WIZ

Datasheet

AI-SPM: AI Security Posture Management

Secure your AI pipelines with AI-SPM

AI has introduced an era of unparalleled innovation, empowering organizations to efficiently build cutting-edge applications across all industries. The Wiz Research Team found that over 70% of organizations already have AI in their environment. As organizations are rapidly adopting AI into their cloud environment, they often face shadow-AI where the security team doesn't have full visibility into all AI components, making it challenging to secure. AI also increases the attack surface by introducing new types of risks such as model poisoning and training data leaks. Ingraining security into AI development becomes paramount in accelerating AI adoption in your environment.

Wiz AI-SPM empowers organizations to accelerate AI adoption while staying protected against AI risks. Wiz provides full visibility into all AI resources with AI-BOM capabilities and detects and prioritizes AI risks in the environment. With AI-SPM you can ensure your AI pipelines are protected across the AI development lifecycle so you can focus on bringing more machine learning models to production.

Agentless AI-BOM

Uncover shadow AI with Wiz AI-BOM capabilities that provide full-stack visibility into AI pipelines on the Wiz Security Graph. Detect AI services, such as Amazon Bedrock and Azure OpenAI, AI technologies, and SDKs without agents.

Detect AI misconfigurations

Enforce AI security best practices for your AI services with built-in misconfiguration rules and extend to your development pipeline with IaC scanning.

Remove critical AI risks

Proactively remove attack paths to your AI models with cloud and workload context around vulnerabilities, identities, network exposures, malware, data, and exposed secrets.

Wiz is trusted by the world's best brands

salesforce
COLGATE-PALMOLIVE
Morgan Stanley
slack
FOX
asos
snowflake
Takeda
BMW
REI co-op
MARS
CHIPOTLE MEXICAN GRILL
LVMH
priceline
experian

Wiz provides coverage for

aws

A unified cloud security platform providing a simple way to assess and remove AI risks in context and rapidly respond to minimize impact

Wiz AI-SPM helps organizations protect their AI pipelines with complete visibility into all AI components and deep risk assessment across misconfigurations, vulnerabilities, identities, data, network exposures, and secrets. This allows AI developers and data scientists to effectively remove critical AI risks from their environment and focus on further AI innovation.

Gain full-stack visibility with agentless AI-BOM

Wiz AI-BOM provides full-stack visibility across AI services, technologies, libraries, and SDKs, without any agents. Security teams can quickly detect new AI projects introduced to the environment in the Wiz Inventory.

Enforce AI configuration baselines with built-in checks

Identify misconfigurations in AI services with built-in rules, extend to your CI/CD pipeline with IaC scanning.

