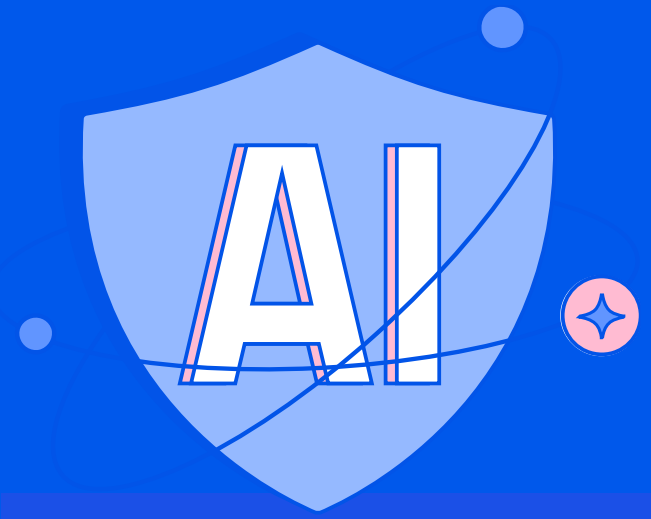
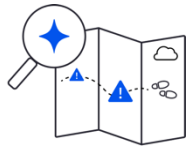
Balancing Innovation and Security: Navigating the AI Landscape



Cloud changed everything

New environment

How do I get visibility into my environment?



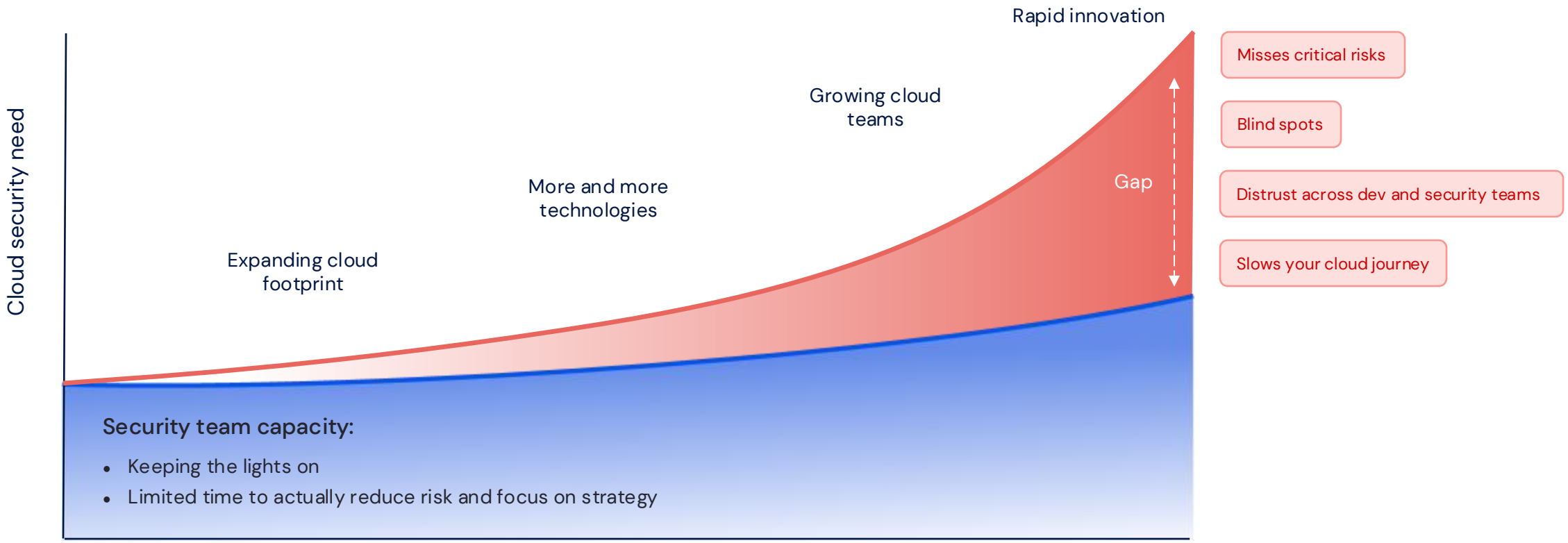
New risks

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

New ownership model

How do I ingrain security into our teams?

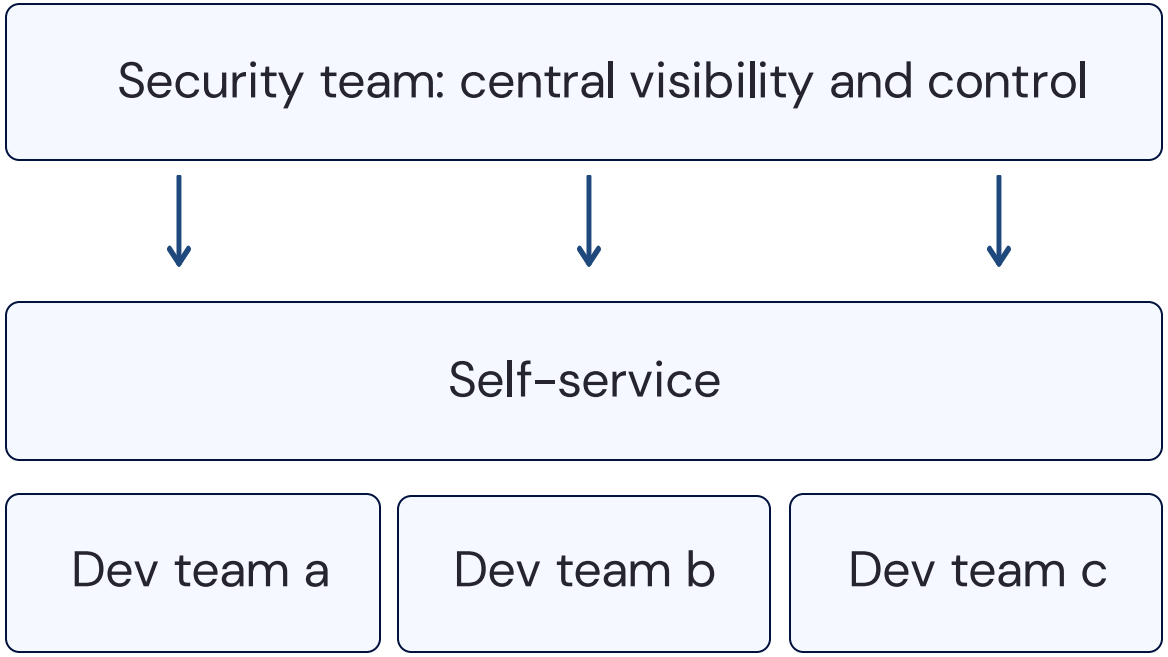
The time to scale your cloud security model is now



