vega

Target ICPs for Channel Partners - March 2026

Who We Sell To

Two lanes — same qualifying signals, different company profiles

LANE 1: Large Enterprise

20,000+ employees
Established security organization
Multi-year, multi-million-dollar deal sizes
Budget for multi-vendor security stack

LANE 2: Cloud-Native, Security-Mature

2,000–20,000 employees
Stack complexity outpaces headcount
Cloud-native, modern data pipelines
Faster cycles, early AI/automation adoption

SHARED QUALIFIERS (BOTH LANES)

Internal security team (3-4+) • Multi-cloud or AWS-primary • Large data volumes • Tech-forward • Non-government

SIEM Landscape Targets

Where we compete — and what we displace

TIER 1 — Strongest Fit

Splunk • Microsoft Sentinel • Elastic

Federation, augmentation, and full displacement validated in active opportunities

TIER 2 — Proven Displacement

Datadog SIEM • Exabeam • Hunters.ai • Anvilogic • SentinelOne

Current active engagements displacing these products

EMERGING — Competitive Targets

CrowdStrike NGSIEM • 7AI • CardinalOps • SentinelOne Data Lake

Appearing in head-to-head evaluations and multi-vendor RFPs

Qualifying Pain Signals

If you hear these from a prospect, they're in our ICP — regardless of company size

SIEM Displacement in Progress

Actively frustrated with their current SIEM — cost, capability, or vendor trajectory. Looking to replace, not just augment.

Stranded Security Data in S3

CrowdStrike FDR, EDR, or other telemetry sitting in S3/object storage — unqueried or with minimal retention (2-3 days).

Detection Engineering Gap

Team owns detection engineering but current vendor pivoted away from it. MITRE coverage gaps creating audit or compliance pressure.

Dual-SIEM Cost Pressure

Running two SIEMs during migration or legacy overlap. CFO/CIO pushing to consolidate. Renewal within 6-12 months.

What Opens the Door

The features and motions that generate the most interest with prospects

TOP-OF-FUNNEL FEATURES

MITRE Assessment
Detection gap analysis against MITRE ATT&CK. Consistently the strongest first impression across deals.

Federated Multi-Source Query
Single KQL query across Splunk + S3 + EDR + cloud. The decisive differentiator in POVs.

CrowdStrike FDR + S3 Unlock
Query stranded EDR data in S3 that was previously inaccessible. Immediate value.

AI Triage
Auto-correlate and contextualize alerts. Live in production at Instacart.

COMMERCIAL ACCELERANTS

AWS Marketplace / PPA
Vega deal counts toward existing AWS commit. 5-year PPA customers are ideal.

Upcoming SIEM Renewal
Renewal within 6-12 months creates urgency and budget event.

Channel Partner Intro
Warm introduction from trusted SI or VAR accelerates procurement.

API-First / Automation
Teams building SOAR/automation workflows value Vega's API extensibility.

Quick Reference: Is This Account In Our ICP?

CHECK THESE BOXES:

- Internal security team (3-4+ people)
- Multi-cloud or AWS-primary
- Running any Tier 1 or Tier 2 SIEM
- Large data volumes (TB/day or 50+ sources)
- Tech-forward, non-government

BONUS SIGNALS (PRIORITIZE):

- Actively unhappy with current SIEM
- CrowdStrike FDR / EDR data in S3
- MITRE coverage gaps / audit pressure
- AWS PPA / Marketplace alignment
- SIEM renewal in next 6-12 months
- Hitting SIEM ingestion limits due to cost

TWO LANES: Lane 1 = 20K+ employees (traditional enterprise) | Lane 2 = 2K–20K employees (cloud-native, security-mature)
Both lanes qualify if they have the stack complexity, security team, and data volume. Don't disqualify on headcount alone.

When in doubt, give us a shout. We'd rather qualify quickly than miss a deal. Reach out to your Vega AE.


Thank You!
vega