

2026

How A Fortune 1000 Consumer Technology Company Replaced Four Detection Tools With One Platform And Cut False Positives In Half

CUSTOMER STORY





A cloud-native consumer technology company unified disjointed point products, siloed workflows, and eliminated legacy SIEM costs with the Vega Agentic Cyber Defense platform.

With Vega, The Cyber Defense Team Achieved:

1,168 detections operational across 50 data sources. Mapped to MITRE ATT&CK, firing every 5 minutes versus the prior 60-minute baseline, with zero engineering effort.	50% False positive volume cut by half through continuous detection tuning and AI-assisted triage.	4 → 1 Four tools down to one platform Detection, search, dashboarding, and investigation now run in place on a low-cost Amazon S3 bucket.
--	---	---

INDUSTRY Consumer technology, fitness, and health	SIZE ~3,500 employees, Fortune 1000	REGION North America
USE CASES SIEM replacement, AI SOC, Cloud Detection and Response, Threat Intelligence	PAIN POINT four tools, no shared analytics layer, and executive scrutiny across every dollar	



The Challenge

FOUR TOOLS, AND NOTHING THAT TIED THEM TOGETHER

Detection ran as four separate products rather than one operating model: two stacks carrying detection logic, an outsourced MDR for response, and a standalone automation tool. No analytics or search layer connected them, and the MDR covered only part of the telemetry, so visibility stayed in pieces.

That architecture fit a smaller estate that fractured as the environment grew across dozens of data sources. The team had nowhere to hunt, build a dashboard, or run an ad-hoc query across everything at once. EKS and Google Cloud carried no detection coverage, which meant adversary activity in either would produce no alert. Detection engineering depended on SQL fluency the broader team did not have, so every new rule queued behind two individuals and time to detect stretched with the queue.

Cost is what carried the problem to the executive team. The CEO and CFO had put security tooling spend under review, and four products stitched together were consuming the budget that would have closed the visibility gaps. Attrition and the absence of a dedicated detection engineering function left the capability fragile on top of that.

The Solution

WORK THE DATA IN PLACE WITH AGENTIC CYBER DEFENSE

Two criteria decided the evaluation. The platform had to arrive with at least 80 percent pre-built detection coverage across the team's existing sources, and total cost had to land at or below current detection spend.

The telemetry already sat in the company's own S3 bucket. Vega indexes in place, where the customer chooses to keep it, normalizes it to OCSF, and correlates it across sources. Nothing was re-ingested or moved to a costly, complex data lake or legacy SIEM.

On top of that data, Vega runs the agentic loop of detection, triage, investigation, and optimization for better, faster cyber defense. Natural language converts to KQL, which is what took detection authoring off the SQL bottleneck. Out-of-the-box detections covered the company's sources on day one. The AI Incident engine correlates related alerts into a single contextual incident instead of leaving a queue of isolated signals. Vega connects directly to the team's existing automation platform, Slack, and MCP, ensuring rapid time to value.



The Outcome

A PURPLE TEAM EXERCISE THAT VEGA CAUGHT BEFORE ANYONE REPORTED IT

During a live purple team exercise, Vega detected red team activity across IAM, S3, and CloudTrail in near real time. The Vega engine correlated three or more separate alerts into one contextual incident and surfaced adversary behavior the team had not yet identified by hand.

Now, the deployment operates on more than 2 TB of telemetry per day across 50-plus data sources with 1,168 detections firing every 5 minutes. False positive volume is half what it was, counted as alerts the team classifies as false before and after. Detection engineering now runs on one source of truth, authored by analysts rather than queued behind SQL expertise, for less than the incumbent renewal would have cost.