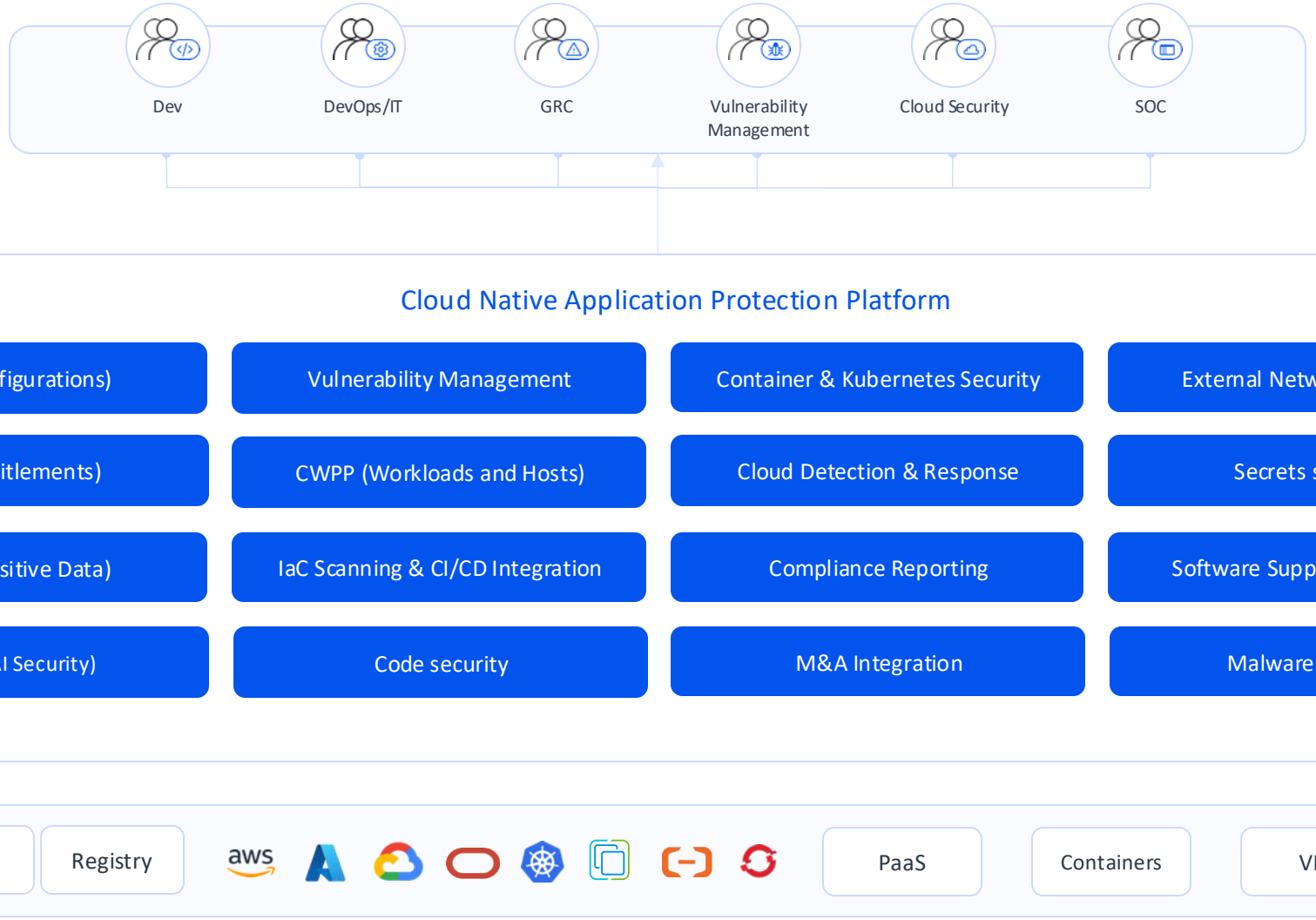
We can't keep doing the same thing

Cloud security needs a new operating model

Cloud security is a team sport



One unified platform for your cloud security journey



AI changes everything
again!

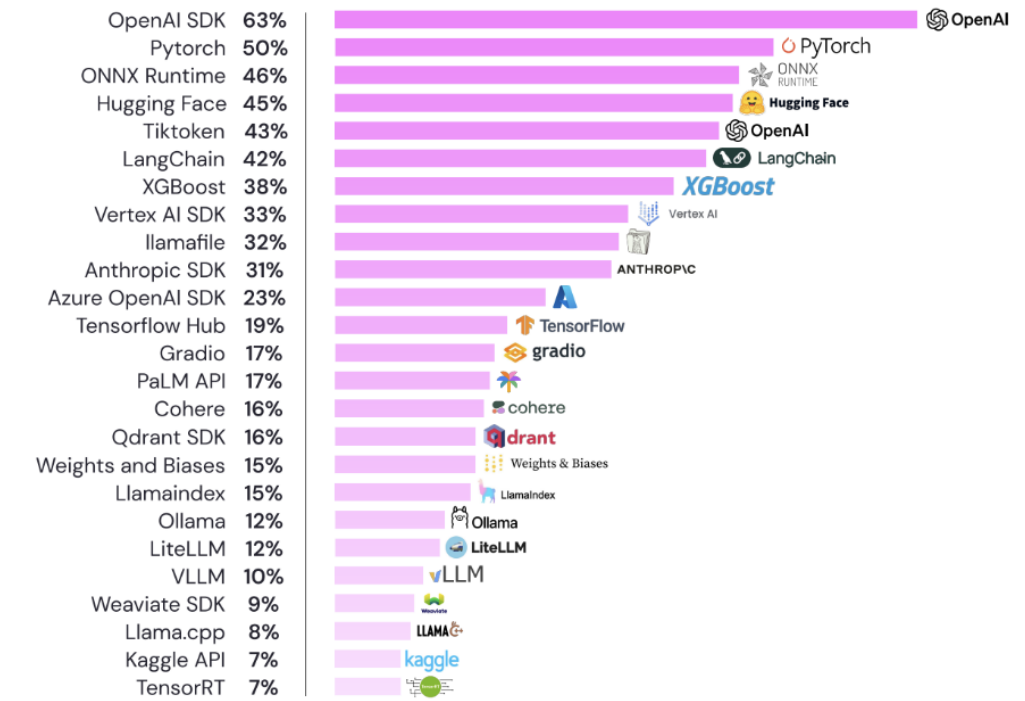
AI has taken over the cloud:

Cloud-based managed and self hosted AI can be found in over 85% of environments

Weaviate · LlamaIndex · TensorFlow · qdrant · LLAMA C++ · kaggle · XGBoost · OpenAI · ONNX RUNTIME · vLLM · cohere · Ollama · PyTorch · ANTHROP\C · Hugging Face · gradio · LiteLLM · LangChain · Vertex AI · W&B

85% of organizations are using some form of AI (either managed or self-hosted)

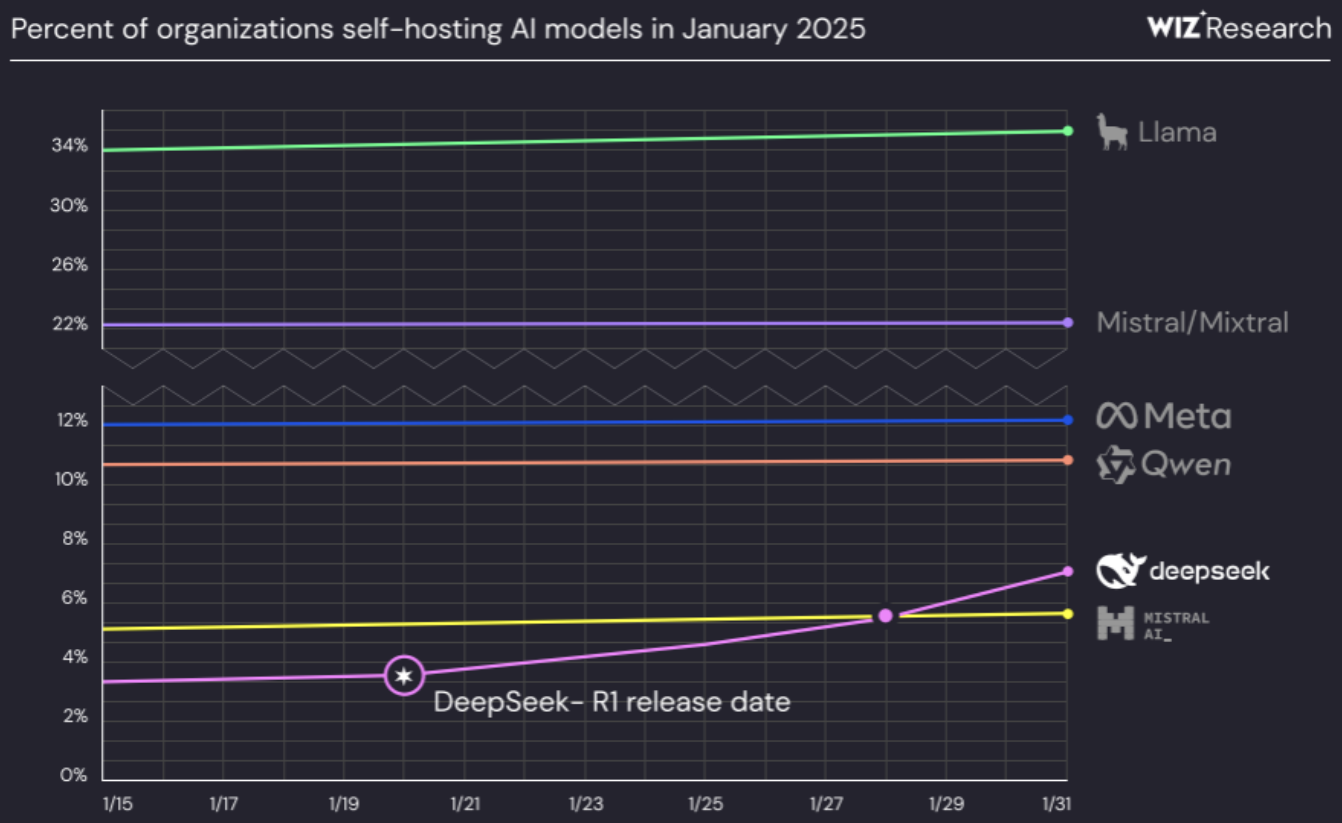
AI hosted technologies by percentage of organizations — WIZ Research



