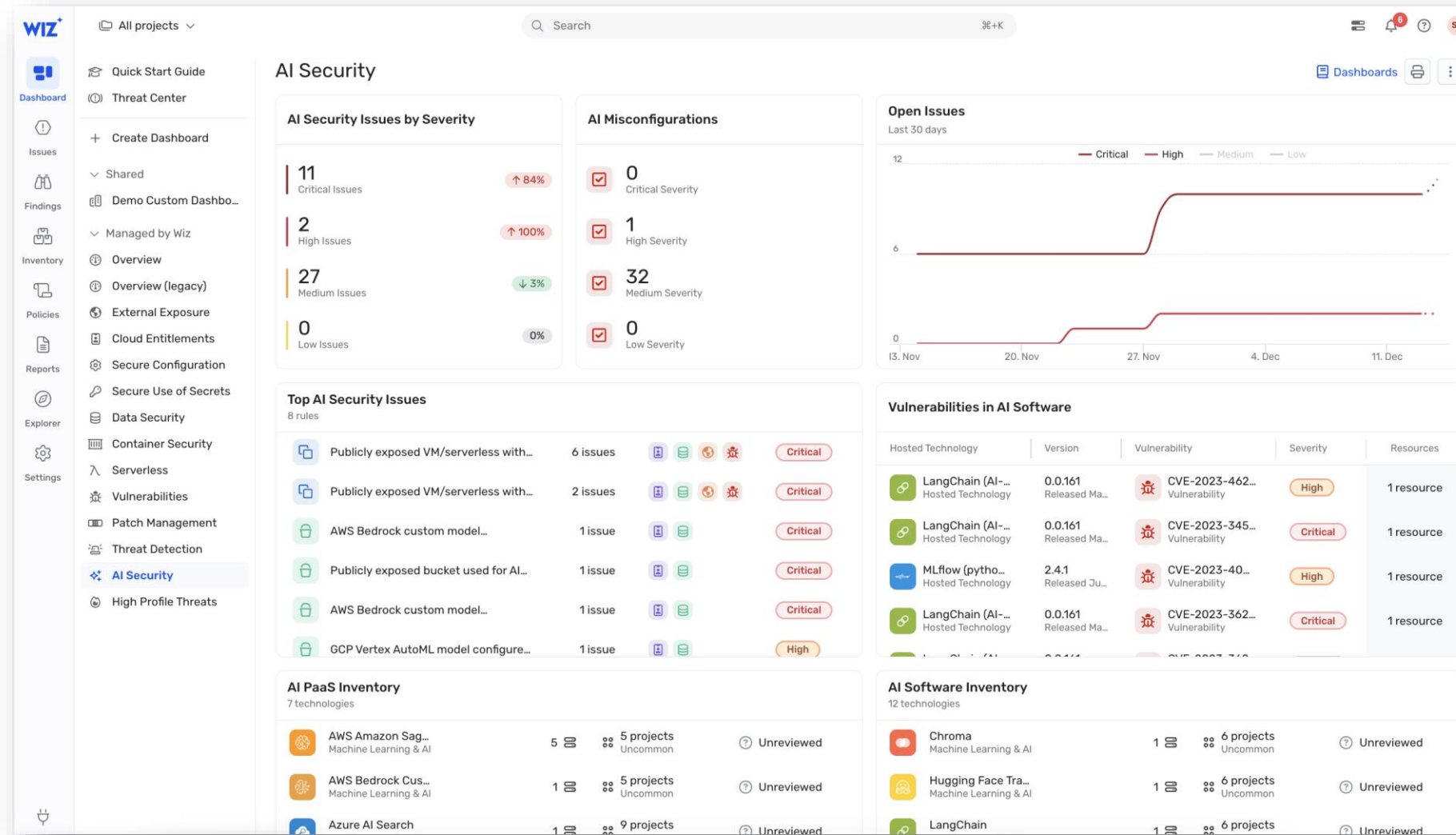
Remove critical attack paths to AI models

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 what AI services and technologies are running in my environment?
- ✓ Do I know what risks exist in my AI pipeline?
- ✓ Can I prioritize the critical risks across the AI pipeline?
- ✓ Can I detect a misuse in my AI pipelines?

One platform for the modern cloud security operating model



Wiz Platform

Wiz Code Secure Cloud Development

Secure every stage of your SDLC to gain visibility & prevent risks in code, pipeline, registries and images



Wiz Cloud Manage Security Posture

Agentless visibility & risk prioritization that proactively reduces the attack surface



Wiz Defend Respond to Cloud Threats

Cloud events and lightweight eBPF-based sensor to protect from unfolding threats as a last line of defense



Root cause analysis for risks and threats (Cloud to Code)

Build securely by design and detect drift (Code to Cloud)



THE LARGEST PRIVATE CYBERSECURITY COMPANY

\$1.9B raised

SEQUOIA

INSIGHT
PARTNERS

andreessen
horowitz

Index
Ventures

Lightspeed

THRIVE
CAPITAL

SECURING LARGE CLOUD ENVIRONMENTS

1 Billion

Resources protected

1 Trillion

Files scanned

THE LEADER IN CLOUD SECURITY

G2 Grid for Cloud-Native Application Protection Platforms (CNAPP)



More than 40% of the Fortune 100 secure their cloud with Wiz



Questions?





Want to see more magic about Wiz AI-SPM?

Follows us on LinkedIn



Book or see a demo

**Come say hello
at booth #10!**

Learn about Wiz AI-SPM

