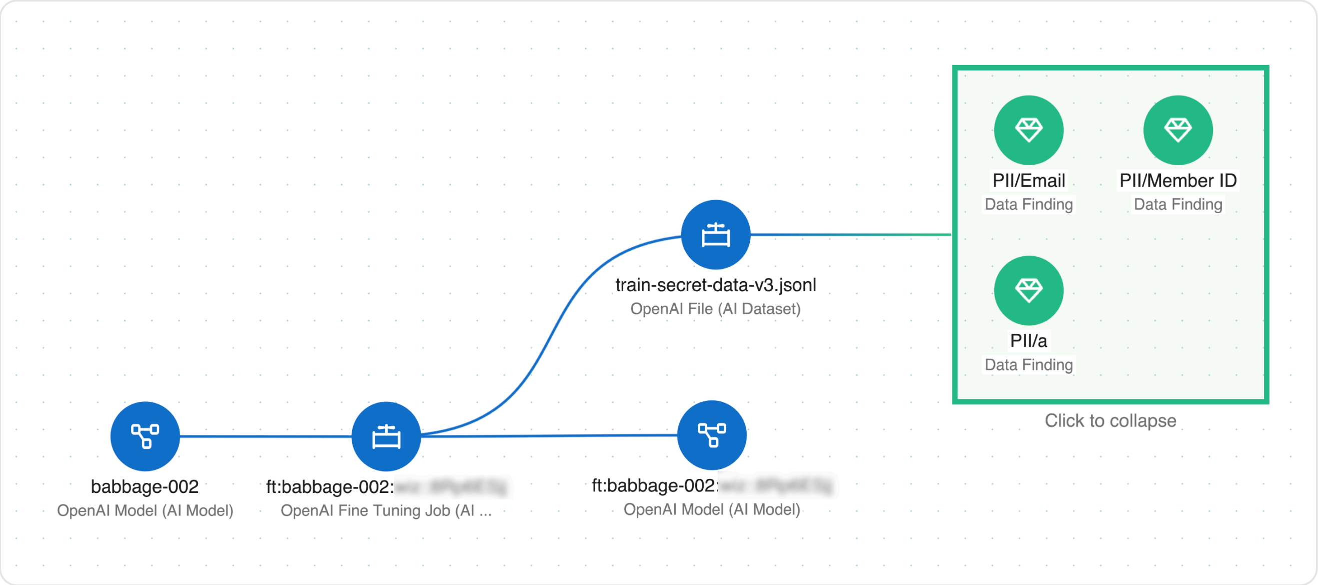
Securing AI

Wiz provides a variety of AI security posture management (AI-SPM) features to help you monitor and protect cloud environments that use artificial intelligence (AI) services and applications. This is totally different from how Wiz uses AI in its own product and docs. Learn about Ask AI and Doc AI.



Setting up a dedicated OpenAI Connector and/or adding permissions for Azure OpenAI allows Wiz to detect AI models, fine tuning jobs, and training datasets in use throughout your cloud estate. Enabling data security for AI allows Wiz to scan datasets for potentially sensitive data and exposed secrets.