WIZ

Organizations quickly adopt new innovative technologies

DeepSeek rapid growth



Wiz Research on DeepSeek

AI applications face the same security risks

← Blog

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

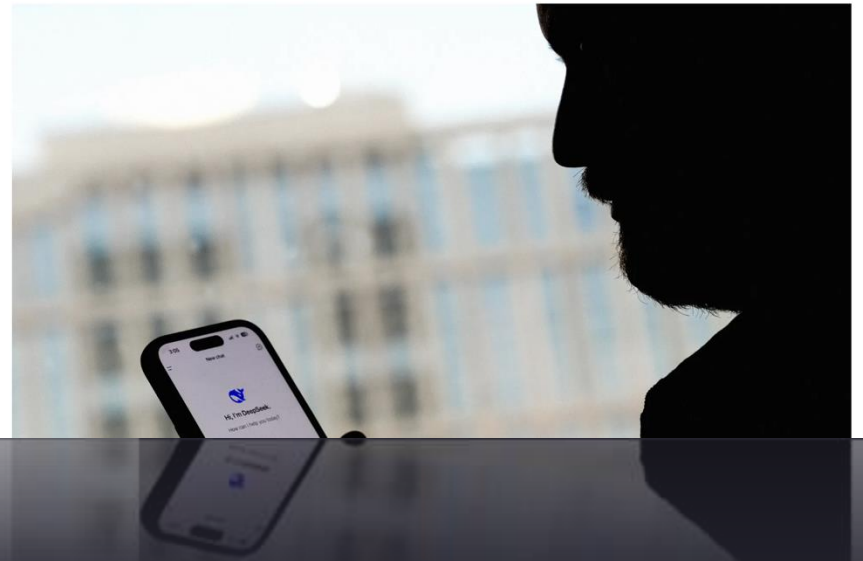
A publicly accessible database belonging to DeepSeek allowed full control over database operations, including the ability to access internal data. The exposure includes over a million lines of log streams with highly sensitive inform

Gal Nagli
January 29, 2025 3 minute read

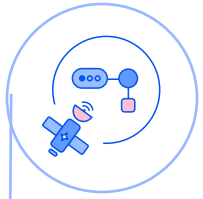
WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

Exposed DeepSeek Database Revealed Chat Prompts and Internal Data

China-based DeepSeek has exploded in popularity, drawing greater scrutiny. Case in point: Security researchers found more than 1 million records, including user data and API keys, in an open database.



Where are you on your AI journey?



Experimentation

- Sporadic use of AI tools
- Shadow AI
- Small POC projects with unvalidated tools

Active development

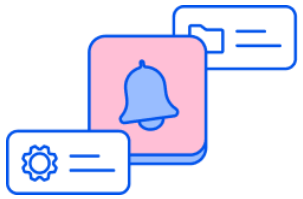
- Dedicated teams & projects
- Partial visibility
- Limited but dedicated AI deployments

Use in production

- Dedicated AI security
- Visibility into cost and tools
- Large AI deployments

No matter where you are on your AI journey,

AI adoption adds a new layer of complexity



New technologies

Where do I have AI in my environment? Do I have full visibility?

New risks

AI-specific risks, how do I detect and remove attack paths in AI pipelines?

New skills

Security teams are not AI experts, how do I upskill them?

AI is here to stay, how do I ensure security doesn't slow down innovation?

We learned from the cloud

Let's apply the learnings to AI

Visibility is the foundation

- Visibility into AI pipelines, models, technologies, toolsets, and data

Continuous risk detection

- Detect AI-specific risks and misconfigurations
- Find sensitive training data
- Identify malicious models
- Detect unintentional exposures and vulnerabilities

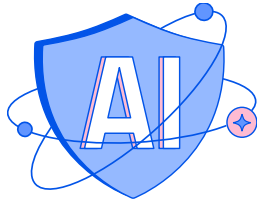
Prioritize critical risk with context

- Correlate AI risks to cloud, workload, and business context to find attack paths to models
- Prioritize the most critical risk on the Wiz Security Graph

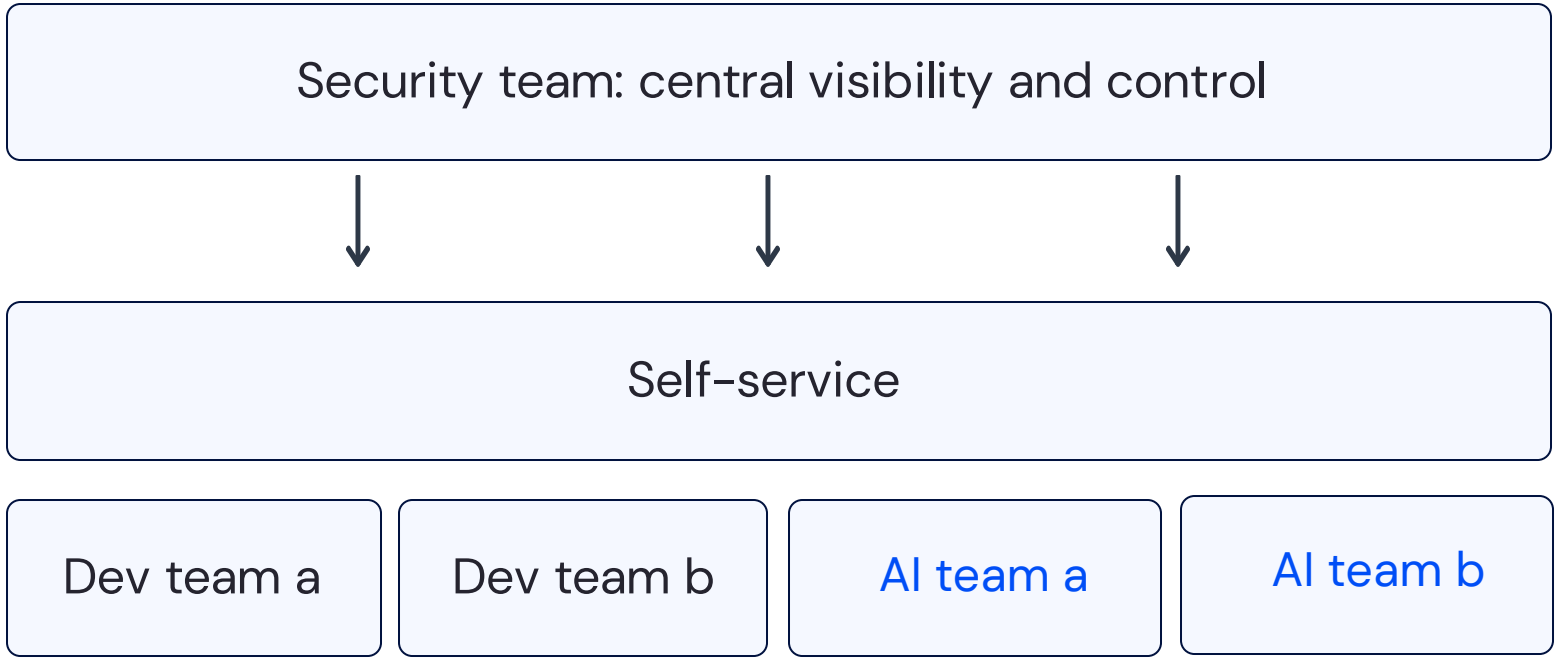
Detect threats as the last line of defense

