gruve

SOLUTION BRIEF

AI Cybersecurity Readiness Assessment: Secure your AI transformation

Partners: Technology-agnostic, comprehensive assessment framework

01

Business problem

Organizations rush to adopt AI technologies across business functions—deploying generative AI chatbots, integrating large language models into applications, building custom AI models, and leveraging AI-powered analytics. Yet most organizations deploy these AI systems without assessing whether their cybersecurity controls can protect AI-specific attack surfaces, secure sensitive training data, or prevent AI model theft and manipulation.

The consequences of insecure AI deployment are severe and growing. AI systems process vast amounts of sensitive data including customer PII, intellectual property, financial information, and healthcare records. Breaches exposing this data through AI systems carry average costs of $4.45 million according to IBM research, with healthcare and financial services breaches exceeding $10 million. Model theft enables competitors to replicate years of R&D investment. Prompt injection attacks manipulate AI systems into bypassing security controls or leaking sensitive information.

Regulatory scrutiny of AI deployment security intensifies quarterly. The EU AI Act establishes comprehensive security requirements for high-risk AI systems. GDPR, CCPA, and sector-specific regulations extend to AI systems processing personal data. SEC cybersecurity disclosure rules and NIS2 Directive create obligations for AI system security that most organizations haven't addressed.

Organizations lack frameworks to assess AI cybersecurity readiness comprehensively. Security teams trained on traditional application and infrastructure security miss AI-specific vulnerabilities including prompt injection, model poisoning, adversarial attacks, training data leakage, and AI supply chain risks. Leadership approves AI initiatives without understanding whether existing security controls adequately protect AI systems—creating blind spots that adversaries actively exploit.

02

Why now

The AI security threat landscape has matured from theoretical to actively exploited. Security researchers demonstrate prompt injection attacks bypassing AI system controls. Adversaries steal proprietary AI models through API exploitation. Malicious actors poison training datasets to backdoor AI systems. Real-world breaches involving AI systems increase quarterly, yet most organizations remain unprepared.

Regulatory frameworks governing AI security are no longer proposals—they're active requirements. The EU AI Act became enforceable in 2024 with substantial penalties for non-compliance. Industry regulators including financial services (OCC), healthcare (FDA, OCR), and consumer protection (FTC) issued AI-specific security guidance. Organizations deploying AI systems without addressing regulatory requirements face enforcement actions, fines, and mandated security improvements costing millions.

The window for proactive AI security assessment is closing. Organizations conducting readiness assessments now can incorporate proper controls, governance frameworks, and compliance capabilities before regulatory examinations or security incidents force expensive retrofitting. Those waiting until after breaches or enforcement actions face 10-100x higher remediation costs plus reputational damage and regulatory penalties.

10-100x

higher remediation costs for those who wait until after breaches or enforcement actions

Competitive dynamics reward secure AI deployment. Organizations demonstrating robust AI security gain customer trust, pass security reviews faster, meet compliance requirements efficiently, and avoid breach-related business disruptions that damage competitor organizations. Early investment in AI cybersecurity readiness creates sustainable competitive advantages.

03

Solution overview

Gruve's AI Cybersecurity Readiness Assessment provides comprehensive evaluation of your organization's preparedness to securely deploy, operate, and govern AI systems enterprise-wide. Our cybersecurity experts combine 17+ years of security operations experience with cutting-edge AI security specialization to assess AI inventory, data protection controls, model security practices, infrastructure hardening, compliance frameworks, and governance mechanisms.

Unlike generic security assessments missing AI-specific vulnerabilities or vendor assessments biased toward specific products, Gruve delivers technology-agnostic evaluation covering all AI platforms, deployment models, and use cases. We assess readiness across technical controls, operational processes, governance frameworks, and compliance requirements—delivering actionable roadmaps prioritizing remediation by risk and business impact.

Assessment dimensions	**Description**
AI system inventory & classification	Comprehensive discovery of deployed AI systems including generative AI integrations, custom models, AI-embedded applications, and shadow AI usage. Risk classification based on data sensitivity, decision authority, and regulatory applicability
Data protection & privacy	Assessment of sensitive data handling in AI systems, training data security, inference data protection, data retention and disposal, privacy controls for PII/PHI/PCI, and data sovereignty compliance
AI model security	Evaluation of model protection mechanisms, adversarial robustness, prompt injection defenses, model theft prevention, poisoning attack resistance, and output validation controls
Infrastructure & platform security	Review of AI hosting environment security, API authentication and authorization, network segmentation, secrets management, access controls, and cloud configuration security
Supply chain risk	Assessment of third-party AI vendor security, open-source model risks, AI API provider security, dependency management, and supply chain attack vectors
Governance & compliance	Evaluation of AI governance frameworks, decision accountability, audit trails, model explainability capabilities, regulatory compliance (EU AI Act, GDPR, sector-specific), and risk management integration

04

Key benefits

Risk identification & quantification
Identify active vulnerabilities and exposures in deployed AI systems with risk quantification translating technical findings to business impact including breach probability, potential financial losses, and regulatory penalties

Regulatory compliance roadmap
Receive detailed compliance gap analysis and remediation roadmap for EU AI Act, GDPR, CCPA, HIPAA, and sector-specific requirements with audit-ready documentation of security controls

Prevention of AI breaches
Avoid $4.5M+ average breach costs through proactive vulnerability identification and remediation before adversaries exploit weaknesses in AI systems processing sensitive data

Accelerated secure AI adoption
Enable confident AI deployment with validated security controls rather than delaying initiatives due to security concerns or deploying insecure systems creating risk exposure

Competitive advantage
Demonstrate AI security leadership to customers, partners, and regulators—passing security reviews faster and building trust that insecure competitors cannot match

05

Service tiers

Tier	Foundation Assessment (3-5 days)	Comprehensive Assessment (10 days)
AI system discovery	Critical systems inventory	Complete discovery including shadow AI
Security testing	High-risk vulnerability assessment	Comprehensive testing all systems
Data protection review	Sample assessment	Complete PII/PHI/PCI discovery
Compliance evaluation	Gap highlights	Detailed regulatory mapping
Remediation roadmap	90-day action plan	12-18 month phased strategy
Investment	$35,000-$60,000	$90,000-$175,000

06

Secure your AI transformation today

Don’t wait for a breach or regulatory enforcement to discover AI security gaps. Schedule a consultation with Gruve’s AI security experts to assess your readiness and receive a clear roadmap to secure AI deployment.

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

Email: info@gruve.ai