PENTESTING FOR DISTRIBUTED AI SYSTEMS

Qurrent

LOCATION

San Francisco. CA

INDUSTRY

Software Development

EMPLOYEES

11-50

CUSTOMERS

Yahoo!
Spire
Roofstock
Pacaso

Qurrent builds and operates custom AI-powered "workforces" for enterprise companies. Their core product orchestrates multiple AI agents to manage complex tasks with productivity, consistency, and transparency. Qurrent must protect customer data across highly customized deployments to provide the reliability that modern AI buyers expect

Penetration Testing For Complex Deployment Models

Qurrent was growing more than 300%, and its product was evolving just as quickly. Their deployment model was intentionally flexible: each AI workforce was deployed separately for every customer. Unlike a traditional SaaS platform with a single well-defined architecture, Qurrent's model varied by customer.

This flexibility created complexity. Complexity can create risks that attackers can exploit. As Qurrent scaled, SOC 2 and HIPAA requirements emerged while customer security expectations increased. They needed evidence of the effectiveness and resilience of the security controls in place, notwithstanding the system's flexibility.

Traditional penetration testing firms struggled to fully understand the risk Qurrent was working to address. They needed a partner capable of understanding custom infrastructure and designing penetration testing around how Qurrent actually delivered AI.

An Approach Designed for Custom AI Architectures

Software Secured approached Qurrent's environment with a long-term view. Instead of forcing a standard testing model onto a non-standard architecture, they redesigned the pentest from scratch to suit their requirements.

Pentesting for Distributed AI Systems

ABOUT SOFTWARE SECURED

20%

of all vulnerabilities are critical or high

26

vulnerabilities on average per pentest

3X

more vulnerabilities found than the leading competitor

They recommended a targeted black-box network penetration test focused on the core elements required for SOC 2 and HIPAA. The goal was to validate the segmentation and ensure that no cross-customer access path existed.

In addition, Software Secured's manual greybox penetration testing was essential for the application layer. The testing process was efficient and straightforward. Qurrent only had to provide a staging URL and credentials; Software Secured handled the rest.

Software Secured also helped to educate the team. They clarified the limits of vulnerability scanning and explained how authenticated web testing validates customer isolation. By showing the engineering team how to interpret findings, they were enabled to prevent similar issues in future deployments.

During remediation, Software Secured established a dedicated Slack channel where Qurrent's developers could message the penetration testers directly. Within the Software Secured Portal, the Qurrent team added labels to the vulnerabilities, enabling easy delegation and unlocking clean workflows between DevOps and engineering. This created structure in a system originally built for speed.

Most importantly, Software Secured treated Qurrent's complexity as a feature of the business. Instead of overwhelming the team, they created a scalable testing model that could grow with every new deployment pattern.

> *"Software Secured thought about our infrastructure the same way we built it: flexible, powerful, and complex. They didn't force us into a box. They tested what mattered."* - ***DevOps Engineer***

Pentesting for Distributed AI Systems

Segmentation Controls for Infrastructure Security

Qurrent gained clarity about its infrastructure and segmentation controls. They validated their redesign and proved that customer environments were isolated and secure.

Achieving SOC 2 and HIPAA early in the company's history paid off immediately. One enterprise win turned into ten more within six months. Security questionnaires became predictable. The sales cycle accelerated because Qurrent could now answer every question with confidence, backed by a reputable pentesting company with deep manual testing experience.

By evaluating infrastructure decisions with long-term durability in mind, customer-level network isolation became a natural part of the evolving architecture. They were now empowered to anticipate and design for potential issues. The engagement reinforced confidence across both engineering and leadership. With a testing approach tailored to Qurrent's unique deployment model, the team gained a reliable, repeatable path for ongoing security validation.

Accelerated Enterprise Growth

Security investments produce measurable revenue impact. Qurrent can close more deals faster because its customers see a partner who takes product security seriously. Software Secured continues to support Qurrent's evolving needs, from authenticated web testing to deeper API assessments.

Long-term thinking turned any product risk into a competitive advantage. Qurrent has dependable systems, secure foundations, and protection that scales with every new deployment.

> *"Infrastructure decisions matter. Software Secured helped us catch risks early, validate our redesign, and build trust with every customer we onboard."*- ***August Rosedale, Co-Founder CTO***