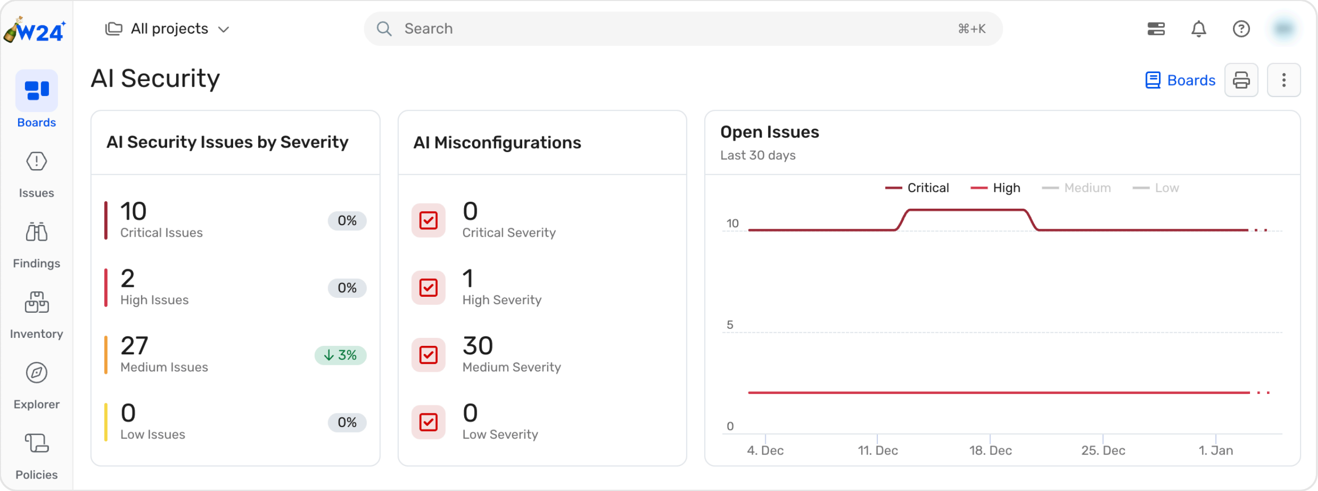
OpenAI vs. Azure OpenAI

Wiz supports both OpenAI and Azure OpenAI for all AI use cases, but there are some key differences in how they are supported:

- OpenAI is scanned via a dedicated Connector
- Azure OpenAI is scanned via a standard Azure cloud Connector. If you defined your Azure cloud Connector before December 2023, you may need to update Azure permissions to add the Cognitive Service OpenAI User built-in role.

> Depending on how Wiz is deployed, OpenAI datasets may be analyzed for potentially sensitive data in the Wiz backend, which may not be in the same region as your OpenAI instances. Learn more.

AI use cases



All projects

AI Security

AI Security Issues by Severity

10	Critical Issues	0%
2	High Issues	0%
27	Medium Issues	↓ 3%
0	Low Issues	0%

AI Misconfigurations

0	Critical Severity
1	High Severity
30	Medium Severity
0	Low Severity

Open Issues

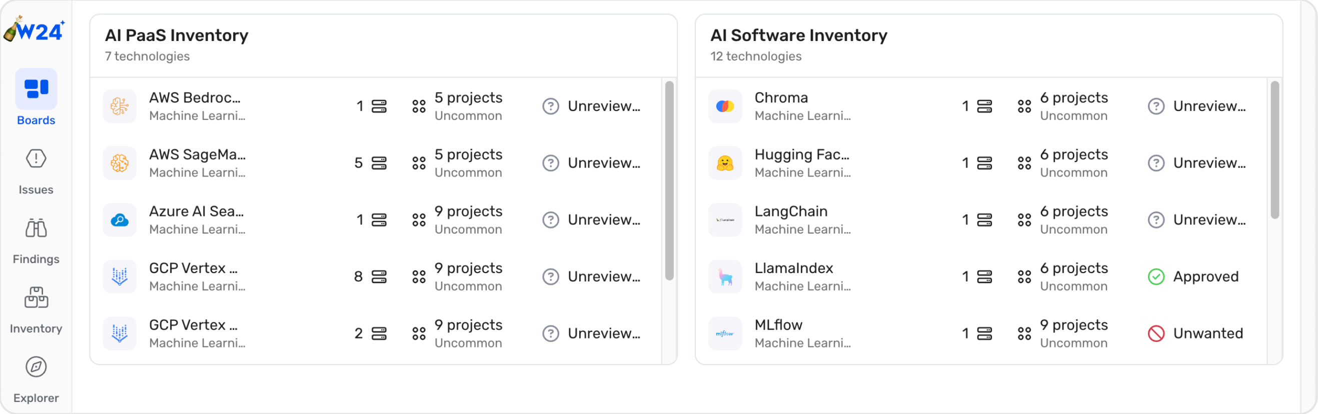
Last 30 days

The AI Security board is a great starting point to explore AI security use cases:

- Visibility into AI usage
- AI security posture management
- Analyze AI models for malicious code
- Data security for AI
- Attack path analysis for AI

Visibility into AI usage

By combining cloud scanning and workload scanning, Wiz builds a full-stack inventory of AI technologies, aka AI bill of materials (AI-BOM).



