AGENTIC SOC SOLUTION BRIEF

Agentic SOC

Stop Fighting AI-Powered Threats with Human-Speed Security Operations.

98%
AI Autonomy
Alert triage handled by AI agents from Day 1.

30x
Detection Coverage
Behavioral observability across your entire attack surface.

50%+
Cost Reduction
Fewer tools, lower spend, stronger security posture.

3 min
Mean Time to Triage
Alert to investigation — guaranteed SLA.

Powered by

Google Security Operations | **Netenrich Resolution Intelligence Cloud™**

Google Cloud
SECURITY
Partner of the Year
Managed Security Service Provider North America
2026

THE CHALLENGE

The Threats Have Evolved. Your SOC Hasn't.

Today's adversaries are not humans targeting brands—they are **autonomous bots operating at machine speed**, continuously scanning for exposed assets across cloud, identity, and endpoints. Phishing-as-a-Service kits bypass MFA in seconds. AI-driven reconnaissance maps your environment silently. Zero-day automation exploits ghost assets before your IT team knows they exist.

Autonomous Bots
Scanning for exposed assets at machine speed.

PhaaS Kits
Bypass MFA in seconds, at scale.

AI Reconnaissance
Maps your environment silently.

Zero-Day Automation
Exploits ghost assets before IT knows.

THE FATALITY GAP

TIME TO COMPROMISE VS. TIME TO RESPOND

<25 min — Attacker: full network encryption

60 min — Legacy SOC: still opening a ticket

0% **Manual SOC success rate against autonomous malware.**

TRADITIONAL VS. AGENTIC

What Does 'Agentic' Actually Mean?

TRADITIONAL / LEGACY SOC	NETENRICH AGENTIC SOC
Human triage (hours to days)	◆ Machine-speed AI (< 3 minutes)
Passive alerting & monitoring	◆ Continuous decisioning & readiness
Tool-centric, manual workflows	◆ Agentic, outcome-driven execution
Precision detections opening up blind spots	◆ Behavioral observability that gives 30x coverage
Static use cases, no context	◆ Dynamic business ontology, full context

THE SOLUTION

Netenrich Agentic SOC:
A Digital Workforce for Modern Threats

Netenrich Agentic SOC is **not a chatbot bolted onto a SIEM.** It is a purpose-built autonomous security operations platform — specialized AI agents working continuously across detection, investigation, and response.

The agents don't assist your analysts. They **replace the work that was slowing them down** — so your team can focus on what AI cannot: judgment, strategy, and the investigations that actually matter.

HOW IT WORKS

From Raw Data to Measurable Security Outcomes

Most platforms stop at detection. Netenrich connects the full chain — from data ingestion to agentic action — without a human bottleneck at each step, turning raw telemetry into **grounded security decisions at machine speed.**

01	02	03	04
FOUNDATION	OPERATING SYSTEM	CAPABILITIES	METRICS
Google SecOps + Wiz	**Resolution Intelligence Cloud™**	**AI Analytics & Continuous Reasoning**	**Measurable Security Outcomes**
Data, telemetry, and threat intelligence at Google scale, plus cloud posture from Wiz.	The decisioning layer correlates posture, signals, and entity context to deliver high AI autonomy.	Gemini, BigQuery, and Vertex AI power behavioral analytics and always-on threat reasoning.	Autonomous action with full analyst visibility; no black box, no hallucinations, no lag.

Connecting data, reasoning, and execution without the human bottleneck.

THE OPERATING SYSTEM PLATFORM

Resolution Intelligence Cloud™: The Convergence Layer

Resolution Intelligence Cloud™ is the intelligence layer that sits **between your data sources and your decisions.** It ingests signals from Google SecOps, Wiz posture findings, and your full entity context — asset graph, ownership, blast radius — then delivers three outcomes that no single tool can provide alone.

