SOLUTION BRIEF · RESOLUTION INTELLIGENCE CLOUD™

Cyber Risk Operations

Move beyond alert-driven security operations.

THE DISCIPLINE, DEFINED

The continuous, automated discipline of identifying, structuring, reasoning over, and reducing risk across an enterprises' digital estate operating at the speed and scale of AI-augmented threats, with full auditability of every risk decision made.

6yrs	210+	50%	98%
In enterprise production	enteprise customers	cost	workload

INSIDE THE BRIEF

Powered by

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

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

THE PROBLEM

Your adversaries upgraded.
Your security program didn’t.

AI-powered attacks don’t respect head count, alert queues, or annual budget cycles.The adversary has operationalized automation. **Most enterprise security programs haven’t.**

<10min

Initial access to lateral movement in AI-augmented attacks

Adversaries operate at machine speed.

Automated attack chains compress the window from initial access to lateral movement to minutes. Human analyst triage operates at a fundamentally different timescale. **More headcount doesn’t close a speed gap.**

4,800+

enterprise SOCs

Alert volume has outpaced human triage.

Moresignals,more tools,more integrations— but the alert queue keeps growing. **Triage has become the job, not the means to a job.** Adding analysts does not close a speed gap.

Annual

Frequency of most risk assessments — not nearly enough

Risk is invisible until it‡’ a crisis.

Point-in-time assessmentsand posturescores disconnected from your actual environment make it impossible to answer the board’s first question: how exposed are we, right now?

THE DISCIPLINE

What Cyber Risk Operations is. And what it isn't.

Most of what the market calls "security operations " is monitoring, alerting, and incident response — reactive, human-paced, and disconnected from continuous risk visibility. **Cyber Risk Operations is different in kind, not degree.**

WHAT IT IS	WHAT IT IS NOT
✓ A continuous operating discipline, not a periodic a sse ssme nt	× Security monitoring or alert management
✓ Decision-level intelligence with full audit trails	× Data plumbing or SIEM infrastructure
✓ An OS layer that compounds in value over time	× Posture scoring disconnected from live environments
✓ Architected for machine-speed threat environments	× A managed service defined by analyst headcount

