gruve

SOLUTION BRIEF

AI Cybersecurity Posture Assessment: Identify and eliminate active AI vulnerabilities

Partners: Technology-agnostic, platform-independent security testing

01

Business problem

Your organization has already embraced AI—deploying chatbots for customer service, implementing machine learning models for business intelligence, integrating generative AI tools across teams, and embedding AI capabilities into applications. But are these production AI systems actually secure? Most organizations discover the answer only after breaches, data leaks, or compliance violations expose costly vulnerabilities.

AI Cybersecurity Posture Assessment addresses a fundamentally different challenge than readiness assessment. While readiness assessments evaluate preparedness for future AI adoption, posture assessments examine the security of AI systems already in production—identifying exploitable vulnerabilities, exposed data, misconfigurations, and compliance violations that exist right now.

The stakes are severe. Organizations discover an average of 15-25 critical vulnerabilities in production AI systems during security assessments. These vulnerabilities enable adversaries to extract sensitive data through prompt injection, steal proprietary models through API exploitation, manipulate AI decisions through adversarial attacks, and bypass security controls through jailbreak techniques. The average breach cost of $4.45 million pales compared to AI-specific incidents where model theft can represent hundreds of millions in R&D investment loss.

Regulatory compliance violations in production AI systems create immediate risk. GDPR, HIPAA, PCI DSS, and sector-specific regulations extend to AI systems processing regulated data. The EU AI Act establishes direct security requirements for high-risk AI systems. Organizations operating non-compliant AI systems face enforcement actions, substantial fines, and mandated remediation disrupting business operations.

Most critically, organizations lack visibility into their actual AI security posture. Security teams trained on traditional application security miss AI-specific attack vectors. Penetration testing firms without AI expertise produce incomplete assessments missing critical vulnerabilities. Meanwhile, adversaries actively exploit AI systems using sophisticated techniques that traditional security tools cannot detect.

⚠

15-25

critical vulnerabilities are discovered on average in production AI systems during security assessments

02

Why now

Your AI systems are processing sensitive data and exposed to threats right now—not in some future planning cycle. Every day of delay means continued exposure to vulnerabilities that adversaries can exploit. Recent high-profile breaches demonstrate that AI systems face active, sophisticated attacks from motivated adversaries seeking data theft, model extraction, and operational disruption.

The regulatory environment has shifted from guidance to enforcement. Regulators actively examine AI system security during audits and investigations. Organizations discovered operating non-compliant AI systems face substantial penalties and public disclosure requirements. Proactive posture assessment enables addressing compliance gaps before regulatory examination rather than scrambling under enforcement pressure.

AI attack techniques have matured rapidly. What were academic research demonstrations 12-18 months ago are now readily available exploitation tools. Adversaries weaponize prompt injection, model extraction, and adversarial attack techniques. Organizations defending AI systems with traditional security controls face sophisticated threats their defenses cannot detect or prevent.

Competitive dynamics reward demonstrated AI security. Customers increasingly demand evidence of AI system security before sharing sensitive data. Partners require security validation before integration. Investors scrutinize AI security posture during due diligence. Organizations providing audit-ready evidence of secure AI deployment gain advantages that insecure competitors cannot match.

10-50x

higher costs when vulnerabilities are addressed post-breach compared to proactive assessments

The cost of addressing vulnerabilities post-breach exceeds proactive assessment by 10-50x. Breaches trigger incident response, forensics, remediation, notification, legal expenses, regulatory fines, and reputational damage totaling millions. Proactive posture assessment costing $30,000-$175,000 prevents losses orders of magnitude larger.

03

Solution overview

Gruve's AI Cybersecurity Posture Assessment provides rapid, expert evaluation of production AI system security through hands-on vulnerability testing, threat simulation, and comprehensive security analysis. Our cybersecurity specialists conduct adversarial testing combining automated scanning with expert manual assessment to uncover AI-specific vulnerabilities that traditional security assessments miss.

Unlike penetration testing firms lacking AI security expertise or automated scanning missing nuanced vulnerabilities, Gruve delivers comprehensive assessment covering all AI-specific attack vectors—prompt injection, model extraction, adversarial attacks, training data leakage, API security, and supply chain risks. We test your production AI systems non-disruptively while identifying exploitable vulnerabilities before adversaries do.

Assessment components	Description
AI system discovery	Comprehensive identification of all deployed AI systems including customer-facing chatbots, internal AI tools, AI-powered applications, custom models, and shadow AI usage, with risk prioritization
AI application security testing	Hands-on testing for prompt injection vulnerabilities, jailbreak techniques, input validation bypasses, output manipulation, business logic exploitation, and authentication/authorization flaws
AI model security analysis	Assessment of model extraction vulnerabilities, adversarial attack resilience, training data access controls, model theft prevention, backdoor detection, and inference attack resistance
AI infrastructure evaluation	Cloud configuration review, network segmentation testing, secrets management assessment, API security analysis, access control validation, and encryption verification
Data protection testing	Sensitive data discovery (PII/PHI/PCI/IP), access control validation, data leakage testing, privacy control verification, retention compliance, and data sovereignty evaluation
Compliance validation	EU AI Act compliance assessment, NIST AI RMF alignment, industry regulation verification (HIPAA, PCI DSS, SOC 2), audit trail evaluation, and regulatory risk quantification

04

Key benefits

Immediate vulnerability discovery
Identify exploitable vulnerabilities in production AI systems before adversaries exploit them, with risk-prioritized findings enabling focused remediation on highest-impact security gaps

Prevention of AI breaches
Stop data breaches (averaging $4.5M+ cost), prevent model theft and IP loss, block sensitive data exfiltration through AI systems, and protect against operational disruption

Regulatory compliance assurance
Verify EU AI Act compliance with auditor-ready evidence, validate NIST AI RMF alignment, confirm industry requirements (HIPAA, PCI DSS, SOC 2), and prevent regulatory penalties

Competitive advantage
Demonstrate AI security to customers requiring validation, pass partner security reviews efficiently, satisfy investor due diligence requirements, and differentiate through verified security posture

Actionable remediation guidance
Receive specific technical remediation steps for each vulnerability, implementation guidance preserving AI functionality, effort estimates for remediation planning, and prioritization by risk and business impact

05

Service tiers

Tier	**Foundation Posture Assessment (3-Day)**	**Comprehensive Posture Assessment (10-Day)**
AI systems tested	3-5 highest-risk systems	All deployed AI systems
Testing depth	Core vulnerabilities	Extensive all attack vectors
Infrastructure testing	Configuration review	Detailed penetration testing
Data protection	Spot-check	Comprehensive PII/PHI/PCI discovery
Compliance validation	Gap highlights	Detailed evidence collection
Roadmap	30-day actions	12-month phased plan
Investment	$30,000-$50,000	$85,000-$175,000

06

Secure your production AI systems now

Your AI systems are processing sensitive data and exposed to threats right now. Don't wait for a breach to discover your vulnerabilities. Schedule an AI Cybersecurity Posture Assessment to identify and remediate active security gaps before adversaries exploit them.

Website: https://www.gruve.ai/

Email: info@gruve.ai