AI PaaS Inventory

7 technologies

AWS Bedroc... Machine Learni...	1	5 projects Uncommon	Unreview...
AWS SageMa... Machine Learni...	5	5 projects Uncommon	Unreview...
Azure AI Sea... Machine Learni...	1	9 projects Uncommon	Unreview...
GCP Vertex ... Machine Learni...	8	9 projects Uncommon	Unreview...
GCP Vertex ... Machine Learni...	2	9 projects Uncommon	Unreview...

AI Software Inventory

12 technologies

Chroma Machine Learni...	1	6 projects Uncommon	Unreview...
Hugging Fac... Machine Learni...	1	6 projects Uncommon	Unreview...
LangChain Machine Learni...	1	6 projects Uncommon	Unreview...
LlamaIndex Machine Learni...	1	6 projects Uncommon	Approved
MLflow Machine Learni...	1	9 projects Uncommon	Unwanted

- The AI PaaS Inventory widget lists AI services that are detected via cloud (direct link)

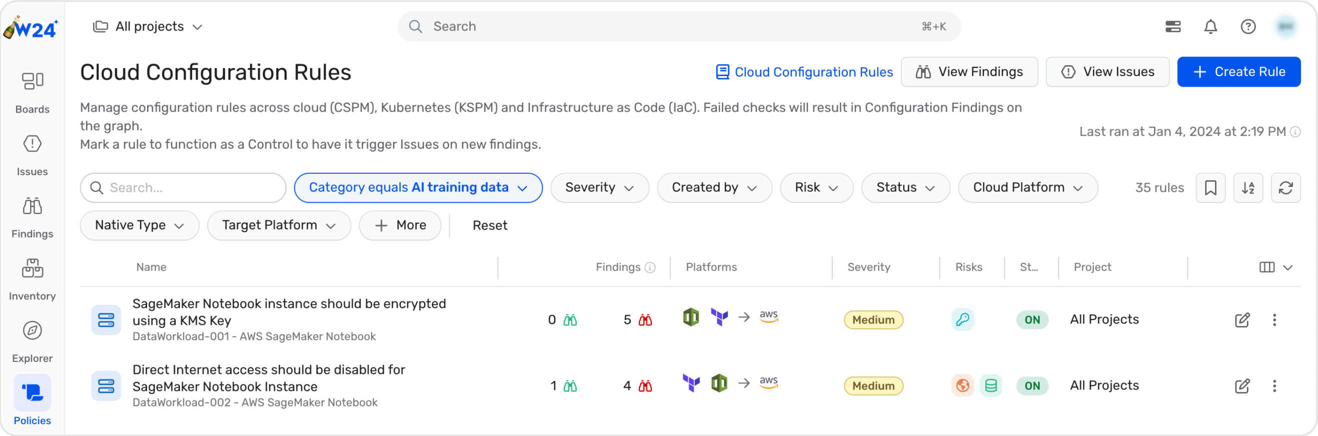
English ▲

- The AI Software Inventory widget lists libraries related to AI installed on workloads, such as AI Azure OpenAI SDK and Vertex AI SDK, which are detected via workload scanning (direct link)

Both widgets link to the full Inventory > Technologies page, where you can explore what has been detected, and where. Learn about the Inventory.

AI security posture management

Wiz identifies misconfigurations in supported PaaS AI services and applications via Cloud Configuration Rules that target supported AI technologies such as SageMaker Domain and Vertex AI.



Cloud Configuration Rules

Manage configuration rules across cloud (CSPM), Kubernetes (KSPM) and Infrastructure as Code (IaC). Failed checks will result in Configuration Findings on the graph.
Mark a rule to function as a Control to have it trigger Issues on new findings.

