

2026

How A Fortune 100 Pharmaceutical Company Turned A 17-Query Global Investigation Into One

CUSTOMER STORY





With Vega, The Cyber Defense Team Achieved:

17

**AWS regional queries
down to one**

A global investigation once meant searching every region separately and reconciling the results by hand.

535+

**TB of data indexed across
66 S3 buckets**

1.27+ PB of uncompressed data were indexed in place across 17 AWS regions, with nothing centralized into a SIEM.

30

**CloudTrail detections across
9 MITRE ATT&CK tactics**

Seven rated Critical, against a prior state of zero detection coverage on more than 6 TB of daily cloud telemetry.



INDUSTRY

Global pharmaceutical and biomedical sciences



SIZE

100,000+ employees, Fortune 100, operations in 150+ countries



REGION

Global, with analysts in the US, Europe, and MEA



USE CASES

SIEM augmentation, AI SOC, Cloud Detection and Response, Threat Intelligence



PAIN POINT

one investigation, seventeen times



The Challenge

THE ESTATE GREW PAST WHAT CENTRALIZING COULD HOLD

The team operates a globally distributed AWS environment across 17 regions generating more than 6 TB of cloud logs daily, alongside endpoint tooling, a growing SaaS security stack, and Microsoft Sentinel. The detection architecture assumed every log could be ingested to one location, introducing unsustainable cost and complexity with a legacy SIEM.

Day to day, analysts queried all 17 regions one at a time. A single global investigation became up to 17 sequential searches reconciled by hand, then repeated in each separate tool, putting real-time global hunting out of reach. Threat intelligence stopped at the report: nobody could trace whether one had ever produced a detection or an investigation.

The detection library was the last constraint. All 75 cloud detections were written in SPL, a query language that belonged to the legacy SIEM and did not fit an in-place analytics strategy. Without moving the AWS data into that SIEM, which cost had already ruled out, none of the 75 could run against the company's cloud data.

The Solution

QUERY 17 REGIONS IN PLACE WITH VEGA

One requirement decided the evaluation: run one query across all 17 AWS regions without centralizing the data. The platform also had to index 6+ TB per day cost-effectively on an object-store-first architecture, index three years of history, connect to Microsoft Sentinel and Wiz for cross-source correlation, and offer granular RBAC.

The logs already sat in the company's own S3 buckets. Vega indexes them there, in place, where the customer chooses to keep them. The Vega platform executes access and queries next to the data in each region, coordinated as one system through a scoped cross-account role. The result is in-place analytics across every region and every repository, addressed through a single KQL interface, without the egress and storage cost of the alternative.

On that foundation Vega runs the agentic loop of detection, triage, investigation, and optimization for better, faster cyber defense. The agents travel to the data, and the verdicts come home to the analyst. Natural language converts to KQL, which is how detection engineering moved off SPL without retraining the team. A curated cloud detection library covered the company's AWS sources, and pairing it with in-place analytics retired a separate license carried purely for cloud anomaly detection.



The Outcome

VEGA BECAME THE STANDARD FOR EVERY CLOUD TELEMETRY REPOSITORY

Vega is now the company's standard platform for query and detection across all cloud telemetry. It has indexed 535+ TB, 1.27+ PB uncompressed, across 66 active S3 buckets spanning CloudTrail, VPC Flow Logs, AWS Config, CloudWatch, GuardDuty, and DNS query logs.

The team enabled 30 CloudTrail detections across nine MITRE ATT&CK tactics, seven rated Critical, on cloud data that had carried no detection coverage at all. Security engineers in the US, Europe, and MEA now run daily investigations across AWS Bedrock, CloudTrail, and CloudWatch, on roughly 6 TB of new telemetry a day, and an analyst with one question about the global estate asks it once.