- Identify suspicious behavior and misuse of AI models
- Respond quickly to threats

AI introduces new teams to the security operating model



Extend the cloud security operating model to AI

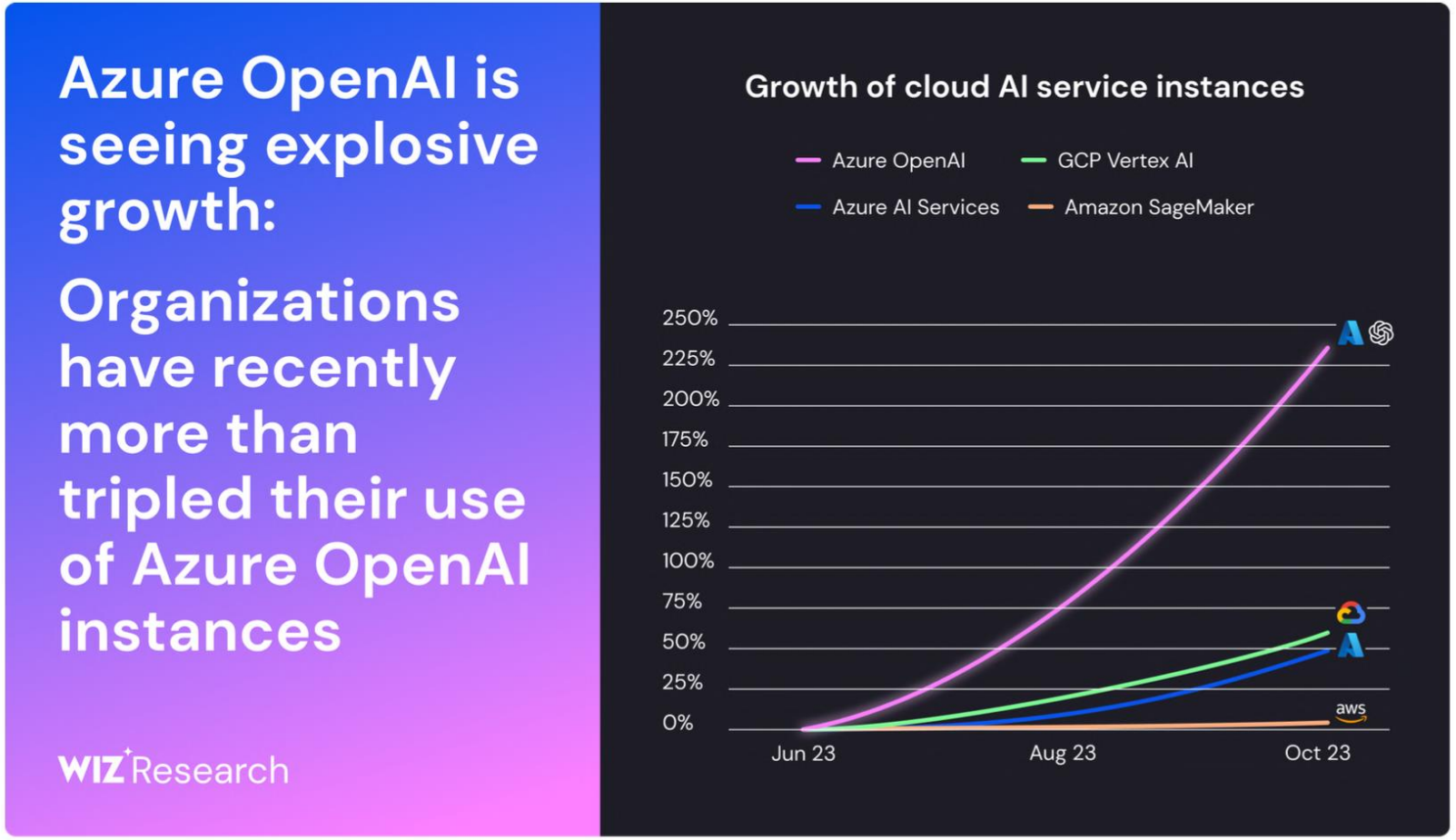


AI-SPM: The four questions security org need to ask

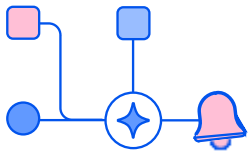
- ❑ Do I know what AI services and technologies are running in my environment?
- ❑ Do I know what risks exist in my AI pipeline?
- ❑ Can I prioritize the critical risks across the AI pipeline?
- ❑ Can I detect a misuse in my AI pipelines?