Remove attack paths to AI

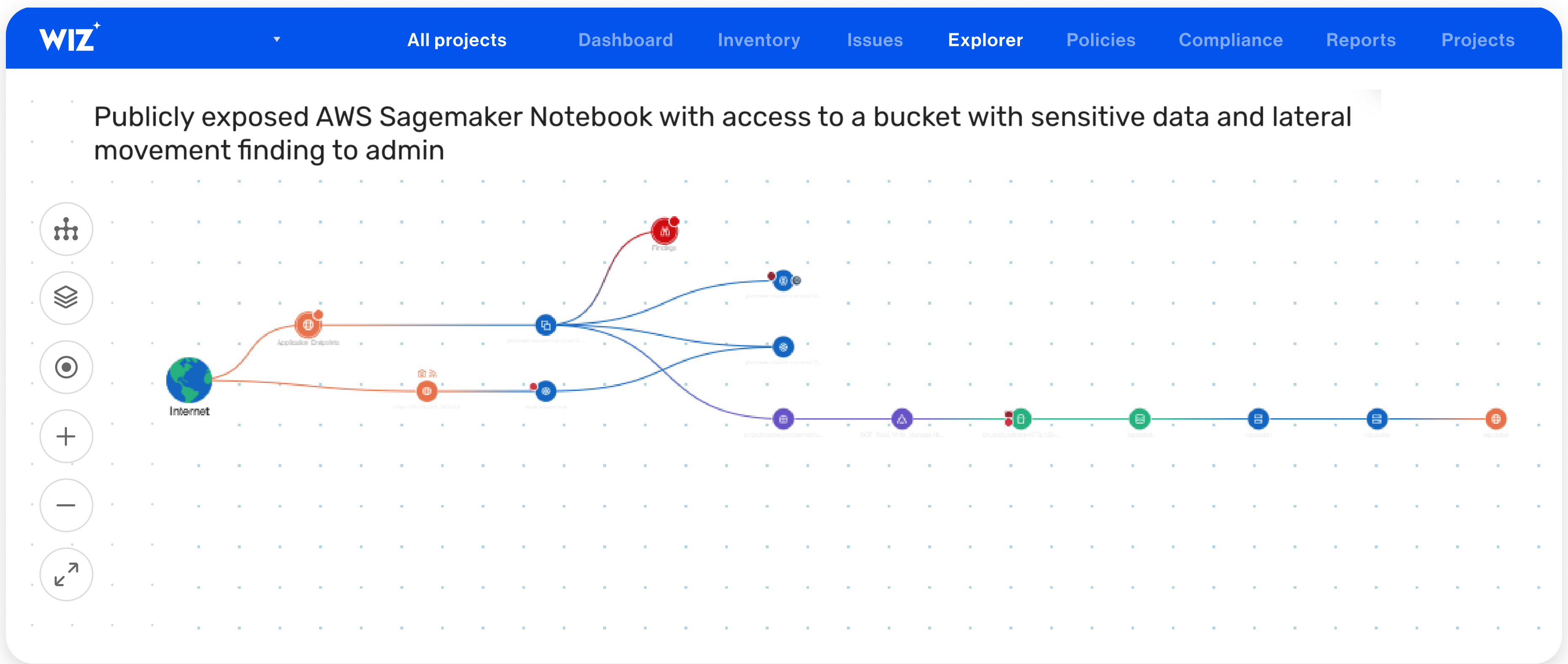
Wiz assesses the AI pipeline across vulnerabilities, identities, internet exposures, data, misconfigurations, and secrets and correlates risks on the Wiz Security Graph so you can proactively remove critical AI attack paths. Wiz DSPM automatically detects sensitive training data in your AI data stores so you can protect your crown jewels.

Detect misuse of AI

Quickly detect suspicious behavior and misuse in your AI pipelines with Wiz's AI threat detection rules, enabling your team to respond and remove threats in near real-time.

Empower AI developers with risk prioritization

Wiz makes it easy for your AI developers and data scientists to quickly understand their AI security posture with the AI security dashboard. The dashboard provides a prioritized queue of AI security issues, so they can focus on the most critical ones.



Publicly exposed AWS Sagemaker Notebook with access to a bucket with sensitive data and lateral movement finding to admin

Wiz transforms cloud security for customers – including 40% of the Fortune 100 – by enabling a new operating model. With Wiz, organizations can democratize security across the development lifecycle, empowering them to build fast and securely. Its Cloud Native Application Protection Platform (CNAPP) drives visibility, risk prioritization, and business agility, and is #1 based on customer reviews.

> Our data scientists and engineers use Vertex AI to build innovative AI-powered applications for our business units. Wiz provides us with full visibility across resources and helps protect our AI infrastructure from security risks.
>
> Ashley Dunn
> Head of Security Engineering, OVO

> Stability AI empowers creators, developers, and researchers to pioneer transformative AI models that unlock human potential. Wiz safeguards our infrastructure and APIs to facilitate seamless integration for partners and service providers, all while advancing the frontiers by supporting our needs related to AI research.
>
> Garry Jean-Baptiste
> CISO, Stability AI

stability.ai