Last ran at Jan 4, 2024 at 2:19 PM

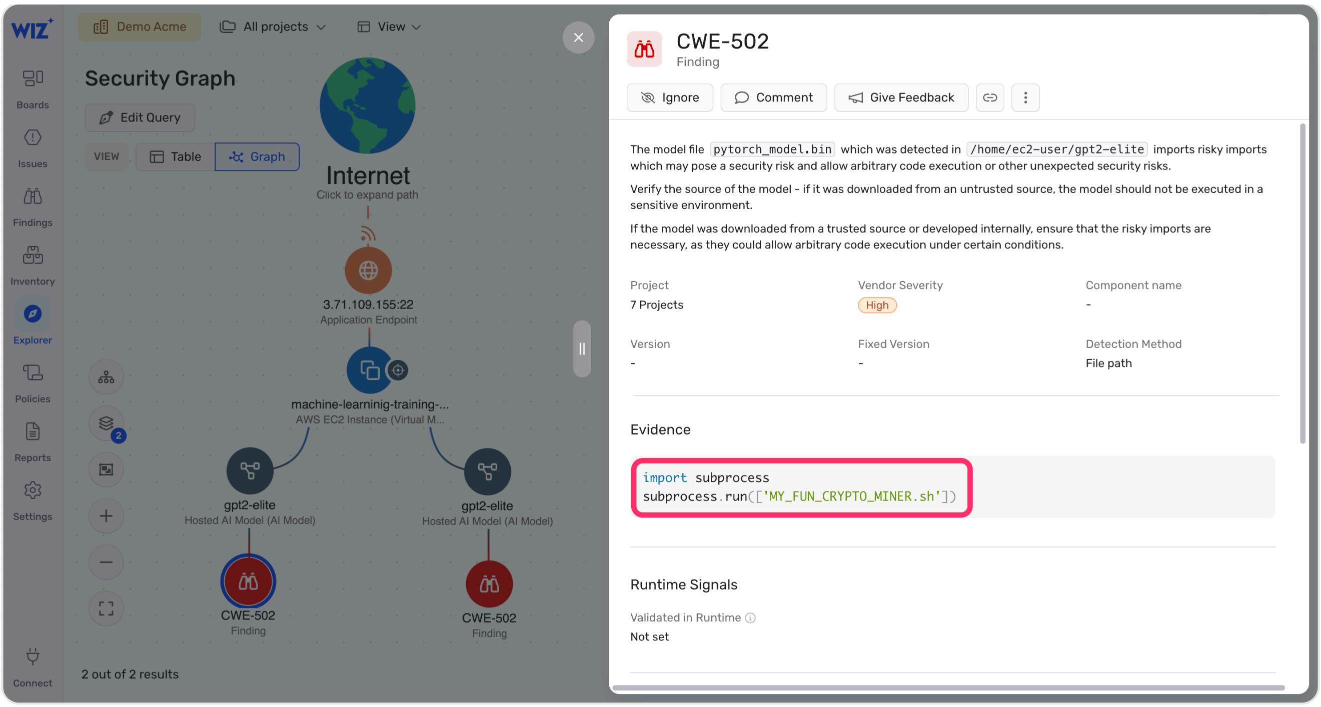
Name	Findings		Platforms	Severity	Risks	St...	Project
SageMaker Notebook instance should be encrypted using a KMS Key DataWorkload-001 - AWS SageMaker Notebook	0	5	→ aws	Medium		ON	All Projects
Direct Internet access should be disabled for SageMaker Notebook Instance DataWorkload-002 - AWS SageMaker Notebook	1	4	→ aws	Medium		ON	All Projects

When a misconfiguration is detected, a Cloud Configuration Finding connected to the relevant technology is added to the Security Graph.

Analyze AI models for malicious code

Wiz scans AI models (PyTorch, Keras, etc.) for potentially malicious code in the model data that could allow attackers to run arbitrary code your workloads.

English ▲



CWE-502
Finding

The model file `pytorch_model.bin` which was detected in `/home/ec2-user/gpt2-elite` imports risky imports which may pose a security risk and allow arbitrary code execution or other unexpected security risks.

Verify the source of the model - if it was downloaded from an untrusted source, the model should not be executed in a sensitive environment.

