

CASE STUDY

A Leading Precision Medicine Company Chooses Ridge Security to Secure Its Applications Before They Reach Production

Ridge Security Technology Inc. www.ridgesecurity.ai

©2026 All Rights Reserved Ridge Security Technology Inc. RidgeBot is a trademark of Ridge Security Technology Inc.

The Customer

A publicly traded U.S. leader in genetic testing and precision medicine, the company serves patients, clinicians, and biopharma partners. Fortune named it to the 2026 Future 120, its ranking of the companies best positioned for long-term growth.

Its patient and clinician portals, therapeutics and real-world data applications, mobile services, and APIs all handle sensitive health data, and each one is a potential entry point for attackers.

The Challenge

The company ships new applications and API updates continuously. Each release risks exposing protected health information (PHI) if an exploitable flaw slips through. That risk is higher in healthcare. The U.S. designates healthcare as critical infrastructure, and attackers target it because patient and genetic data is valuable and disruption is costly. One breach can halt clinical operations, delay results to patients, and damage trust with clinicians and partners.

The company also works under heavy regulation. HIPAA governs how it protects PHI, and state privacy laws add requirements for genetic data.

Auditors and partners want evidence that security controls work, not long lists of possible weaknesses.

The security team needed proof of which API and web app vulnerabilities attackers could actually exploit.

The supply chain adds complexity. APIs link the company to biopharma partners, labs, clinicians, and third-party services, and every connection widens the attack surface. Acquisitions widen it further. Inherited applications, infrastructure, and internet-facing assets arrive with unknown security posture and must be assessed quickly, before they are integrated.

To keep up, the team needed to test earlier, in development, staging, and pre-production, before go-live. It also needed validated findings to reach developers fast, inside the workflow they already use.

By the Numbers

100
Web applications tested

1,000+
Assets tested

6x
More frequent testing, biweekly instead of quarterly

80%
Faster meantime to remediate

How Ridge Security Solved It

Challenge	RidgeBot Solution	Result
Continuous releases New apps and API updates ship constantly. Flaws found after go-live leave PHI exposed longer and cost more to fix.	**Dynamic Web Pentesting** Attacks running apps in dev, staging, and pre-prod. Proxy support reaches non-public environments.	Testing shifted left. Exploitable flaws are caught before release.
Proof for regulators HIPAA and state genetic privacy laws require evidence that controls work. Lists of possible weaknesses don't satisfy auditors or partners.	**Exploit-Based Validation** Each finding is confirmed by safely exploiting it, with proof of exploitability attached.	Clear evidence for auditors and partners, not noise.
Partner and supply-chain APIs APIs connect the company to biopharma partners, labs, and third-party services. Scanners couldn't prove what was exploitable.	**API Security Testing** Exploits and validates weaknesses in internal service, inventory, and data insights APIs.	Real API risks closed before release, with evidence attached.
A targeted, growing attack surface Healthcare is critical infrastructure and a primary target. Acquisitions add internet-facing assets with unknown security posture.	**Attack Surface Assessment** Maps and tests external assets, including inherited ones, for exploitable exposures.	Exposures closed before attackers reached them. Acquired assets assessed before integration.
Slow handoffs Findings sat in reports instead of developer queues.	**Jira Cloud Integration** The DevSecOps Connector syncs validated findings to the right Jira projects and workflows.	Remediation starts immediately, in the tool developers already use.

What RidgeBot Tested

Web Applications

- Patient and clinician portals
- Therapeutics applications
- Real-world data platform
- Mobile services
- Analytics dashboards
- Corporate website

DEV STAGING PRE-PROD PROD

APIs

- Internal service APIs
- Inventory API
- Data insights API

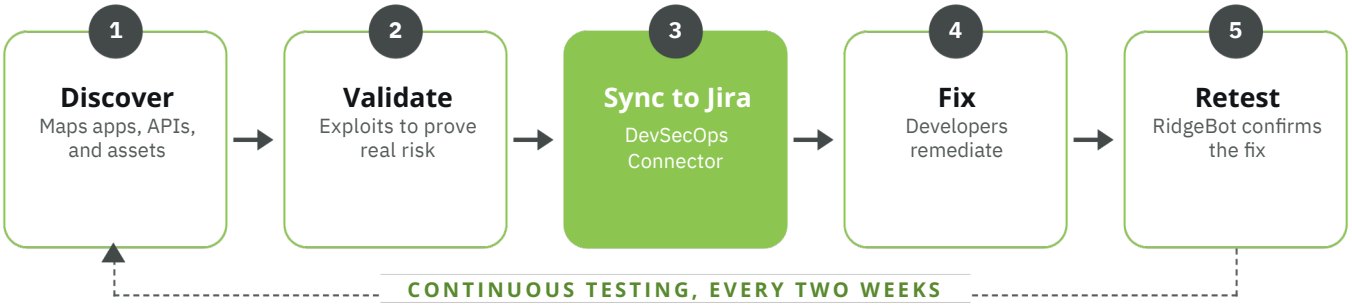
DEV PROD

External Attack Surface

- Internet-facing assets
- Exposed services

EXTERNAL

Validated Findings, Straight to Developers



The Jira Cloud integration is the core of the company's remediation workflow. Every finding RidgeBot validated became a tracked Jira issue, with proof of exploitability attached.

Ridge Security supported the rollout with recurring technical reviews, health checks, and upgrade guidance. The team also connected RidgeBot to its existing vulnerability management platform via API.

The result: testing moved from quarterly to every two weeks, developers received validated findings with proof attached, and mean time to remediate fell by 80%.

> "As a critical pillar in our AI-first cybersecurity transformation strategy, Ridge Security has played a crucial role in helping our team identify, prioritize, and manage attack surfaces through its sophisticated automated penetration testing capabilities, keeping our defenses ahead of adversaries."
>
> *Chief Information Security Officer, Leading Precision Medicine Company*