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

1. Massive adoption of AI services

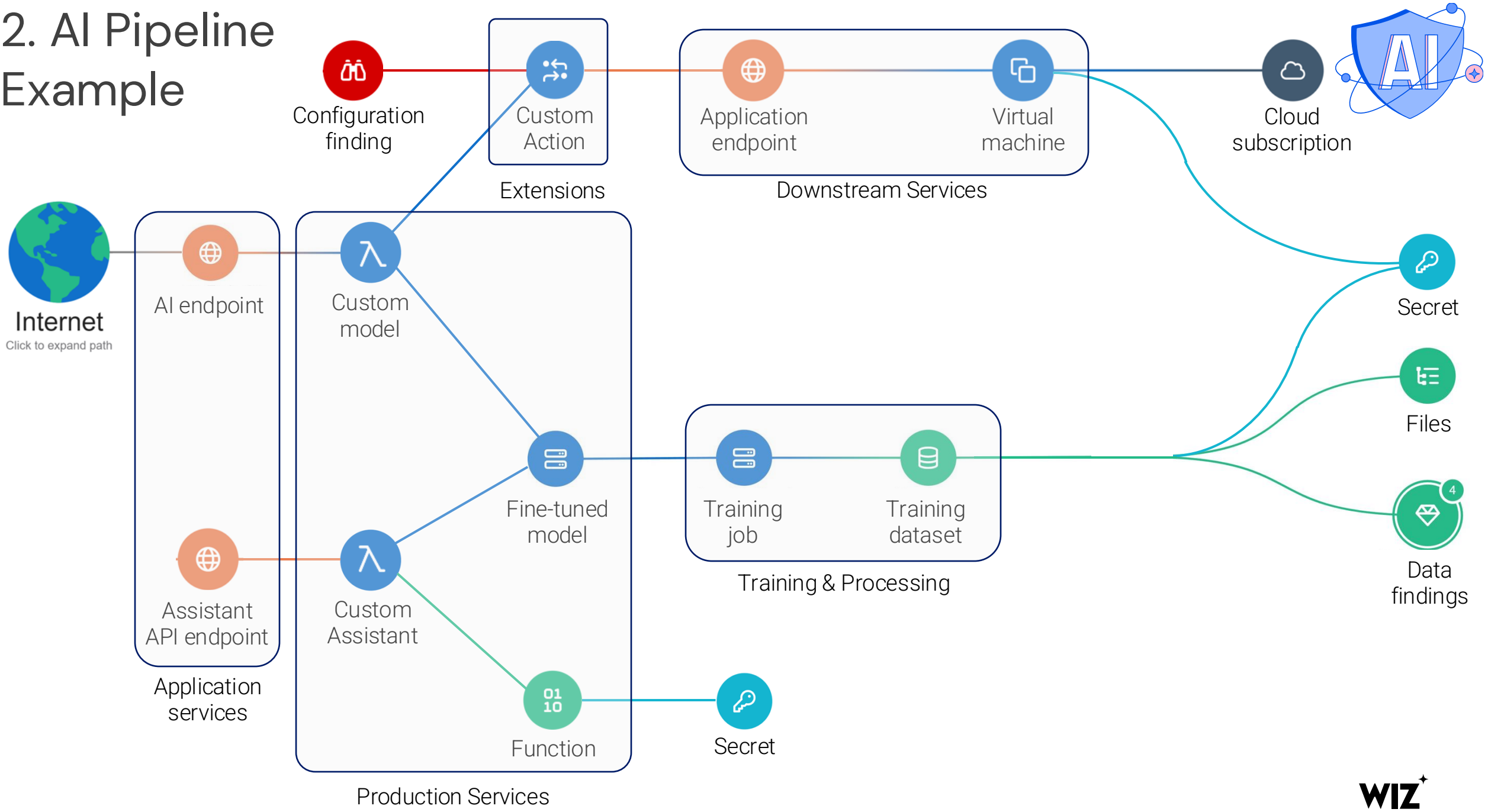


Source: [State of AI in the Cloud 2024]



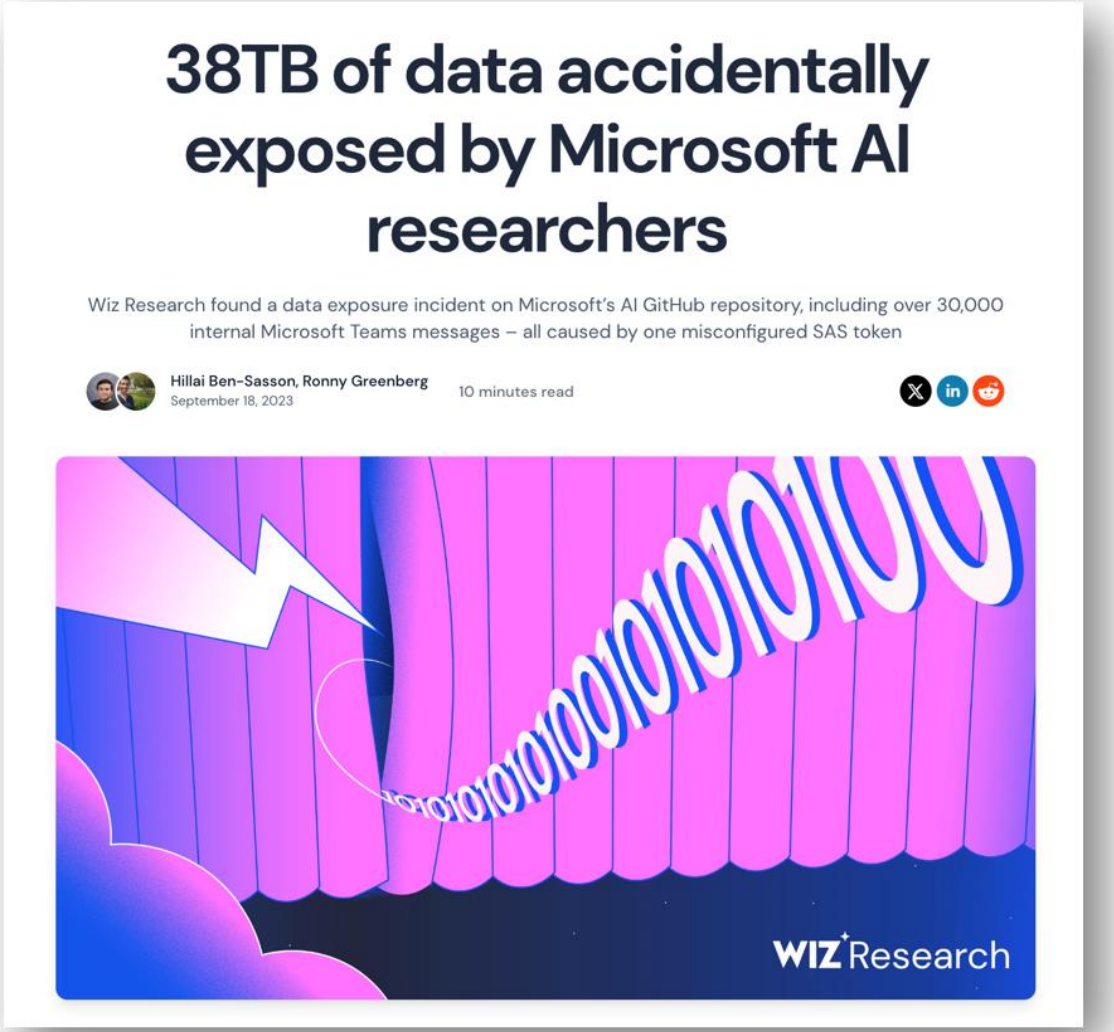
2. Do I know what risks exist in my AI pipeline?