If the model was downloaded from a trusted source or developed internally, ensure that the risky imports are necessary, as they could allow arbitrary code execution under certain conditions.

Project	Vendor Severity	Component name
7 Projects	High	-
Version	**Fixed Version**	**Detection Method**
-	-	File path

Evidence

```
import subprocess
subprocess.run(['MY_FUN_CRYPTO_MINER.sh'])
```

Runtime Signals

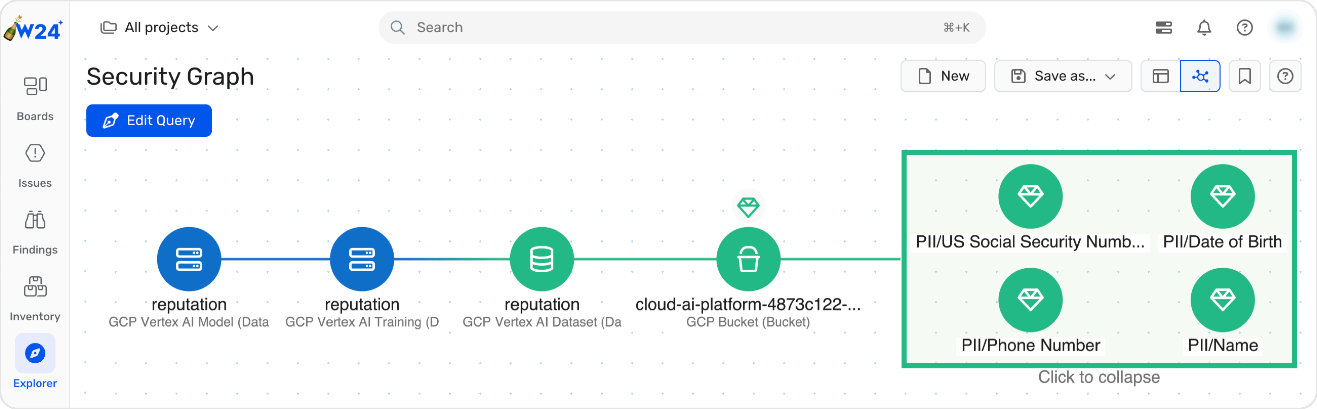
Validated in Runtime ⓘ
Not set

Data security for AI

This feature requires either a Wiz Standard or a Wiz Advanced license. Learn more.

Data security for AI services must be separately enabled on the Settings > Scanners > Data Security page.

Potentially sensitive data such as training data used by AI services and applications can be detected by Data Classification Rules. For example, you can search for all buckets used by AI services that contain sensitive data:



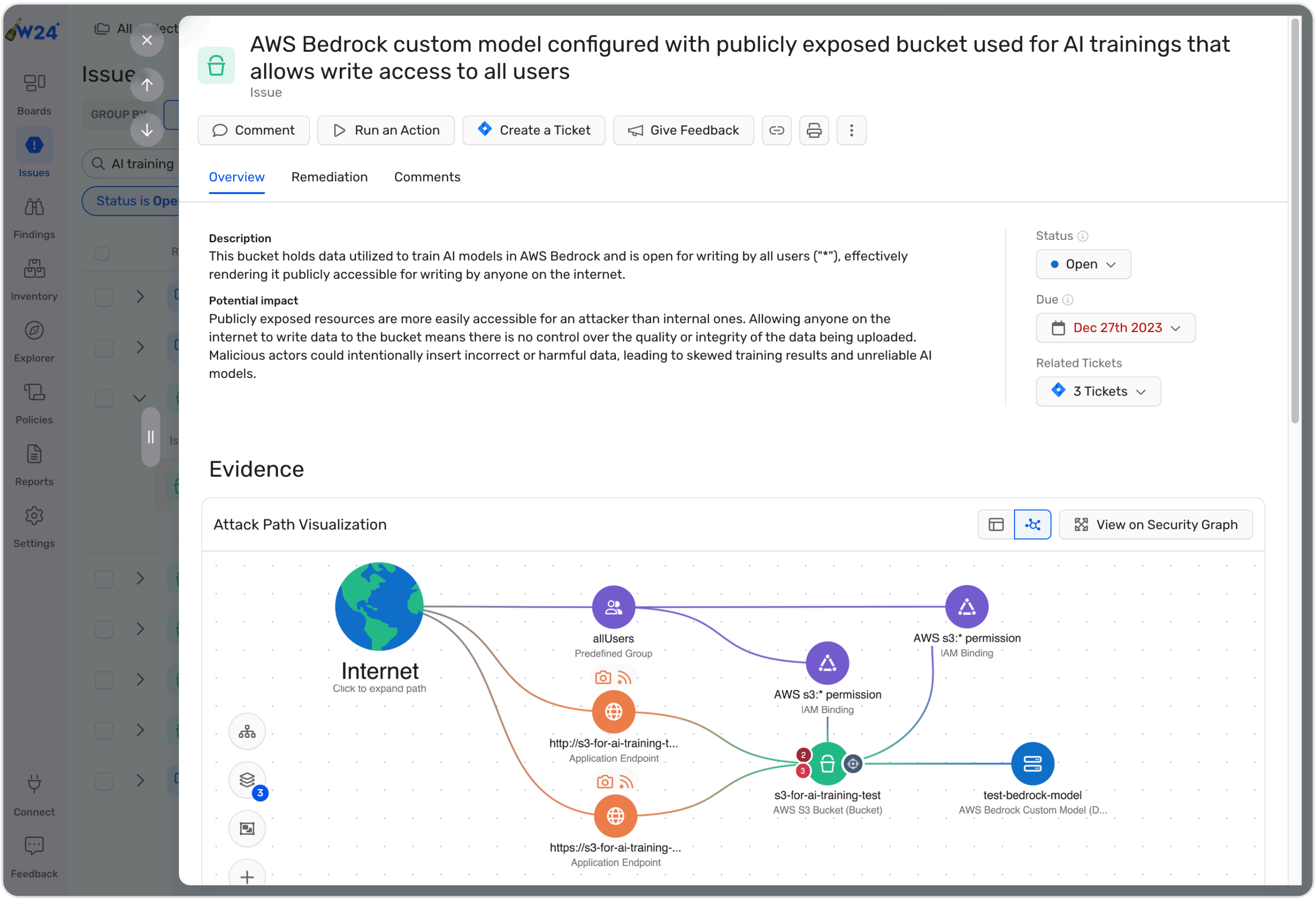
When potentially sensitive data is detected, a Data Finding connected to the relevant technology is added to the Security Graph.

English ▲

Attack path analysis for AI

This feature requires either a Wiz Standard or a Wiz Advanced license. Learn more.

Wiz detects toxic combinations of risks that could open attack paths leading to AI services and applications. These correlate exposure, identity, data and vulnerability analyses to reveal attack paths. For example, Wiz can detect a publicly exposed bucket used for AI training allows write access to all users:



AWS Bedrock custom model configured with publicly exposed bucket used for AI trainings that allows write access to all users

Issue

Description

This bucket holds data utilized to train AI models in AWS Bedrock and is open for writing by all users ("*"), effectively rendering it publicly accessible for writing by anyone on the internet.

Potential impact

Publicly exposed resources are more easily accessible for an attacker than internal ones. Allowing anyone on the internet to write data to the bucket means there is no control over the quality or integrity of the data being uploaded. Malicious actors could intentionally insert incorrect or harmful data, leading to skewed training results and unreliable AI models.

Status: Open

Due: Dec 27th 2023

Related Tickets: 3 Tickets

Evidence

Attack Path Visualization

When a Control detects an attack path, an Issue is created.

Supported AI models

Wiz detects the following AI models:

- Pytorch models— `.pt` , `.ckpt` , `.bin` files
- Tensorflow models— `.h5` , `.keras` , `.pb` files
- HuggingFace models, including all of the formats mentioned above along with with `.json` configuration files
- Other models— `.onnx` , `.gguf` and LLaMA files

Updated 10 days ago

English

← Threat Detection

Security Graph Queries →

Did this page help you? 👍 Yes 👎 No

English ▴