USE CASE

How a Medical Device Manufacturer Made Security Testing Continuous

Across Network, Web and API Assets

Summary

Medical device manufacturers operate estates that change faster than an annual or semi-annual assessment cycle can describe. Exposure concentrates in the interfaces connecting systems to suppliers, clinicians, and cloud platforms, and conventional testing scopes are often thinnest precisely there. By bringing testing in-house, this manufacturer replaced a twice-yearly report with a capability their own team operates, extended coverage from a negotiated sample to networks, websites, and APIs across the estate, and closed the gap between discovering an exploitable risk and confirming that they fixed it.

© 2026 All Rights Reserved Ridge Security Technology Inc.

The threat environment

Medical device manufacturers operate estates that change faster than an annual or semi-annual assessment cycle can describe. Exposure concentrates in the interfaces connecting systems to suppliers, clinicians, and cloud platforms, and conventional testing scopes are often thinnest precisely there. By bringing testing in-house, this manufacturer replaced a twice-yearly report with a capability their own team operates, extended coverage from a negotiated sample to networks, websites, and APIs across the estate, and closed the gap between discovering an exploitable risk and confirming that they fixed it.

BREACH CAUSE

53%

Of healthcare breaches are attributed to system intrusion, which has overtaken human error as the most common pattern.

API EXPOSURE

70%+

Annual API breach rate reported for healthcare — one of the two highest of any sector, alongside financial services.

EXPLOITED VULNS

43%

Of vulnerabilities added to CISA's Known Exploited Vulnerabilities catalog in a recent 12-month period involved an API surface.

EXPLOIT EASE

97% / 59%

Of examined API vulnerabilities were exploitable with a single request, and required no authentication at all.

COST IMPACT

$7.42M

Average cost of a healthcare data breach — the highest of any industry for fourteen consecutive years.

Sources: Verizon Data Breach Investigations Report, healthcare sector data. Wallarm, The 2026 API ThreatStats Report. IBM Cost of a Data Breach Report.

The pattern behind these figures matters as much as the figures themselves. Exposure concentrates in the interfaces that connect systems to one another, and the business continuously adds those interfaces as it grows. Fixed annual or semi-annual testing schedules cannot keep pace with an estate that changes at a different rate.

© 2026 All Rights Reserved Ridge Security Technology Inc.

Organizational context

A North American medical device manufacturer manages approximately 1,000 IT assets across corporate network infrastructure, public-facing websites, and APIs. Their estate supports connected products, third-party supplier integrations, and cloud services, and it changes continuously as teams release applications, add integrations, and expose new API versions.

For several years, an external firm tested security twice a year to meet a compliance requirement. The work was sound, but the arrangement could not keep pace with an estate that changed weekly because the capability sat outside the organization. Every question required a scope, a schedule, and a commercial conversation, so the team never asked most questions at all.

BEFORE

TWICE A YEAR

External firm, scoped per engagement.

→

AFTER

WITHIN DAYS

In-house, event-driven, continuous.

© 2026 All Rights Reserved Ridge Security Technology Inc.

Ridge Security solution

The manufacturer moved its entire security testing operation in-house with Ridge Security's AI-based continuous security validation solutions. The team evaluated several automated offensive security products and selected Ridge Security because it gave them the most complete picture across networks, websites, and APIs rather than depth in a single asset class.

The change did more than increase testing frequency. It gave the team the ability to initiate testing the moment a question arose. They now run tests when a new threat emerges, when they publish a new application, when a third-party supplier system connects to the environment, and when they introduce or version a new API. Previously, each of those events created exposure that remained untested until the next scheduled window.

Ridge Security tracks the CISA Known Exploited Vulnerabilities catalog and releases test scripts for current threats every other week. When an exploit moves from theoretical to active use in the wild, the team can determine within days whether it reaches their estate.

DEPLOYMENT & DATA PRIVACY

Ridge Security deploys inside the customer environment, testing internal network segments, internal applications, and non-public APIs on the same terms as external assets. Test data, exploit evidence, and reports stay on the customer's own infrastructure — never transmitted to Ridge Security or anywhere else.

© 2026 All Rights Reserved Ridge Security Technology Inc.

Areas of testing focus

The team tests across three domains, while a fourth capability defines what belongs in scope.

DEFINES SCOPE

ATTACK SURFACE DISCOVERY

Runs across the asset range and identifies what's actually reachable — open ports, hosted websites, responding URLs and API endpoints. The gap between a documented inventory and a reachable one is where most unexamined exposure sits.

