Latio

AI Security
Market Report

Reporting Period
Q2 • 2025

Prepared by
James Berthoty

TABLE OF CONTENTS

REPORT INTRODUCTION 3

AI USE CASES 4

AI ADOPTION & SECURITY NEEDS 11

OLD SOLUTIONS, NEW PROBLEMS 15

MARKET MAP AND LEADERS 18

TOOL BUYING FLOW CHART 29

VENDOR BREAKDOWNS 34

CONCLUSION 45

AI Security Landscape

AI security in 2025 has been defined by a disjointed landscape of solutions to unclear problems.

A venture capital fueled marketing frenzy has led to widespread confusion across social media, with significant misunderstandings around both use cases and best practices. **This report cuts through the noise to clarify what's been lost in the murkiness of so-called "AI-TRiSM."**

While the AI Trust, Risk, and Security Management category was created to bring a range of solutions under a single label, it has often flattened the important distinctions between tools, especially when it comes to what problems vendors are solving and how.

Most of AI Security might feel new, but many of the underlying challenges are quite familiar. In nearly every category we'll cover, there are existing tools that offer similar functionalities to various startups.

While that may suggest security teams should wait to adopt new solutions, it will take time for these traditional vendors to match the pace and specialization of newer, AI-native offerings.

As with any security decision, the right choice depends heavily on three important factors:

- **Your specific risk profile**
- **Technology stack**
- **Organizational priorities**

By the end of this report, you'll walk away with two things:

- A clear understanding of when and why to use an AI security tool, including what specific use cases these tools are designed to address.
- A structured overview of the vendors currently in the space, what they offer, and how to evaluate them based on your needs.

We'll also include a simple decision flowchart to help guide your tool selection based on real-world scenarios.

We hope this information is helpful, and we thank you for using Latio as your source for trusted industry insights.

AI SECURITY USE CASES

Let's start by outlining the different AI security use cases. These can be separated into four major categories:

01 End User Data Control

1. Data Loss Prevention
2. SaaS Access control
3. Secure Code Creation

(IT teams)

02 AI Posture Management

1. Infrastructure Discovery
2. ML-BOM/AI-BOM
3. Data Pipeline Posture
4. Static Code Testing

(Infrastructure teams)

03 Application Runtime

1. Prompt Injection Protection
2. Visibility into runtime models
3. Authn/Authz
4. Dynamic Testing

(AppSec/DevSecOps)

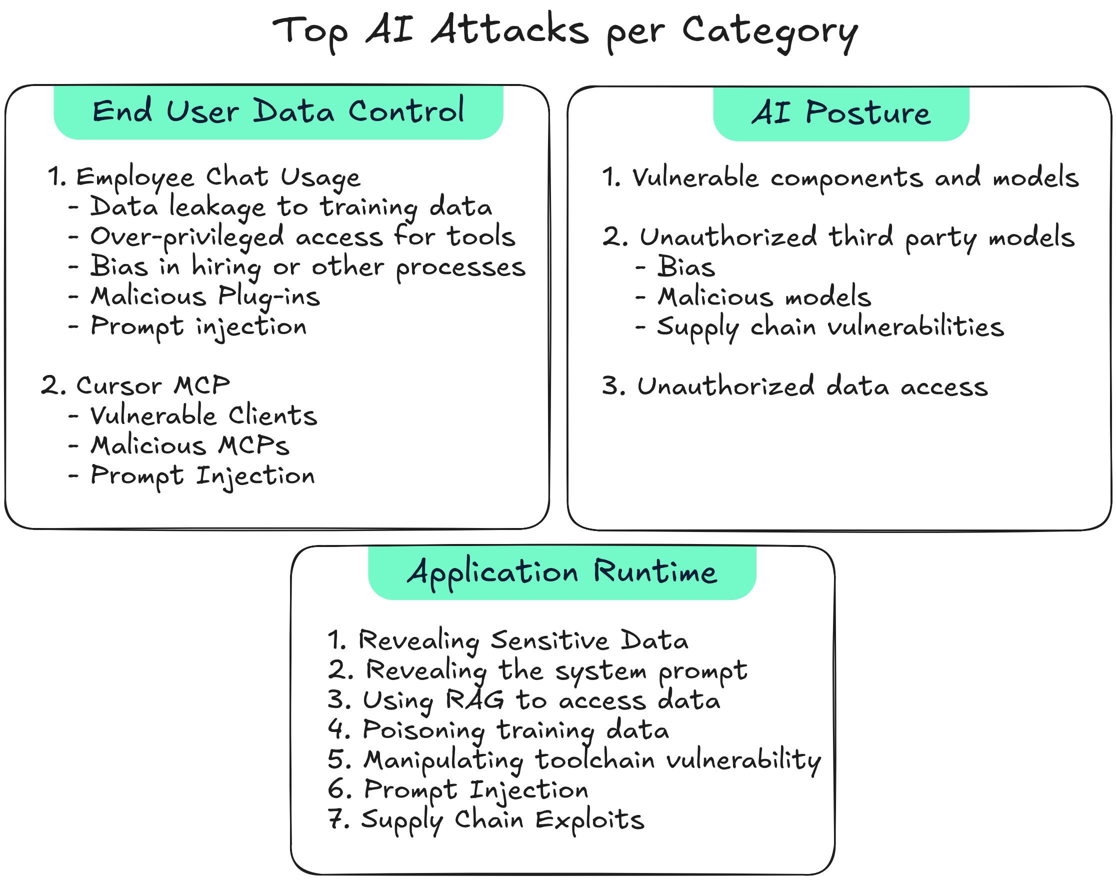
04 AI for Security

1. AI for SOC
2. AI for Vulnerability Management
3. AI for AppSec

(SOC and AppSec)

As a brief aside, you could argue for a fifth category, **policy and compliance management** around AI concerns, but we're choosing to exclude it from this report. It's a smaller use case and typically less relevant to security engineers.

Risk Types



Top AI Attacks per Category

End User Data Control

1. Employee Chat Usage
   - Data leakage to training data
   - Over-privileged access for tools
   - Bias in hiring or other processes
   - Malicious Plug-ins
   - Prompt injection

2. Cursor MCP
   - Vulnerable Clients
   - Malicious MCPs
   - Prompt Injection

AI Posture

1. Vulnerable components and models

2. Unauthorized third party models
   - Bias
   - Malicious models
   - Supply chain vulnerabilities

3. Unauthorized data access

Application Runtime

1. Revealing Sensitive Data
2. Revealing the system prompt
3. Using RAG to access data
4. Poisoning training data
5. Manipulating toolchain vulnerability
6. Prompt Injection
7. Supply Chain Exploits

Each category of AI tooling is designed to protect against specific risks for these categories. On the end user data side, tools protect employee endpoints against manipulation, or stop employees from sharing unauthorized materials with unauthorized AI systems.

On the posture side, security teams struggle to get deep insights into how models are being developed and deployed, and what datasets these models have access to. While many teams are relying on third party models, self hosted models are especially vulnerable to different poisoning or supply chain attacks. Additionally, models can have vulnerabilities the same as any other code packages.

Finally, runtime application security is the most at risk for real world attack, especially once a system is wired up to internal data. Early iterations of AI applications were low risk, as they merely surfaced a user's data back to them; however, agentic architectures have rapidly increased risk as agents take actions on behalf of users, and have access to sensitive data.