

HOW CURATU AI USED AI PENETRATION TESTING TO PREPARE FOR ENTERPRISE GROWTH



LOCATION

Waterloo,
Ontario

INDUSTRY

Software
Development

EMPLOYEES

2-10

FUNDING

3.1 M

Curatu AI is an early-stage AI SaaS company building an automation platform that allows businesses to create workflows, integrate APIs, and deploy AI-powered experiences across channels including web chatbots, voice, and WhatsApp.

Preparing Early for SOC 2 and Enterprise Security Reviews

Curatu AI's team is looking ahead. As the platform grows, they expect the number of security questions they receive to increase, and larger customers will likely ask how systems have been independently tested.

They are considering pursuing SOC 2 Type II in the future and know that building the necessary security practices will take time. The team also recognized that the security expectations surrounding an AI SaaS platform go beyond checking a compliance box. Curatu AI's platform allows customers to integrate APIs, configure authorization methods, and build automations that can interact with potentially sensitive information. Some of that information also flows through AI components.

For CTO Rahul, the goal was broader:

"We just want to make sure that each and every piece of our application is secured completely."

Curatu AI wanted a penetration test that would evaluate the application as an attacker would, rather than an automated scan designed to satisfy a compliance requirement.

HOW CURATU AI USED AI PENETRATION TESTING TO PREPARE FOR ENTERPRISE GROWTH

Testing the SaaS and AI Attack Surface Together

Curatu AI's first pentest needed to account for two overlapping attack surfaces: the traditional security risks of a multi-tenant SaaS application and the emerging risks associated with AI. Software Secured scoped a human-led application penetration test covering areas including authentication, authorization, permissions, public APIs, and cross-tenant access.

Cross-tenant testing was particularly important for Curatu AI's SaaS architecture. Testing needed to determine whether authorization controls properly separated customers and prevented one tenant from accessing another tenant's data, workflows, or automations. The AI functionality added another layer.

Curatu AI's environment included AI workflows, RAG capabilities, and an MCP server. That meant the engagement needed to consider AI-specific attack paths alongside conventional web application and API testing. The scope incorporated established security methodologies, including the OWASP Top 10, the OWASP API Security Top 10, the OWASP Web Security Testing Guide, and NIST guidance. Instead of treating AI security as a separate checkbox, the goal was to evaluate how Curatu's AI functionality interacted with the rest of its application and attack surface.

Finding the Right Pentest Scope for an Early-Stage Startup

Curatu AI was also navigating a familiar startup problem: how much security investment makes sense before customers begin demanding it? This was the company's first pentest, and budget mattered. Software Secured presented different testing options but recommended against immediately purchasing the most comprehensive package.

Curatu AI needed enough depth to meaningfully assess its application and prepare for future security scrutiny without paying for a testing program designed for a much larger organization. The team was also already aware of several issues it planned to address before testing.

Software Secured suggested a different approach: rather than spending limited engineering time trying to anticipate and eliminate every possible issue beforehand, let the pentest help determine which security risks actually deserved priority. For an early-stage engineering team, finding potential issues is only part of the job. Teams also need to understand which ones represent meaningful risk and where engineering time will have the greatest impact.

HOW CURATU AI USED AI PENETRATION TESTING TO PREPARE FOR ENTERPRISE GROWTH

Making the Pentest Part of the Development

Curatu AI was concerned that penetration testing could disrupt its application or affect its customers. Because application penetration testing intentionally pushes functionality into unexpected states, Software Secured recommended conducting the application portion against staging rather than introducing unnecessary risk to the production environment.

Curatu AI agreed to bring its staging environment closer to production where necessary for testing. The engagement was also designed so the pentest wouldn't end when the report was delivered. Each identified vulnerability would include remediation guidance, with Software Secured's pentesters available to provide additional technical context when necessary.

Because Curatu AI already used GitHub, vulnerabilities could also be moved from Software Secured's Portal into its existing development workflow rather than being manually recreated and tracked separately. Three rounds of retesting over the following year gave Curatu AI a way to return after remediation and verify that fixes worked as intended.

Establishing a Security Baseline

The engagement gave the team an independent assessment of its application and a security baseline it could build on as the company matured. More importantly, Curatu AI chose to establish that baseline before an auditor or enterprise customer forced the issue.

Curatu AI's application brings together customer data, API integrations, authorization mechanisms, multi-tenant functionality, and AI-driven workflows. As the company grows, customers are likely to ask increasingly detailed questions about how those systems are secured and independently tested. Curatu AI now has a foundation for those conversations and a starting point for determining how its security testing should evolve alongside the product.

"We wanted to get ahead of security before it became a requirement. As an AI company handling customer data, we knew we needed to understand the risks across both our application and our AI functionality. Software Secured gave us a thorough, practical assessment and a clear path for addressing what matters most."

Aneeq Musa, CEO, Curatu AI