Building an Enterprise Security Fabric with Agentic Ai

Combined company case, market need, and technology foundation.

Go-Forward Business Plan

COMMERCIAL ROUTE
Lead commercially oriented Shield sales and support through the VigilAigent team and brand.

TECHNOLOGY INTEGRATION
Embed selected Shield capabilities to improve effectiveness, speed alert resolution and reduce false positives.

IMMEDIATE SYNERGY
$3 million in annual cost-of-doing-business savings identified and implemented across the organizations.

Why the Market is Changing

CUSTOMER AND THREAT PRESSURES

- Customers want more visibility, fewer tools, and one integrated ecosystem.
- Ai-enabled attacks move too quickly for human-only security operations.
- Gaps between disconnected tools create room for attackers to evade detection.
- Organizations also need visibility into authorized Ai, shadow Ai, and misuse of legitimate Ai tools.

THE COMBINED RESPONSE

- A security fabric that ingests telemetry from across the enterprise attack surface.
- Intrusion Shield technology adds network visibility and enrichment that can expose activity other tools miss.
- An open ecosystem designed to incorporate existing tools and customer data.
- A common back end intended to support scalability and reduce integration-management costs.

The VigilAigent Platform

THE ORACLE™
The core of the agentic digital workforce. It sees, decides and acts—escalating to humans or initiating response.

OMNIVIZ
Correlates telemetry, tickets, customer context, analyst knowledge and external enrichment in one investigation view.

INTRUSION SHIELD
Adds proprietary intelligence, network-level prevention and agentless coverage for IoT, critical infrastructure and AI activity.

Why Machine-Speed Decisions Matter

THE ORACLE IN PRODUCTION

The ORACLE has been trained on more than one billion events per day and is designed to shorten the time from detection to conclusion; because attacker breakout can occur in minutes or even seconds.

SCALE
1B+
events analyzed each day

SPEED
2:37
average decision time

ECONOMICS
99%
cost reduction per alert

SYNERGY
$3M
annual savings implemented

Intrusion + VIGILAiGENT™

Building an Enterprise Security Fabric with Agentic Ai

Combined company case, market need, and technology foundation.

What the Demonstration Showed

1. INGEST
Bring telemetry and alert data into OmniQueue.

2. CORRELATE
Add customer history, prior tickets, data-lake evidence and external intelligence.

3. DECIDE
Use task-specific sub-oracles and verification agents to reach a confidence-scored conclusion.

4. ACT
Close, escalate, contain, tune a rule or launch an automated workflow.

INVESTIGATION & GOVERNANCE

- Transforms difficult raw alert data into a step-by-step analyst recommendation in seconds.
- Maintains detailed audit trails, job status, token use, cost, and decision rationale.
- Searches historical alerts, prior analyst notes, users, IP addresses, and rules across the data lake.
- Captures analyst feedback to continuously improve the decision engine.

AUTONOMOUS RESPONSE AND WORKFLOW CREATION

- Can recommend rule tuning, filters, scripts and response actions.
- Built a workflow to disable a compromised user, create a ticket and notify stakeholders.
- Generates reviewable code and suggested tests, with development-team quality control before production.
- Compresses workflow development that could take hours, days or weeks into minutes.

Demonstrated Operating Leverage

VOLUME	PROCESSING	HUMAN EQUIVALENT	PRODUCTIVITY
4,436	**$276**	**$24K–$50K**	**10–20X**
ORACLE jobs in 7 days	reported cost for those jobs	management labor estimate	estimated analyst capacity

Commercialization Opportunities

EXPAND MANAGED SERVICES
Use the combined platform to deepen enterprise and MSP relationships and expand revenue from existing partners and customers.

LICENSE THE DIGITAL WORKFORCE
Integrate agentic investigation and decision capabilities directly into third-party platforms without requiring the full MDR service.

PLATFORM PARTNERSHIPS
Management cited a planned test with Google Security Operations and a second-stage opportunity with a legal-technology company.

AI + AGENTLESS SECURITY
Address authorized Ai, shadow Ai, malicious use of legitimate tools, IoT and critical infrastructure through network visibility.

DATA LICENSING
Create additional monetization opportunities from proprietary cyber intelligence and data.

ORGANIC + INORGANIC GROWTH
Use a common back end, non-linear SOC staffing and an expanding distribution network to improve growth and acquisition economics.

Key Investor Takeaway

For current and potential investors, the combination of Intrusion and Vigil**Ai**gent presents a financial opportunity centered on revenue growth, margin expansion and operating leverage. The integration of proprietary threat intelligence, agentic Ai and an established commercial channel creates the potential to grow recurring and higher-margin revenue, reduce the cost of alert investigation and response, and scale the business without a proportional increase in security-operations headcount.