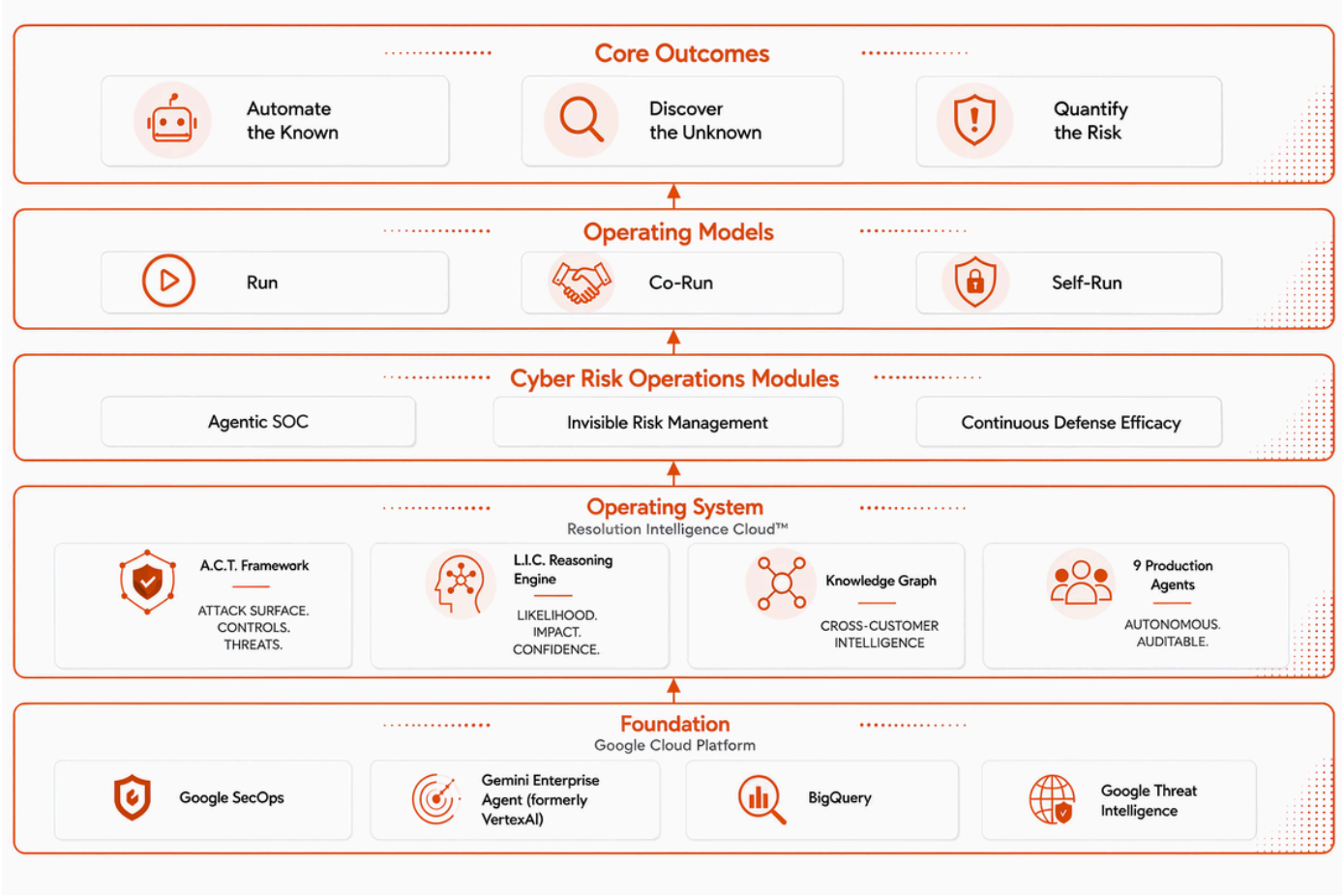
THE ARCHITECTURAL DISTINCTION

An operating system, not a platform — a platform is something you build on; an operating system is something you run on. It accumulates ontology, develops network effects, and becomes more valuable with every deployment.

THE RESOLUTION INTELLIGENCE CLOUD™

One operating system. Four layers that compound.

An OS accumulates ontology, develops network effects, and becomes more valuable with every deployment unning on Google SecOps as its substrate. Here i show the layers stack..



FOUNDATION → OPERATING SYSTEM → OUTCOMES

The distinction matters architecturally: Full capability depth requires Google SecOps as the primary substrate. Netenrich is the operations layer that turns that investment into measurable outcomes — not a reseller agreement.

FOUR PILLARS · PART 1 OF 2

The architecture that makes the discipline defensible.

These are not features —they are the system processes that make risk operations possible at machine speed.
Every operating mode runs on the same foundation..

01 A.C.T. Framework

ATTACK SURFACE | CONTROLS | THREATS

Your CMDB tells you what you owned last quarter. A.C.T. tells you what exists right now — cloud instances, containers, shadow assets, and the controls actually functioning on each one. A critical asset with a failed control under active threat isn't a medium-severity alert. It's your highest-priority risk.

GIVES YOU: A living model of your environment — not last quarter's asset scan. **The difference between knowing rain is coming and knowing your roof has a hole.**

02 L.I.C. Engine

LIKELIHOOD | IMPACT | CONFIDENCE

Legacy security reports on activity — events blocked, tickets closed, alerts triaged. L.I.C. reports on outcomes. Likelihood is calculated from threat capability and control effectiveness. Impact is derived from the business value of the specific asset at risk. Confidence reflects data fidelity. Together they produce a risk score in dollars of financial exposure — the language the board actually speaks.

GIVES YOU: When the board asks "Are we secure?" — you answer with a **number, not a narrative.**

FOUR PILLARS · PART 2 OF 2

Intelligence that compounds. Agents that act.

