nagomi

CUSTOMER STORY

How Redis Replaced 2.5 Months of Threat Mapping With One Live View.

See how Redis uses the Nagomi Agentic Exposure Ops Platform to replace months of manual threat analysis with continuous, control-first visibility from Nagomi.

INDUSTRY	Real-Time Data Platform
CHALLENGE	Redis's lean security team was spending months manually mapping defensive controls to threats every time the business asked "are we protected?" A 2.5-month effort to answer that question across the top 10 threats was already out of date by the time it was finished.
SOLUTION	Redis deployed Nagomi to continuously correlate signals from CrowdStrike, Wiz, and the rest of the stack against a live threat model — delivering real posture answers in seconds instead of months.
RESULTS	◆ Replaced a 2.5-month manual threat-mapping exercise with a live view ◆ Recovered 1.5 months of engineer time from an abandoned internal build ◆ A single view of posture across every tool the team already runs ◆ Daily scanning so posture changes show up the day they happen ◆ Agent-driven answers grounded in live data, with every finding traceable

01 / 03 THE CHALLENGE

A lean team, a growing stack, and a question that took months to answer.

Redis is a real-time data platform trusted by enterprises worldwide. Justin Lachesky leads Cyber Resilience, one of three functions inside Redis's security organization, covering security architecture, engineering, and all of threat detection and response.

The team is lean by design. Redis decided long ago that scaling to 20 or 30 security engineers was not the path. It would lean on technology instead. The team ran CrowdStrike, Wiz, and a stack of other defensive tools across cloud workloads and employee endpoints. Each tool produced signals, none of them answered the question the business kept asking.

"Are we protected from this threat actor?" Every time a new name hit the news, the question came back. And every time, the team had to do the work by hand: research the threat, map the TTPs into MITRE ATT&CK, cross-reference every tool, every feature, every setting, and build the picture one data point at a time.

When the CISO asked for a broader answer, a real posture view across the top 10 threats, the team took the assignment on. It took **two and a half months** to pull everything together. Fighting JSON formats. Manually linking defensive capabilities to threats across platforms. By the time the picture was ready, it was out of date. Controls had shifted. Posture had changed. The team had to start over.

The cost of building it themselves

WEEK 0

The ask

CISO requests posture across Redis's top 10 threat actors and campaigns.

WEEKS 1–10

2.5 months mapping by hand

Threats researched, TTPs mapped to MITRE ATT&CK, every tool cross-referenced.

WEEK 11

Stale on arrival

Controls had shifted. Posture had changed. The team starts over.

WEEKS 12–17

In-house build, then shut down

A 1.5-month internal correlator works — but is too expensive to keep running.

02 / 03 THE SOLUTION

One live view across every tool the team already runs.

When Nagomi was brought in, integration was simple. Every tool Redis already ran had a native connection. API token, service account, and the data flowed.

Once the data was in, the team went to the attack mapping page and loaded their top 10 campaigns. The full MITRE ATT&CK framework appeared with every tactic scored against the real configuration. One click drilled into any tactic to see the tests behind the score, each test tied to live data pulled from the platforms the team already trusted. With Nagomi's daily scanning, the platform provided a living view, fresh data meant the team could act on what they saw the day they saw it.

BEFORE NAGOMI

Months of manual work, stale by delivery.

- — 2.5 months to answer one posture question
- — 1.5 months building (then shutting down) an in-house correlator
- — Snapshots out of date the day they shipped
- — Coverage gaps surfaced only by coincidence

WITH NAGOMI

A living view, always grounded in live data.

- + Top-10 threat posture as a default view
- + Daily scanning catches posture changes the day they happen
- + Every tactic score traceable to a real test in a real tool
- + Defensive plans turn into a repeatable cadence

> *"Nagomi helped us address the unknown. It gets so hard to make decisions when you don't have ground truth. Nagomi made it a lot easier for us to get that ground truth across the whole stack."*
>
> **Justin Lachesky**
> Director of Cyber Resilience, Redis

Ground truth across the stack

The defensive plan workflow has become a repeatable cadence. Nagomi surfaces specific improvements that would raise posture against the threats the team cares about most. The team works through them, makes the configuration changes, and watches the score update when the daily scan runs. Endpoint coverage gaps that once surfaced by coincidence now surface in near real time.

03 / 03 RESULTS & WHAT'S NEXT

Decisions that were too expensive to make are routine now.

2.5 mo
Manual threat-mapping replaced with a live view

1.5 mo
Engineer time recovered from an abandoned internal build

Daily
Scanning cadence — posture changes show up the day they happen

Looking to the future

Going forward, Redis plans to extend Nagomi further into exposure management and agent-driven remediation. The team is already exploring how the Nagomi agent can scale them faster — not just in answering questions, but in connecting findings to action. Ticketing integration and exposure prioritization sit on the near-term roadmap.

For a lean security team, Nagomi has changed what is possible. Redis had ground truth on individual tools before. It did not have ground truth across them. Now, the picture is connected, and decisions that were once too expensive to make are routine.

Redis's experience underscores what security leaders with lean teams have been saying for years. The problem is not a lack of tools. The problem is the work between them. **Close that gap, and everything else gets easier.**

About Nagomi

Nagomi is the Agentic Exposure Ops Platform designed to prevent the preventable breach. In an era where security teams are consumed by tool fragmentation and manual validation, Nagomi provides the unified operating model necessary to close the gaps between detection and remediation. By aligning existing tools, teams, and intelligence into a single coordinated system, Nagomi's agents automate the investigation of exploitable risks, trigger precise remediation workflows, and continuously verify that exposure remains eliminated. We don't just find gaps. We end them. Recognized by Gartner as a Cool Vendor, Nagomi is a pioneer in Automated Security Control Assessment (ASCA), helping organizations move beyond fragmented dashboards to a state of strategic harmony — restoring operational capacity and ensuring defense effectiveness at scale.