PointGuard AI

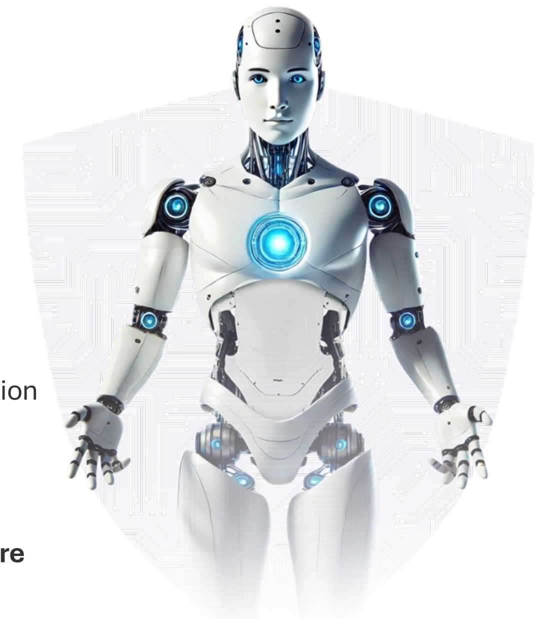
Security Posture Management

Part of a comprehensive AI Security & Governance Platform

AI Discovery | **AI Security Posture Mgt.** | Automated Red Teaming | AI Runtime Guardrails

Securing AI Projects at Every Stage

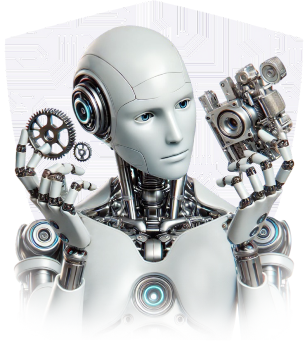
As AI deployments grow, organizations must ensure their AI platforms remain secure, compliant, and resilient. PointGuard AI Security Posture Management detects misconfigurations, malware risks, and vulnerabilities while automating remediation, enforcing compliance, and prioritizing issues.



Broad Protection for AI Development Platforms

PointGuard integrates directly with leading AI development platforms to continuously monitor and prevent errors, security risks, and threats. With automated remediation, compliance enforcement, and prioritized issue management, PointGuard enables secure AI adoption while fostering innovation and trust.

- **Ensures resiliency against cyberattacks**
- **Detects threats to AI infrastructure, models, and supply chains**
- **Integrates AI platforms from Databricks, AWS, Azure, Google, and more**



Detects Misconfigurations in MLOps Systems

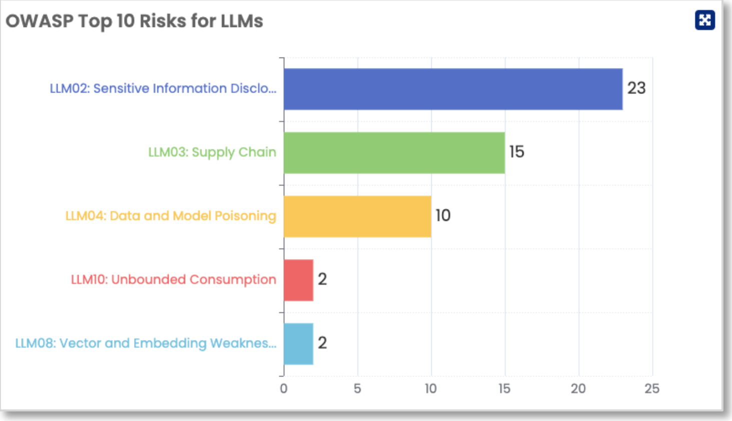
Misconfigurations in AI systems can open doors to major breaches, often going unnoticed until it's too late. PointGuard AI provides an extra layer of protection, identifying vulnerabilities, insecure permissions, and unauthorized system changes. It is optimized for the unique needs of LLMOps & MLOps platforms to ensure your AI environment is secure.

- **Provides continuous protection for LLMOps & MLOps platforms**
- **Identifies critical configuration errors that can lead to breaches**
- **Detects insecure permissions and unauthorized system changes**

Maps Findings to Leading Security Frameworks

PointGuard AI not only detects security issues – it also correlates them to industry-leading frameworks including the OWASP Top 10 for LLM Applications and Databricks DASF 2.0, helping to align detection with adversarial tactics and streamline compliance through industry best-practices.

- **Directly maps findings to leading frameworks:**
- **OWASP Top 10 for LLM Applications**
- **Databricks DASF 2.0**



Automates Remediation Workflows

PointGuard's automated workflows track exceptions and false positives and accelerate the remediation process, ensuring swift and efficient resolution of security vulnerabilities. Seamless integration with popular ticketing and collaboration tools fit directly into existing security operations.

- **Integrates with Jira, ServiceNow, and Teams**
- **Automates notifications and issue tracking**
- **Speeds up issue resolution to reduce disruption**

SC 2025 Awards WINNER

© 2025 | PointGuard AI |All rights reserved

AI Security Posture Management Capabilities

MLOps Platform Integration	
Platform Integration	Deep integration Databricks, Amazon SageMaker, Amazon Bedrock, Azure AI, Azure OpenAI, and Google Vertex AI
Detects Misconfigurations	Goes far deeper than CSPM platforms to harden MLOps processes.
Detects Insecure Access Permissions	Ensure security by default by detecting low-security access to models, datasets, and other AI resources.
Sample Security Risks Addressed	
Data Poisoning	Verifies insecure access permissions that result in poisoning training/inference datasets
Data Security	Validates that data is encrypted at rest and in transit
Malicious Libraries	Scans scripts and libraries used in notebooks for malicious code
Model Asset Leaks	Ensures models, checkpoints and other artifacts are stored securely with correct access controls
Model Theft	Governs model promotion, secures model serving end-points, manages credentials, and runs models in isolation
Supply Chain Attacks	Evaluates open-source model risk, hardens source-code repo access and runtime for MLOps and LLMOps
Connected Applications	Maps security posture and issues to connected applications and underlying vulnerabilities
Industry Framework Support	Maps all findings to industry-leading frameworks including OWASP Top 10 for LLM Applications, and Databricks DASF 2.0
Platform Capabilities	
Remediation Workflows	Automates ticket creation in Jira and ServiceNow and alerts stakeholders through Slack, MS Teams, and PagerDuty.
Notification Systems	Alerts stakeholders through Slack, MS Teams, and PagerDuty
Metrics & SLAs	Tracks metrics and team SLAs for model approvals, security findings, MTTR, security maturity and more.

Part of a Comprehensive Platform

PointGuard is the only vendor to secure both AI systems and software applications—protecting everything from code and third-party libraries to LLM models, datasets, and MLOps. The robust platform operationalizes AI security with comprehensive dashboards, metrics, SLAs, and automated remediation workflows with ticketing systems like Jira and ServiceNow.

Get Started with a Free AI Risk Assessment

Let us demonstrate the power of the PointGuard AI platform providing an overview of your AI security posture with actionable recommendations. Learn more at:

www.pointguardai.com/free-discovery