The final two pillars turn a living mode linto a network effect—and a network effect into autonomous, always on operations.

03 Knowledge Graph

COLLECTIVE INTELLIGENCE

NETWORK EFFECT

Every deployment enriches a shared, anonymized intelligence layer. Attack patterns seen in one environment sharpen detection across all others — automatically. The system applies radical relevance filtering: a Linux ransomware campaign is noise for a Windows-only shop. The graph knows your stack and filters accordingly.

GIVES YOU: Detection accuracy that compounds with every deployment — a **network effect human-scale operations structurally cannot replicate.**

04 Nine Agents

AUTONOMOUS

AUDITABLE

ALWAYS-ON

Not AI bolted onto broken architecture. Not a chatbot suggesting next steps. Purpose-built agents that maintain state, execute multi-step workflows, and decide autonomously — handling 98% of alert processing so analysts focus on the 2% requiring human judgment. Data validation, correlation, investigation, behavioral analytics, threat hunting. Continuously, with full audit trails.

GIVES YOU: **Operations that scale with threat volume, not headcount.**

98/2 **The 98/2 Principle**
Machines handle the noise. Humans handle the strategy — judgment, creativity, and adversarial thinking.

A DIGITAL WORKFORCE OF AI AGENTS

Nine agents. One coordinated pipeline.

Specialized AI agents organized across four operational functions working from signal to action, completing end-to-end in under three minutes,with no shift gaps and no hand-off delays.

PHASE 01 — Visibility & Validation

Data Validation Agent
Ensures signal fidelity and data integrity before processing begins.

Third-Party Context Agent
Enriches signals with external threat intelligence at scale.

GOOGLE SECOPS

PHASE 02 — Detection & Intelligence

Signal Analytics Agent
Converts raw alerts into contextual signals for downstream reasoning.

Behavioral Analytics Agent
Detects anomalies across historical behavioral baselines.

Threat Modeling Agent
Maps observed behavior to known threat actor TTPs in real time.

Detection Engineering Agent
Continuously tunes detection logic without manual effort.

GOOGLE SECOPS

PHASE 03 — Investigation & Correlation

Correlation Agent
Connects disparate events across identity, cloud, and endpoint.

Investigator Agent
Autonomous deep-dive investigation on prioritized incid e nts .

Triage & Investigation
Automated incident triage workflows, native to the platform.

GOOGLE SECOPS

PHASE 04 — Autonomous Defense

Response / Remediation Agent
Executes agentic containment and remediation actions.

Threat Hunt Agent
Proactively hunts low-and-slow threats in behavioral data.

Threat Hunting Agent
Proactive hunting across the full security data lake.

GOOGLE SECOPS

Netenrich customers typically experience up to a 98% reduction in manual operational workload — allowing analysts to focus on investigation, strategy, and higher-order security decisions rather than repetitive alert triage.

OPERATING MODES

One system. Three ways to run it.

We don't proliferate products.The Resolution Intelligence Cloud™ is identical across all three modes what changes is who operates it.

MODULE 01

AGENTIC SOC

An autonomous, software-driven architecture embedded natively in your environment. Replaces legacy, reactive alert triage with machine-speed detection, investigation, and containment.

CORE CAPABILITIES

- Hyper-autonomous AI agents — Data Validation, Threat Modeling, Correlation, Deep Forensic Investigation
- Petabyte-scale ingestion & normalization across endpoint, identity, cloud, and network layers
- Multi-signal correlation grouping cross-layer anomalies into unified, context-rich Situations
- L.I.C. quantitative risk scoring fusing MITRE ATT&CK stages and FAIR frameworks
- Automated response playbooks via Google SecOps SOAR
- Detection & hunt toolkits

ENGAGEMENT MODELS

RUN
We operate it fully

Netenrich manages all detection, triage, investigation, and containment end-to-end. You receive outcomes and board-ready risk reporting — not alert queues.

Best for: Lean teams and mid-market enterprises

CO-RUN
We operate, you steer

Full transparency into every agent decision and L.I.C. risk score. Your team tunes detection logic and audits any workflow. Netenrich runs the system — you direct it.

