relyanceai

AI Security Checklist

PHASE 1 • IMMEDIATE

See Every Data Exposure

AI Asset Discovery

□ Inventory all AI models, agents, and datasets across your environment

□ Discover shadow AI and unsanctioned tools deployed without security review

□ Map MCP servers and third-party AI integrations

□ Identify AI features enabled within existing SaaS vendor contracts

Sensitive Data Mapping

□ Classify PII, PHI, PCI, and enterprise-specific data across AI workflows

□ Trace how sensitive data enters, flows through, and exits AI systems

□ Map data flows across training pipelines and inference endpoints

Code and Pipeline Visibility

□ Scan source code repositories for AI-related risks and credentials

□ Audit CI/CD pipelines feeding data into AI training workflows

□ Identify code-level exposures missed by cloud-only scanning tools

PHASE 2 • CONTEXTUAL

Understand Compounding Risk

Identity-to-Data Intelligence

□ Map how AI agents, service accounts, and automated workflows access sensitive data

□ Trace permission chains from agent to API key to service account to data store

□ Treat AI agents and MCP servers as first-class identities alongside human users

Compound Risk Detection

□ Correlate data sensitivity, identity permissions, and access behavior in real time

□ Surface dangerous combinations that no individual scan would flag

□ Assess AI supply chain risks in the context of the sensitive data they can reach

Overprivileged Access Review

□ Audit AI agent permissions against the principle of least privilege

□ Identify agents with administrative access to regulated data stores

□ Review non-human identity coverage gaps across your AI environment

PHASE 3 • OPERATIONAL

Resolve Fast with Integrated Risk Response

Contextual Remediation

- □ Ensure every finding includes what is wrong, who is involved, and what data is at risk
- □ Deliver code-level fix guidance, not just posture alerts
- □ Eliminate the investigation tax of stitching context across 4+ tools

Continuous AI Governance

- □ Implement runtime policy mapping and model lineage tracking
- □ Monitor for behavioral drift as models get retrained and agents gain new tools
- □ Maintain a historical audit framework that stays current as AI systems change

Live Compliance Mapping

- □ Automate continuous mapping to EU AI Act, NIST AI RMF, and ISO 42001
- □ Replace point-in-time questionnaires with always-current vendor AI risk assessments
- □ Generate compliance evidence from live AI inventory, not retroactive reports

Top AI Security Risks to Address

Data Exposure Risks

□ Prevent sensitive data leakage through AI training or inference flows

□ Detect shadow AI processing regulated data without governance controls

□ Validate that third-party AI vendors handle data per contractual terms

Agentic AI Risks

□ Monitor for autonomous agent overreach and unintended tool chaining

□ Detect privilege escalation by AI agents accessing data beyond intended scope

□ Track AI agents operating as insider threats at machine speed

AI Supply Chain Risks

□ Vet third-party models, MCP servers, and open-source components before deployment

□ Map supply chain vulnerabilities to the sensitive data those components can reach

□ Monitor for compliance drift as runtime behavior diverges from regulatory controls

AI Security Tool Evaluation Criteria

What to Look For

- □ Complete visibility across code, cloud, SaaS, and the full AI stack
- □ Data journey context that maps relationships, not just inventory
- □ Compound risk detection correlating data, identity, and agent behavior
- □ Contextual remediation with severity, scope, and resolution path
- □ Agentless, API-first architecture for fast deployment

What to Watch Out For

- □ Scanner-only tools that discover but lack context or remediation
- □ Siloed AI-SPM products disconnected from data security posture
- □ Periodic scan architectures too slow for real-time agentic AI risks
- □ Tools that ignore non-human identities and AI agent permission chains

Want the full picture?

This checklist is a companion to our AI Security Whitepaper. Download the full guide at relyance.ai for a deep dive into the risk landscape, current tool gaps, and how to build a complete AI security program.