2. AI Pipeline Example



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

3. Real-life example of an AI toxic combination

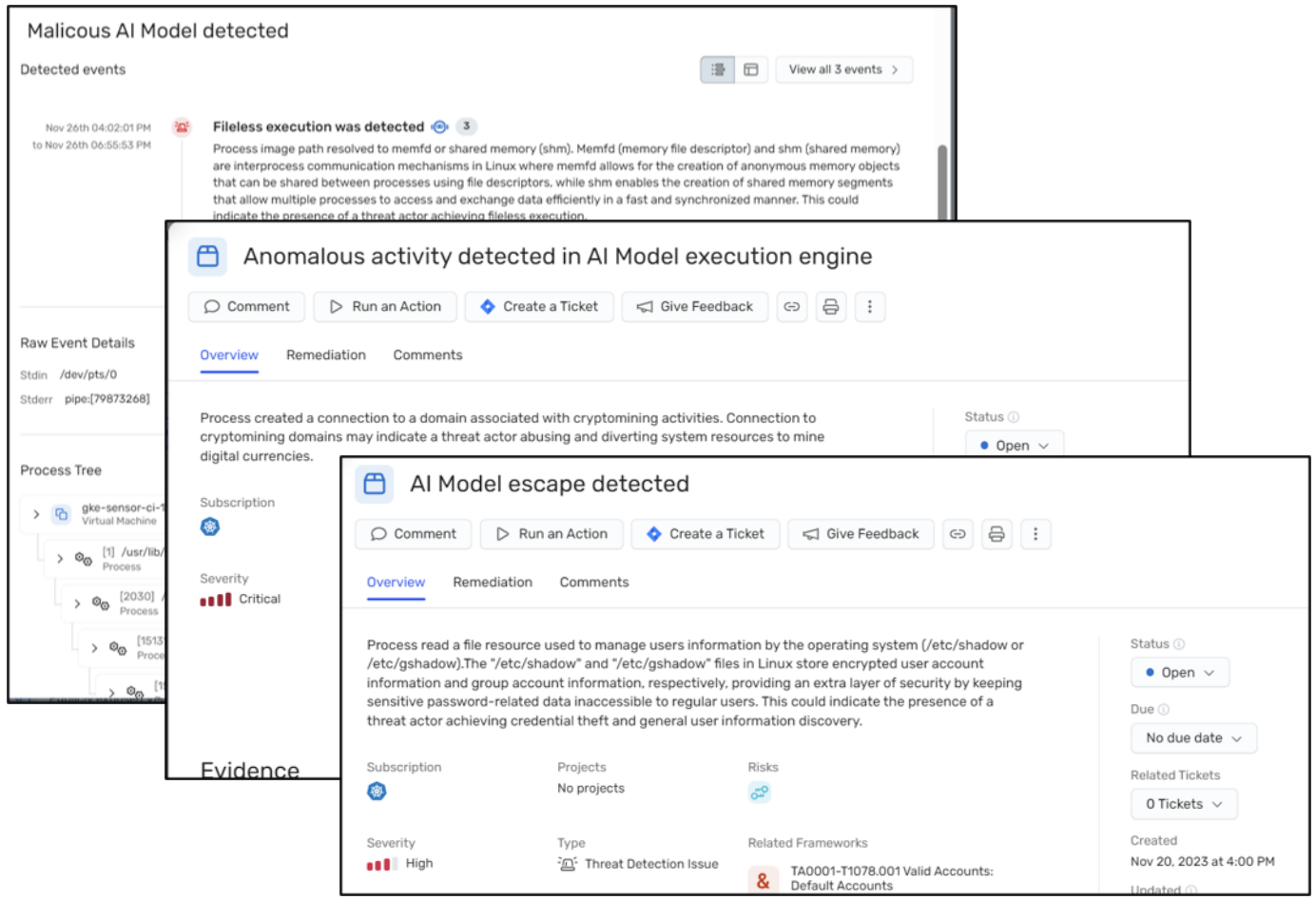


4. Can I detect a misuse in my AI pipelines?

4. 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



Introducing Wiz AI-SPM

Wiz becomes the first CNAPP to provide AI-SPM capabilities, helping organizations accelerate AI adoption securely

Wiz AI-SPM

Secure AI Framework

Infrastructure

Secure your Pipelines

- Secure AI Research and data lifecycle
- Secure AI platforms and services (CIEM, Network, encryption etc.)
- Input & Output Guardrails
- Model inference & Serving

Model

AI Models are IP

- Integrity
- Supply Chain
- Model Theft
- Malicious models
- Poisoning

Data

Secure your AI Data

- Data Sources
- Data Pipelines
- Training data
- Data integrity and bias

Application

AI is a modern App

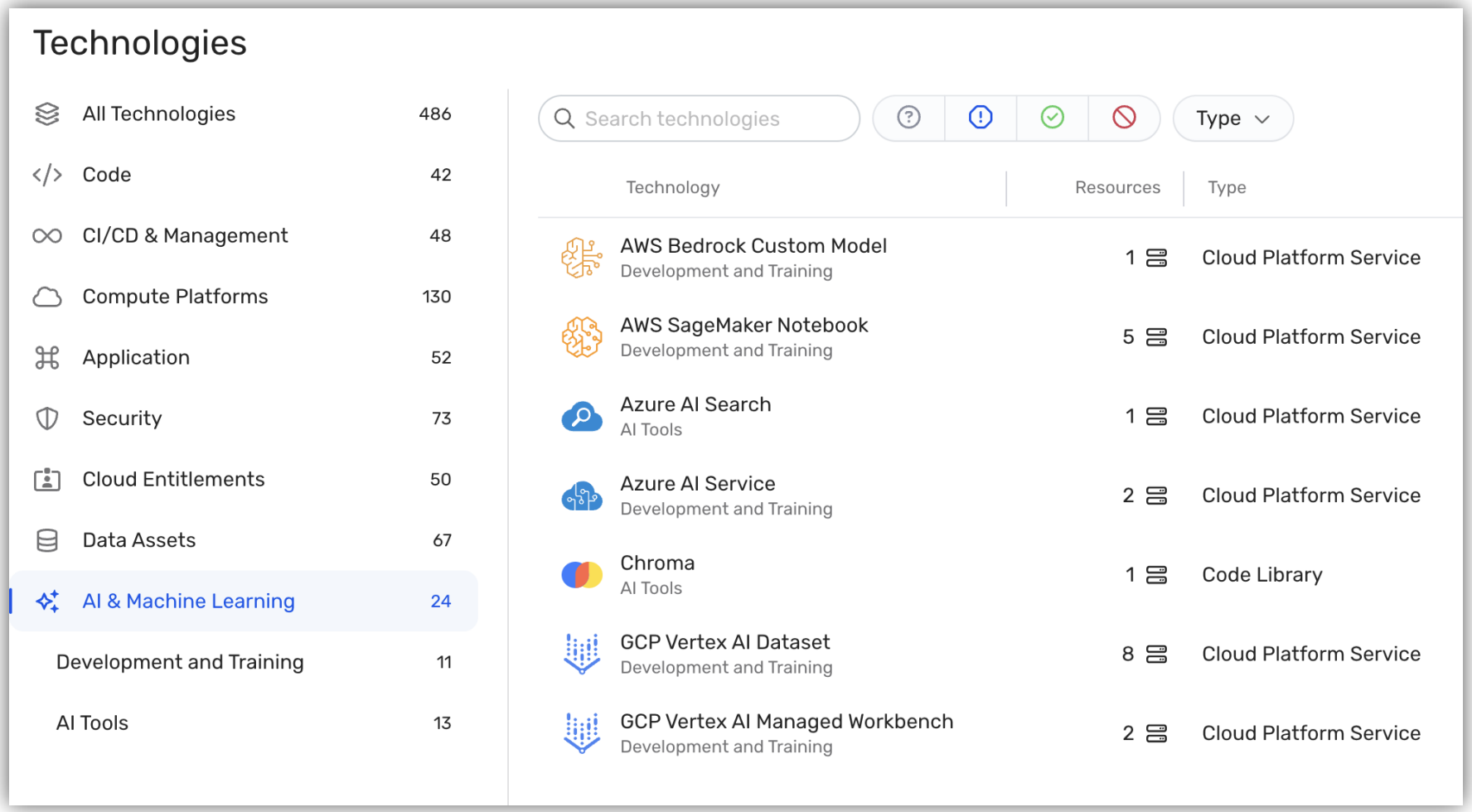
- AI & Model SBOM
- Exposure
- Plugins and Extensions
- Vulnerabilities
- Rate limiting and gating
- DoS

Agentless visibility with AI-BOM

Detect every AI tech. with AI-BOM
AI services, SDKs, etc. all without agents. Full visibility on the technology inventory (Sagemaker, VertexAI , Bedrock)