DATA SOURCES

- Google SecOps signals
- Wiz posture findings
- Full entity context

THREE OUTCOMES NO TOOL DELIVERS ALONE

01 **Posture ↔ Signal correlation**
Know which structural weaknesses are actively exploited, not just theoretically exposed.

02 **Behaviors mapped to known weaknesses**
Connect runtime behavior to your specific attack surface.

03 **Contextualized situations → ActOns**
AI-generated, grounded action recommendations — no hallucinations.

POWERED BY THE FULL GOOGLE SECURITY STACK

Google SecOps provides data, telemetry, and threat intelligence at Google scale. Gemini, BigQuery, and Vertex AI power continuous reasoning. Wiz provides cloud posture context. Together, they **eliminate the data silos that plague legacy MDR architectures.**

Google SecOps

Data, telemetry, and threat intelligence at Google scale.

Gemini

Continuous reasoning across your environment.

BigQuery + Vertex AI

Behavioral analytics and always-on reasoning.

Wiz

Cloud posture context, fully integrated.

ARCHITECTURE

A Digital Workforce That Never Sleeps

Google SecOps and Netenrich AI agents operate in unison across different phases, each purpose-built for its role in the detection-to-response chain. Specialized agents run continuously— **no shift gaps, no alert queues, no human hand-off delays.**

01 Data & Signal Integrity	02 Detection & Intelligence	03 Investigation & Correlation	04 Proactive & Autonomous Defense
• Data Validation Agent	• Threat Modeling Agent	• Correlation Agent	• Response / Remediation Agent
• Signal Analytics Agent	• Behavioral Analytics Agent	• Investigator Agent	• Threat Hunt Agent
• Third-Party Context Agent	• Detection Engineering Agent	• Triage & Investigation (TIN)	
		• Malware Analysis Agent	

Agent attribution:

■ Purpose-built AI agents developed by **Netenrich**

■ Native AI agents from the **Google Security Operations** platform

A Alerts ——→ Signals B Events ——→ Context C Noise ——→ Decisions D Decisions ——→ Action

KEY DIFFERENTIATORS

Why Netenrich. Why Now.

3 min Mean Time to Triage

The Fatality Gap closes in 25 minutes. Our contractual SLA closes it in 3. From the moment an alert fires, the Netenrich pipeline runs autonomously: alert to story, impact analysis, L.I.C. (Likelihood, Impact, Confidence) scoring, and investigation — all in under 3 minutes.

98% AI Autonomy from Day 1

The 3-minute SLA is possible because 98% of known threats never reach a human queue. Most MDR vendors claim 'agentic' but operationalize it as AI-assisted triage — humans still in the loop. Netenrich agents execute autonomously; your analysts supervise and focus on the 2% that genuinely requires human judgment.

50%+ Operational Cost Reduction

Legacy stacks bill you at every layer — per GB ingested, per AI query, per analyst hour, per tool renewed. Netenrich consolidates all of it. Analytics-driven data engineering reduces ingestion by more than 55%, AI autonomy eliminates L1/L2 analyst tiers entirely, and 98% automated triage means your remaining team operates at a fraction of traditional headcount — without the coverage gaps.

30x Detection Coverage

Sub-second search across your full behavioral history enables broad behavioral detections instead of narrow precision rules — turning the 1,200 alerts per month a legacy MDR generates into 200,000+ behavioral observations, dramatically expanding your threat surface coverage. All with a full data lake included.

30 days Deployed

A three-week migration sprint: Week 1–2 for data onboarding and visibility; Week 2–3 for detection tuning and behavioral analytics; Week 3–4 for full autonomy and AI-driven response. No disruption to existing operations.

Glass Box, Not a Black Box

You see exactly what our AI sees. Full transparency into every agent decision, every correlation, every action taken. Your team supervises; the AI executes.

