PointGuard AI for Databricks

Enabling AI Innovation with Security, Governance, and Confidence

Artificial intelligence (AI) is revolutionizing industries by enabling faster insights, automation, and innovation. As enterprises invest heavily in platforms like Databricks, known for its leadership in AI and data engineering, ensuring robust security has become a critical priority. Many fast-moving AI projects, driven by data scientists bypass conventional security processes. This creates gaps that leave AI systems vulnerable. PointGuard AI, a Databricks Validated Technology Partner, bridges this gap by offering AI security that supports and enables innovation without creating bottlenecks.

Growing AI Security Challenges

As AI adoption grows, companies face significant security risks that can disrupt operations and compromise sensitive data. Key challenges include:

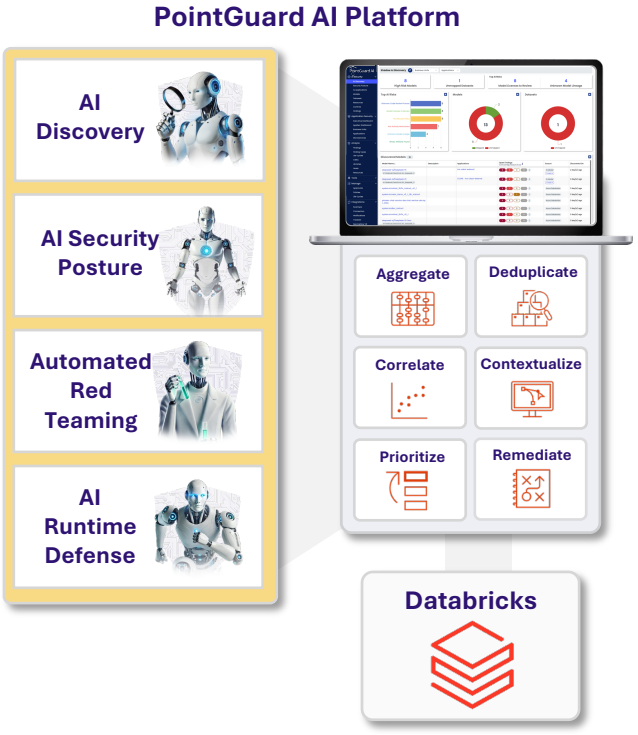
- **Lack of Visibility into AI Projects and Supply Chains:** Limited oversight of AI models, especially those involving open-source components, creates security blind spots.
- **Expanded Attack Surface:** New attack vectors, such as model poisoning and prompt injections, demand proactive defenses.
- **Sensitive Data Leaks:** Misconfigurations and weak access controls can expose confidential or regulated data.
- **Remediation Delays:** Slow, manual remediation processes hinder timely threat resolution and sustainable governance.

Given the complexity of AI environments, robust security governance is crucial to address these challenges.

PointGuard AI for Databricks: Comprehensive Security

The partnership between PointGuard AI and Databricks delivers a comprehensive solution to secure AI systems across the entire lifecycle. PointGuard's four core modules address key security challenges while seamlessly integrating into the Databricks MLOps environment:

- **AI Discovery:** Detects and inventories models, datasets, notebooks, and pipelines, enabling governance and maintaining a real-time security inventory.
- **AI Security Posture Hardening:** Monitors for misconfigurations, enforces access controls, and provides automated remediation, preventing unauthorized data exposure.
- **Automated Red Teaming:** Uses model scanning and automated Red Teaming to identify risks like model poisoning and vulnerabilities before they can be exploited, ensuring resilience against threats.
- **AI Runtime Defense:** Detects anomalies, prevents data leaks, and identifies misuse in real time through inline scanning of sensitive information.



www.pointguardai.com
info@pointguardai.com

PointGuard AI for Databricks

Commitment to Customer Success

PointGuard collaborates closely with Databricks with a joint solution that is easy to deploy and manage, automating time-consuming security checks. Together, they help enterprises adopt AI securely while minimizing operational friction and maximizing business outcomes.

Full Support for DASF 2.0

PointGuard AI fully integrates with the Databricks AI Security Framework (DASF) 2.0, mapping all findings to more than 60 controls and AI-specific risks.

"PointGuard's integration with DASF 2.0 is a testament to their dedication to advancing AI security standards."
- Arun Pamulapati, Databricks

Customer Paint Points	PointGuard AI Solution
Visibility and Supply Chain Security	
Lack of visibility into MLOps security posture	• Discovers and inventories LLM pipelines • Establishes governance for models & AI resources
Unknown risk levels for open-source models	• Assesses model risk through knowledge base • Automates approval workflows for new assets
AI supply chain lacks established controls	• Creates AI-BOM and verifies integrity of assets
Expanded AI Attack Surface	
Models may contain malware or other flaws	• Deep model testing detects prompt injections, jailbreaking, toxicity, malware, & vulnerabilities
Notebooks may make unsanctioned connections to business applications	• Identifies and maps AI resources to connected applications with approval workflows
MLOps security settings may be misconfigured creating inadvertent exposure	• Automatically detects misconfigurations. Maps risk findings to Databricks DASF controls
Sensitive Data Protection	
Leaks of sensitive data and IP	• Verifies data classification and controls access • Ensures datasets are encrypted at rest or in transit
Data poisoning, model theft, training abuse	• Detects model tampering, content anomalies and unbounded consumption
Limited access controls to AI resources	• Identifies excessive permissions to enforce principle of least privilege
Governance and Remediation	
Need to align risks with industry standards	• Maps all findings to leading AI frameworks including OWASP Top 10 for LLM Applications.
Tedious manual, one-off data collection impedes compliance	• Continuous, automated compliance with intuitive drill-down dashboards and reporting
Slow, disconnected, manual remediation wastes resources and creates backlogs	• End-to-end workflows prioritize and automate remediation, ticketing, and notifications