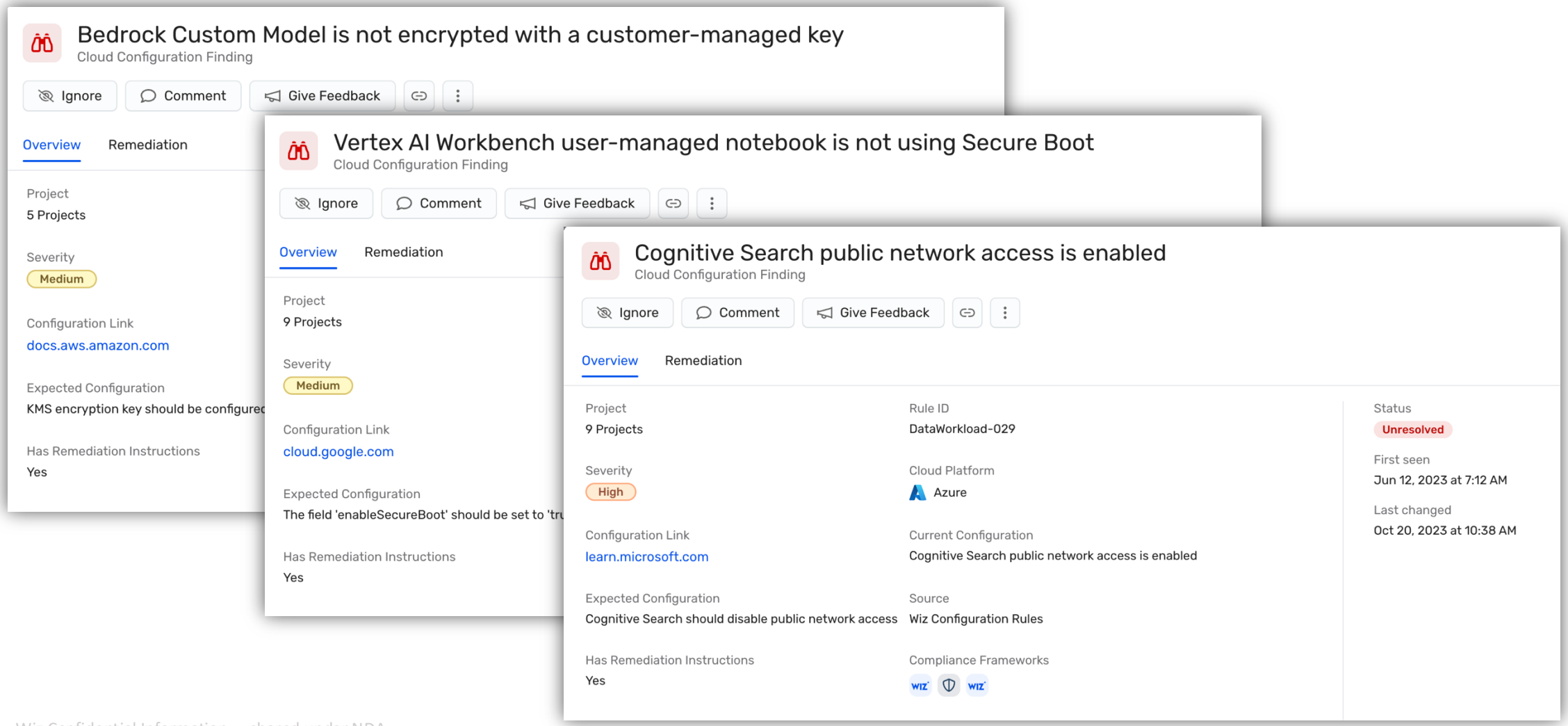
Remove shadow-AI
As soon as your developers start using a new AI service, the security team gains visibility

End-to-end AI pipeline visibility
Detect every resource in your AI pipelines, from the virtual machines hosting the machine learning job, to the data store used for training



AI Misconfigurations

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



Detect attack paths to AI

Deep risk analysis in AI pipelines

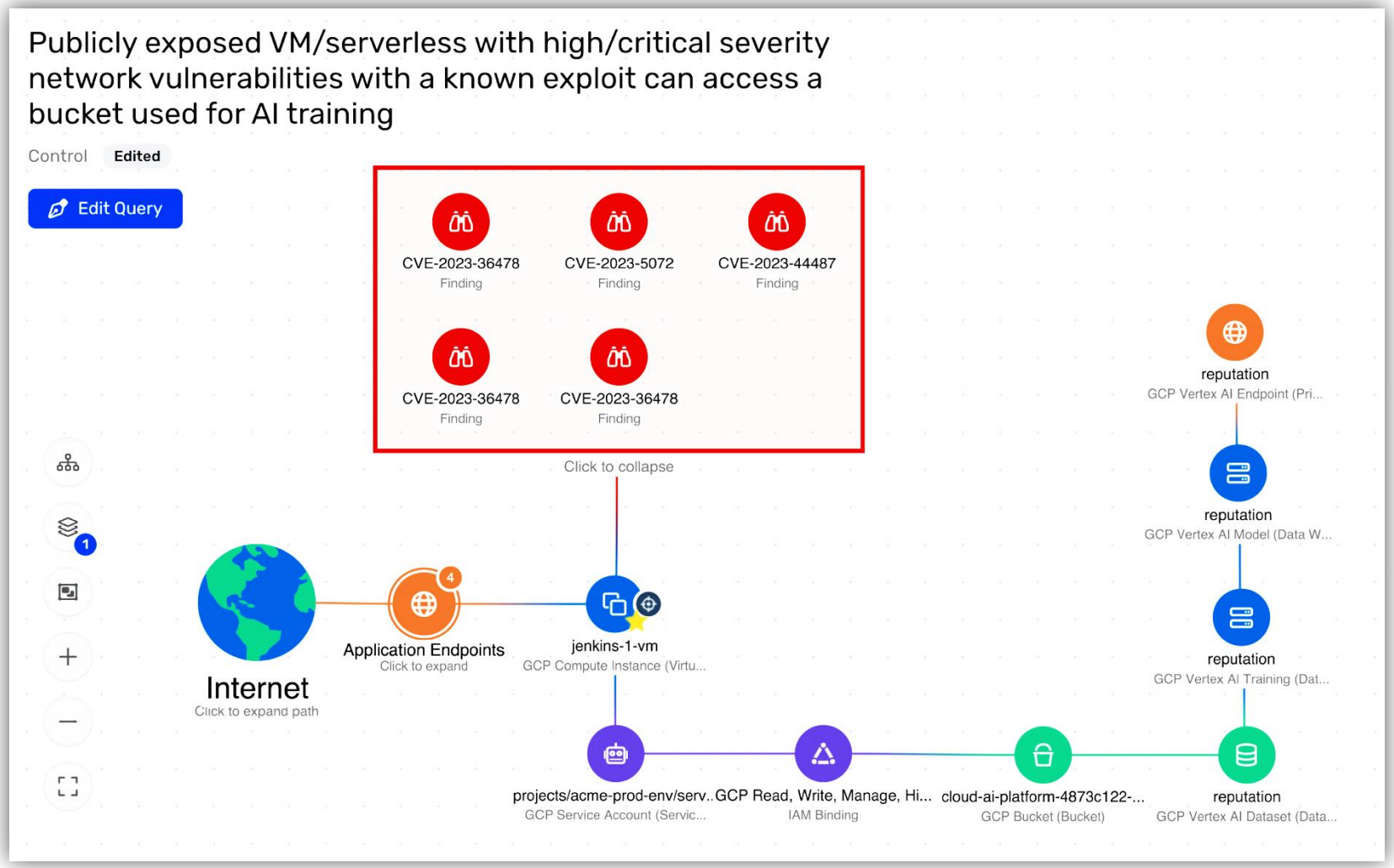
Risk analysis across AI vulnerabilities, misconfigurations, permissions, data, secrets, and network exposure

Protect sensitive training data

DSPM extended to AI to detect sensitive AI training data and protect against data risks such as data poisoning

Remove critical attack paths to AI models

Wiz identifies attack paths in your AI pipelines and allows you to proactively remove the most critical risks with context