BUSINESS VALUE

The Hidden Cost of Standing Still

Most security architectures carry costs that rarely appear on a single line item but accumulate silently across every quarter. Understanding where the budget actually goes is the **first step to rationalizing it.**

The Ingestion Tax

Every byte of data ingested into a legacy SIEM carries a per-GB cost. Security teams are forced into an impossible choice: pay to ingest everything and watch costs spiral, or drop logs to stay on budget — and accept the blind spots that come with it. Neither is a security posture. It is a **billing model masquerading as one.**

The AI Token Surcharge

As vendors retrofit AI onto legacy platforms, AI inference costs appear as variable, unpredictable surcharges — charged per query, per investigation, per enrichment call. The more your team relies on AI assistance, the higher the bill. Effective AI-powered security should not penalize usage; **it should reward it.**

The Tool Sprawl Premium

A SIEM. A SOAR. Threat intelligence feeds. A separate data lake. Point solutions for each gap that surfaces. Each tool adds licensing cost, integration overhead, and analyst context-switching. The result is a portfolio of **60+ tools**, many underutilized, none communicating natively — each requiring its own renewal conversation.

The Human Ceiling

As threat volume grows, the only lever legacy MDRs offer is headcount. More alerts require more analysts — a model that scales costs linearly while security efficacy remains flat. Hiring cannot keep pace with machine-speed attacks, and each analyst represents not just salary but **training, retention, and off-hours coverage risk.**

Netenrich consolidates all of it.

Google SecOps platform | SOAR & Threat Intel | Hot Data lake | Unlimited AI tokens | 24/7 Autonomous Operations | 30-Day Migration Sprint

CUSTOMER PROOF

Proven at Enterprise Scale

"We moved from managing alerts to managing risk. We now operate with far greater confidence and precision."

— **Kumar Palaniappan · CISO, Cloud Software Group** (Citrix, TIBCO)

"With Netenrich and Google SecOps, our team now focuses where it counts — on meaningful investigations, not chasing noise. Response times have improved, signal quality is sharper, and we can present a clear, confident security picture to the board."

— **Harsh Jha · CTO, Nuvama Group**

REPRESENTATIVE OUTCOMES

ENTERPRISE SOFTWARE

52 → 6

SOC analysts

Was: 52-person SOC on Splunk drowning in noise, cloud entirely unmanaged.
Now: Team of 6 drives proactive security engineering and full cloud coverage — none replaced, all repurposed.

WEALTH MANAGEMENT

98%

of triage automated from Day 1

Was: Legacy SIEM noise; posture assembled the night before every board review.
Now: Always-on board visibility; team elevated to strategic investigation.

NETWORKING

30×

detection coverage

Was: Prior MDR delivered 1,200 precision alerts/mo — narrow rules, massive blind spots.
Now: Behavioral observability across 200,000+ behaviors/mo. The invisible is now actionable.

MEDIA & ENTERTAINMENT

40%

ingestion reduction

Was: 150TB/yr on Securonix; budget forcing critical log drops.
Now: Reduced to 90TB via analytics-driven data engineering, with coverage extended to new cloud environments.

GETTING STARTED

The 30-Day Roadmap to Continuous Readiness

WEEK 1–2

Foundation

Data onboarding and full-environment visibility across cloud, identity, and endpoints.

WEEK 2–3

Intelligence

Detection tuning, behavioral analytics, business ontology construction, and threat surface mapping.

WEEK 3–4

Autonomy

Specialized AI agents fully operational; agentic response live; 3-minute SLA active.

210+

Axis Securities · HPE · Cohesity · Juniper · Citrix · Nuvama Wealth · TIBCO · LendingKart

ENTERPRISES · PROVEN AT SCALE

Take the 30-Day Agentic SOC Challenge →

Get your transformation plan today. No disruption. No lock-in.

Google Cloud SECURITY Partner of the Year Managed Security Service Provider North America 2026

KNOW MORE: NETENRICH.COM/SOLUTIONS/AGENTIC-SOC