Best for: Google SecOps buyers who won't accept a black box

SELF-RUN
Your team operates it

Agentic SOC capabilities licensed as an OS your engineers build on. Forward-deployed Netenrich engineers embedded at stand-up to accelerate and support.

Best for: Detection engineering teams with existing operational depth

MODULE 02

INVISIBLE RISK MANAGEMENT

Migrates defenses from static configurations to live behavior analytics — exposing where operational lines systematically break down before adversaries find them first.

CORE CAPABILITIES

- Standing Posture across 5 Lenses: Identity, Data, Workforce, Exposure, Production
- Posture & control intelligence — surfaces privilege drift, silent failures, unencrypted repositories
- 20+ extensible behavioral models tracking count, volume, and structural anomalies
- Cross-model anomaly sequencing into cohesive kill-chain narratives with AI-generated timelines
- Monthly posture-driven threat hunting scoped to your real-world risk gaps
- Continuous risk register with live-telemetry escalation guardrails

ENGAGEMENT MODELS

RUN
We operate it fully

Netenrich continuously monitors posture across all five lenses, runs monthly threat hunts, and maintains the risk register. You receive prioritized risk intelligence — not raw findings.

Best for: Security leaders who need risk visibility without operational overhead

CO-RUN
We operate, you steer

Your team gains full access to behavioral model outputs, posture lens data, and risk register logic. Netenrich operates the analytics layer — your team directs hunt priorities and risk thresholds.

Best for: Teams with security analysts who want to engage with risk data directly

SELF-RUN
Your team operates it

Behavioral models, posture lenses, and risk register as licensed primitives your engineers configure and extend. Netenrich engineers available for model calibration and methodology support.

Best for: Mature security engineering teams building custom risk operations

MODULE 03

CONTINUOUS DEFENSIVE EFFICACY

The apex configuration. Operationalizes the full A.C.T. framework to continually manage true risk and deliver provable readiness metrics — in the language boards and regulators require.

CORE CAPABILITIES

- Executive A.C.T. posture dashboard — provable defensive readiness across all ecosystems
- Attack surface engineering — Digital Twin mapping Crown Jewels by business unit
- Continuous control validation — closes the Detection-to-Prevention Gap
- Threat-to-control correlation — adversary tactics mapped against your active controls
- Business-aligned risk register — exposure gaps quantified as financial impact
- Automated board scorecards — technical logs transformed into ROI-ready financial metrics

ENGAGEMENT MODELS

RUN
We operate it fully

Netenrich manages the full A.C.T. framework — maintaining the Digital Twin, validating controls continuously, and delivering automated board scorecards on your cadence.

Best for: CISOs who need board-ready risk output without building the capability in-house

CO-RUN
We operate, you steer

Your team participates in A.C.T. configuration, Crown Jewel classification, and board scorecard review. Netenrich operates the system — your team validates and contextualizes.

Best for: Teams who want to own the narrative around board reporting

SELF-RUN
Your team operates it

The full A.C.T. framework, control validation engine, and risk register as a licensed system your engineers operate. Forward-deployed Netenrich expertise for strategic methodology guidance.

Best for: Large enterprises with dedicated risk engineering and governance teams

IN PRODUCTION

We built it. Its' running in production.

The Resolution Intelligence Cloud™ is not a road map. The A.C.T. framework, L.I.C. reasoning engine, and nine roduction agents are **operational across enterprise customers today.**

6yrs	210+	50%	30%	98%
In Enterprise Production	Enterprise Customers	Reduction in Security Operations Cost	Increase in Detection Coverage	Reduction in Manual Operational Workload

CUSTOMER EVIDENCE — RUNNING TODAY

Cohesity

COLLABORATIVE OPS

Following the Veritas acquisition, Cohesity needed to consolidate security operations across rapidly growing environments while managing escalating SIEM costs, alert fatigue, and operational complexity.

