HOW A HEALTHCARE SAAS PLATFORM MET STRICT BANKING SECURITY REQUIREMENTS WITH CONTINUOUS PENETRATION TESTING

Take Command

LOCATION

Texas

INDUSTRY

Insurance

EMPLOYEES

50-200

CUSTOMERS

Nystrom
Turn Community Services
Lycoming College

FUNDING

25 M

Take Command is a fast-growing healthcare technology company transforming how employers provide health benefits. The company supports more than 5,000 employers, brokers, and businesses across the U.S. Diligent security practices have enabled Take Command to scale, partner with regulated banks, and protect sensitive healthcare and financial data year-round.

From Annual Pentests to Continuous Audit Readiness

A new banking partner, a bare-metal rewrite, quarterly pentest mandates, and a hard deadline that mattered more than Black Friday were all happening.
The healthcare landscape was changing. Following the Affordable Care Act, employers started shifting away from traditional group plans toward Health Reimbursement Arrangements (HRAs). Take Command shifted to meet this change. They created a pre-reimbursement platform backed by banking infrastructure that allows employer funds to flow directly into individual accounts. The platform needed to withstand scrutiny from auditors, banking partners, and regulators while protecting sensitive personal and financial data at scale.
For years prior, annual, time-boxed penetration tests were enough. But as the platform evolved, Take Command rebuilt its system to tie directly into banking workflows that handle pre-reimbursement funds.

Most companies discover their security gaps after a partner says no.
Take Command chose to confront theirs before open enrollment.
The shift triggered new expectations. Quarterly penetration testing became mandatory. Internal network testing was required, and Pentesting partners now needed prior approval. SOC 2 Type 2 was required, and HIPAA controls were in scope. PCI was next.

Everything had to be secured, tested, and approved before open enrollment—the most critical period of the year. There was no flexibility. Any delay would block banking workflows and disrupt customers at a moment when reliability mattered most.

HOW A HEALTHCARE SAAS PLATFORM MET STRICT BANKING SECURITY REQUIREMENTS WITH CONTINUOUS PENETRATION TESTING

Beyond Checkbox Security

The intersection of healthcare data, financial transactions, and regulatory oversight raised the bar for security. For Take Command, penetration testing couldn't be a checkbox exercise. We needed to make it a continuous capability that keeps pace with the platform and partner expectations.
Software Secured aligned testing directly to the banking partner's requirements. This included quarterly gray-box application testing, internal network penetration testing across multiple environments, and deep validation of custom business logic. The engagement was structured as a subscription, shifting costs from capital expense to operating expense and removing friction around scope and scheduling.

The model supported how Take Command actually builds and ships software. Serverless environments were in scope, and weekly deployments continued without interruption. Testing took place in staging using de-identified data, protecting production workflows while preserving realism. Findings flowed directly into Take Command's existing processes, with evidence-backed reports that included screenshots, clear reproduction steps, and actionable remediation guidance. Jira integration reduced manual effort, while Slack enabled real-time coordination during active testing windows.

Unlimited retesting removed unnecessary pressure. Critical issues were addressed and validated ahead of open enrollment, while lower-risk findings could be scheduled without blocking compliance milestones. Just as importantly, documentation was always ready when partners asked for it. Lastly, security reviews never became a bottleneck because testing methodology, tester credentials, and approval letters were prepared in advance, ensuring delivery deadlines were always met.

Predictable Security Outcomes for a Growing Platform

With the new testing model in place, Take Command's CTO no longer worries about whether security will hold up under partner scrutiny. Testing reflects real-world expectations, eliminating last-minute surprises during audits and reviews. Vulnerabilities move cleanly into existing workflows, reports align with SOC 2 evidence requirements, and ongoing artifacts strengthen partner trust.

Planning has become simpler and more predictable. Multi-year pricing removed cost volatility, and quarterly testing no longer means renegotiating scope. Legacy systems are assessed with intention, without over-investing in platforms nearing retirement. Audit cycles are faster, evidence is consistent, and reporting language aligns with auditors' expectations. Most importantly, security now supports the business instead of competing with it. Testing enables product launches, remediation aligns with the roadmap, and open enrollment stays on schedule.

HOW A HEALTHCARE SAAS PLATFORM MET STRICT BANKING SECURITY REQUIREMENTS WITH CONTINUOUS PENETRATION TESTING

Building Long-Term Security Confidence with Banking Partners

Take Command entered open enrollment with confidence. The new platform was tested and remediated before peak traffic, and the banking partner requirements were met ahead of schedule. Quarterly penetration testing is now part of normal operations. SOC 2 Type 2 compliance is maintained with less effort. HIPAA controls are supported. PCI readiness is underway.

Security is planned and repeatable. It scales with the business.

> *"Software Secured helped us incorporate a security program we are proud of.."*
> ***Senior Director of Engineering***

Take Command now treats penetration testing as a long-term partnership, not a yearly task. That shift enables growth in a regulated market where trust, uptime, and security determine who gets to move forward.