Wiz AI-SPM

Remove AI threats in real-time with Wiz Defend

Real-time threat detection

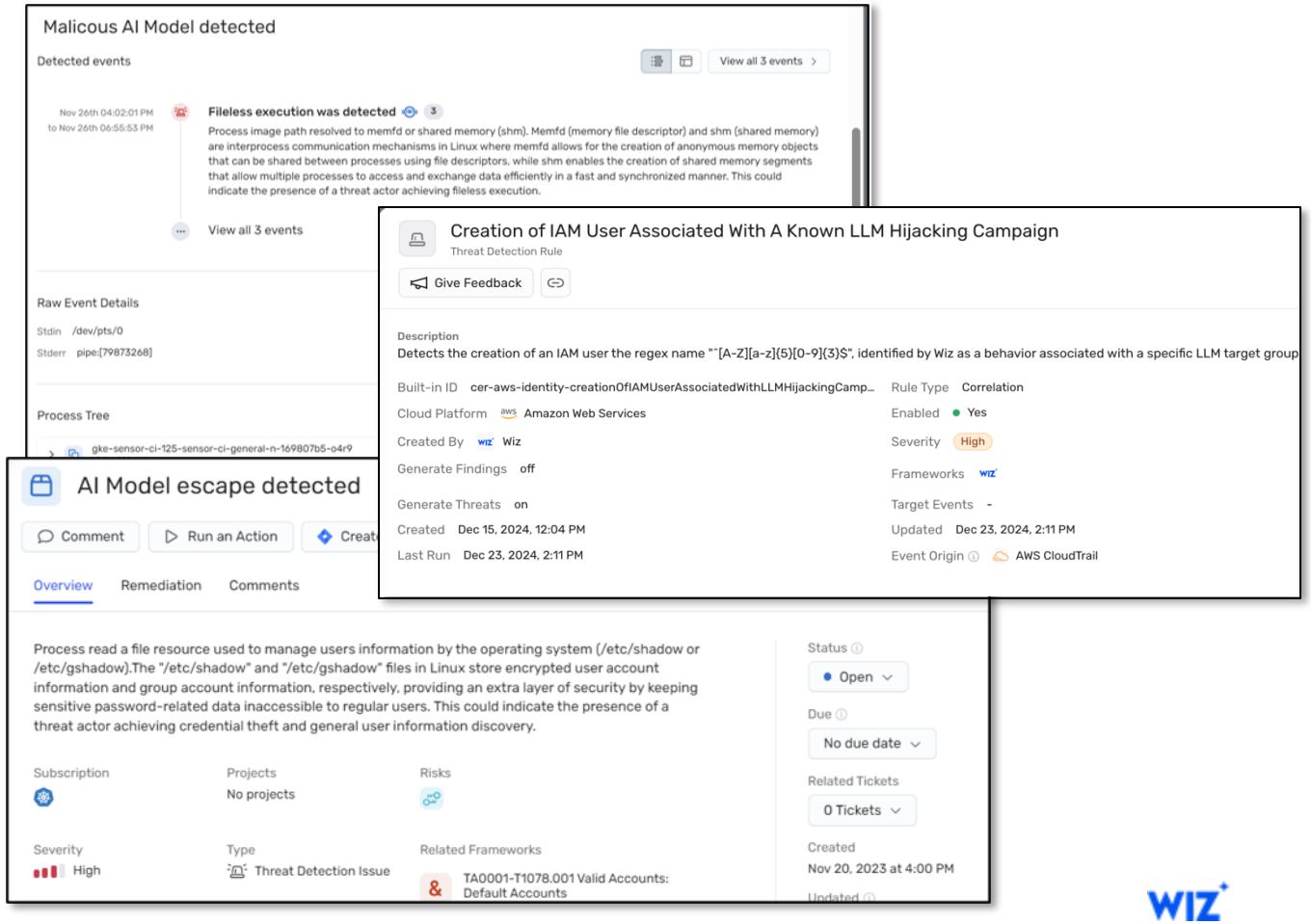
Built-in threat detection rules to detect suspicious activity and misuse of AI models

Detect common LLM attack techniques

The Wiz Research Team adds new rules based on emerging AI attack techniques found in cloud environments

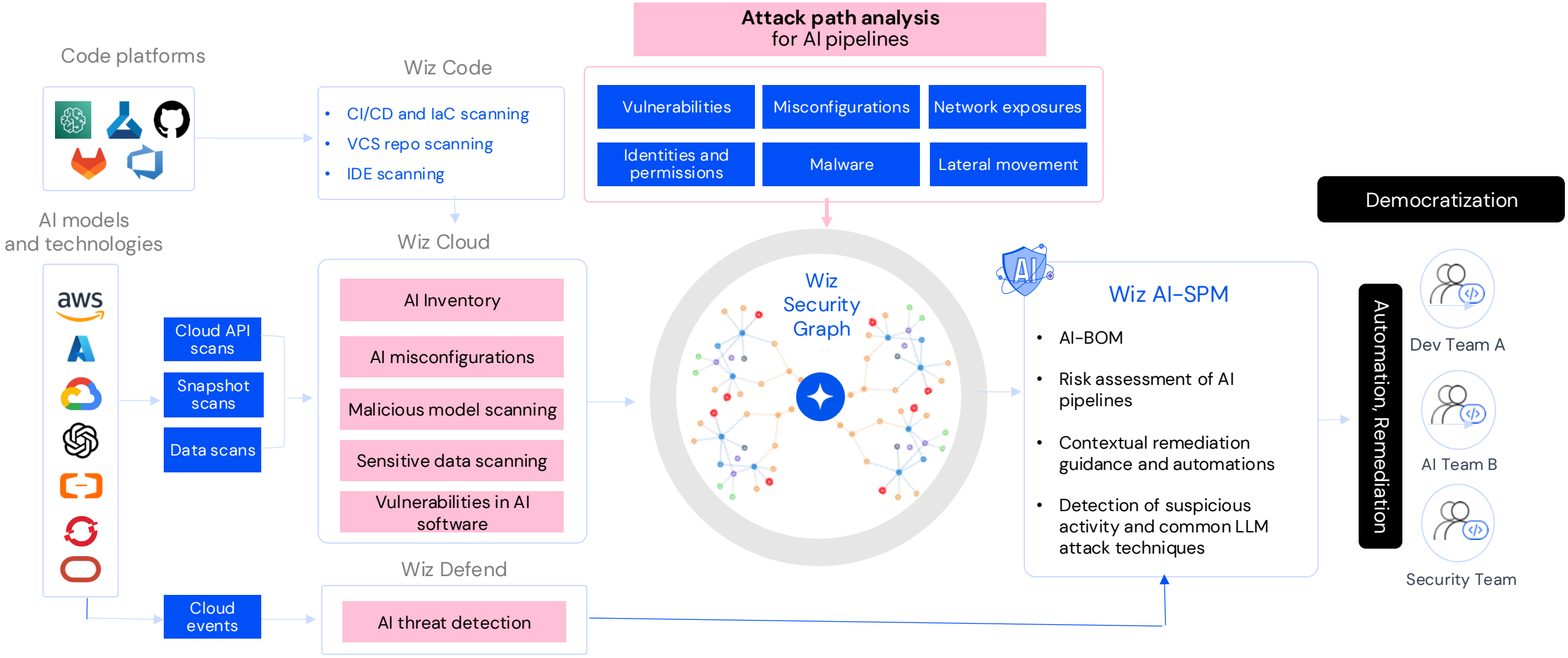
Reduce blast radius with cloud context

Threats are correlated to cloud context to understand how an attacker can move around the environment and reduce attack surface



Operationalizing Wiz AI-SPM

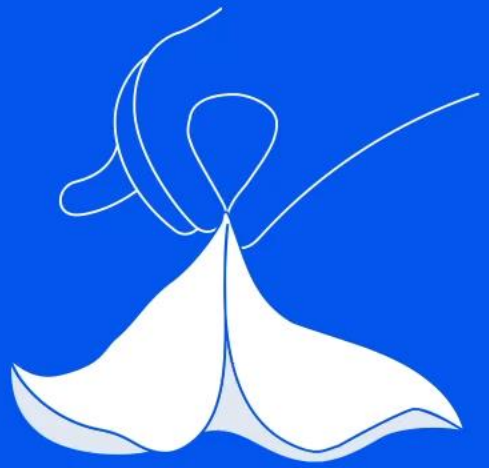
Wiz AI-SPM empowers organizations to increase AI innovation securely by providing visibility into AI technologies and models, risk assessment for AI pipelines, and threat detection.



> We use Wiz AI-SPM to accelerate the pace of AI application development and deployment, while enforcing AI security best practices. As a result, we can deploy AI applications that are secure by design and build trust with key stakeholders.

Rohit Kohli

Deputy Chief Information Officer, Genpact



Want to see more magic about Wiz AI-SPM?

Follows us on LinkedIn	Book or see a demo	Learn about Wiz AI-SPM
linkedin.com/company/wizsecurity	wiz.io/demo	wiz.io/solutions/ai-security-posture-management