Healthcare Provider Secures Sensitive Data with Continuous Penetration Testing

At A Glance

INDUSTRY Healthcare

COMPANY SIZE >300 employees

USE CASE Secure Third Party Applications

RESULT Clear Remediation Evidence & Faster Fixes

The Challenge

A prominent healthcare provider operating a network of clinics and hospitals relies on a third-party vendor to develop and maintain its public-facing application. The platform handles patient records, appointment scheduling, prescriptions, and sensitive medical data across a large user base.

Without direct control over the development process, the security team faced a compounding problem. Many of the application's functionalities were undocumented, making thorough vulnerability assessment difficult. Business logic flaws went undetected by traditional scanning tools, and coordinating remediation through an external vendor introduced delays that left gaps in the application's security posture for longer than acceptable.

Solution

The customer deployed Equixly to automate security testing across the application, mapping business logic flows and identifying vulnerabilities without requiring access to source code or documentation.

Equixly's findings were delivered with clear, contextual evidence that the security team could share directly with the third-party vendor, removing ambiguity from remediation, allowing the vendor to act immediately.

Outcome

Vulnerabilities that had previously gone undetected were surfaced and evidenced rapidly, accelerating remediation cycles and significantly reducing the time sensitive patient data remained exposed. The findings were specific, reproducible, and straightforward for the third-party to act on. With Equixly embedded into their security process, the customer moved from reactive vulnerability management to continuous assurance, ensuring their patient-facing platform remains secure as the application evolves.

© 2026 Equixly