HOST PENETRATION TESTING

WINDOWS LINUX NETWORK DEVICES DB SERVERS APP SERVERS

Ongoing hygiene across the estate, plus immediately when a relevant exploit enters active use.

WEBSITE PENETRATION TESTING

PUBLIC-FACING SITES INTERNAL WEB APPS

Tested both black-box and authenticated. Runs on every app release, plus a recurring cycle.

API SECURITY TESTING

GET POST PUT REPEAT

Reports against the OWASP API Security Top 10. Runs on every new API or version.

The team keeps testing production-safe and schedules it into defined windows. They save and reuse task configurations, so a release test or supplier onboarding test repeats a known configuration instead of requiring a fresh scoping exercise each time. The annual license places no cap on the number of tests, which makes event-driven testing workable in practice rather than only in principle.

© 2026 All Rights Reserved Ridge Security Technology Inc.

The Ridge Security advantage

Among the test types they use, API testing produced the findings the team considered most consequential. It surfaced severe, exploitable risks on interfaces they previously could not see at all. The customer keeps the specific findings confidential because Ridge Security solutions run on their premises.

RISK COVERAGE

EXPOSED PII | BROKEN ACCESS & AUTHORIZATION | ACCOUNT TAKEOVER | DATA & SESSION HIJACKING | CODE DISCLOSURE | WEAK OR REUSED CREDENTIALS

Ridge Security solutions give the team visibility and support fast remediation for risks including exposed personally identifiable information, broken access and authorization, account takeover, data and session hijacking, code disclosure, and weak or reused credentials. The platform establishes whether an asset can actually be exploited rather than only whether a vulnerability is present, and it shows the exploit path and kill chain instead of inferring risk from a version number. That distinction determines what the team fixes first because prioritization reflects real exposure in their specific environment rather than a theoretical severity score.

The platform maps findings to the OWASP Top 10 and OWASP API Top 10 — frameworks the development teams already work in — and routes results into existing tooling rather than creating a separate artifact.

DEV WORKFLOW

Jira | GitLab | ServiceNow

VULNERABILITY MANAGEMENT

Rapid7 | Tenable | Qualys

Because the license does not cap test volume, the team can retest a remediation immediately and confirm that they closed it rather than mark it resolved and revisit it months later. The loop from discovery to verified fix runs in days and stays inside one team, turning remediation from an assertion into a demonstrated result.

© 2026 All Rights Reserved Ridge Security Technology Inc.

Extending coverage to business logic risk

Continuous testing across the estate establishes what is exposed and what the team can patch. It does not establish whether something works exactly as designed and is still dangerous.

Alongside CVE-based risk, Ridge Security's agentic platform identifies business logic flaws and misconfigurations by reasoning through multi-step attack chains the way a human red team would. It runs bounded, production-safe engagements against one authorized target at a time. Its dual-agent architecture separates the agents that probe from independent agents that reproduce every finding before the platform surfaces it, so the platform rejects results it cannot evidence. For remediation, Ridge Security's agentic platform gives security teams specific steps to resolve each issue in its actual context, which matters most for flaws that have no vendor advisory behind them.

In a medical device manufacturer's estate, that lets the team answer questions no CVE list can answer:

1. *Can a distributor account reach another distributor's order history or pricing?*
2. *Can a clinician account retrieve records outside its own care relationship?*
3. *Can someone replay device registration or enumerate serial ranges?*
4. *Can an attacker make a multi-tenant cloud platform leak across tenant boundaries?*
5. *Can a connected supplier system use a trust relationship to move further into the estate than it was ever authorized to go?*

Each scenario chains together individually reasonable steps that end somewhere unreasonable, and CVE-based testing will not surface them because nothing in the chain is technically broken.

© 2026 All Rights Reserved Ridge Security Technology Inc.

About Ridge Security

Ridge Security empowers CISOs to build cyber resilience through AI-native continuous offensive security. By helping organizations continuously validate their security posture, focus on proven cyber risks, and accelerate remediation, Ridge Security enables security teams to stay ahead of evolving threats while maximizing the effectiveness of their existing security investments. Recognized by Gartner and Frost & Sullivan, Ridge Security serves enterprises worldwide across financial services, government, telecommunications, and other critical industries.

Ridge Security Technology Inc.
https://ridgesecurity.ai/
© 2026 All Rights Reserved Ridge Security Technology Inc.

Follow us online

© 2026 All Rights Reserved Ridge Security Technology Inc.