OUTCOMES

- Significant reduction in alert noise and operational fatigue
- Faster, more contextual threat investigation workflows
- Improved control over security data ingestion costs

Sutherland

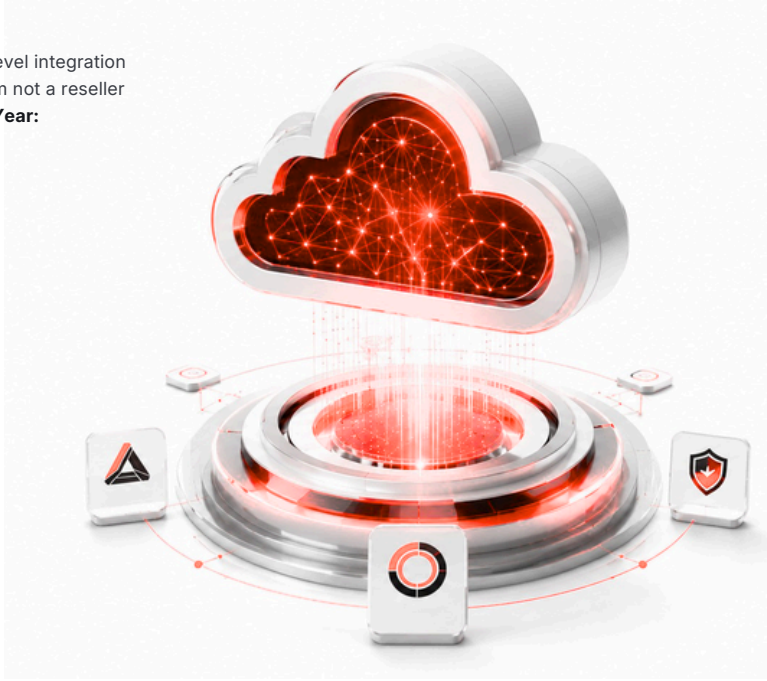
AUTONOMOUS OPS

Sutherland's legacy SIEM struggled to scale with growing data volumes, creating alert overload, limited visibility, and slow, manual incident response across a large global enterprise environment.

OUTCOMES

- Improved SOC visibility across cloud-scale environments
- Reduced alert fatigue through contextual detections
- Faster incident response with automated workflows

Google SecOps Partnership. Architecture-level integration as the operations layer on Google's platform not a reseller agreement. Named **Google Partner of the Year: Security North America MSSP.**



KEY QUESTIONS

The questions security leaders ask most.

Straight answers on how Cyber Risk Operations differs and how it fits the stack you already run.

Q How is this different from MDR or MSSP?

MDR and MSSP are labor arbitrage businesses — their unit economics require headcount to grow with threat volume. Cyber Risk Operations runs at machine speed using agents, not analysts. A fundamentally different operating model.

Q How is this different from CTEM or RBVM?

CTEM and RBVM tell you what's exposed. Cyber Risk Operations goes beyond identification to continuous operational reduction — A.C.T. structures, L.I.C. reasons, agents act, the graph compounds. CTEM is an input, not a substitute.

Q Do I have to replace my existing tools or SIEM?

No. The Resolution Intelligence Cloud™ is built on Google SecOps and operationalizes the infrastructure you already have. For organizations already on Google SecOps, there's no platform migration required.

Q Can I start with one mode and change later?

Yes. The operating modes are expressions of the same OS — not separate products. Organizations can transition toward greater internal ownership as capabilities mature, via structured migration pathways.

Q How does L.I.C. satisfy auditors and GRC?

L.I.C. produces explainable, line-by-line auditable outputs mapping to NIST CSF, ISO 27001, SOC 2, SEC disclosure rules, and NIS2 — with supporting evidence directly usable in audit and board reporting.

Q How does the Knowledge Graph protect privacy?

The graph operates on anonymized, aggregated behavioral and threat-pattern data — not raw logs or customer-identifiable content. No customer's data is accessible by any other customer.

CYBER RISK OPERATIONS

Move Beyond Alert-Driven Security Operations.

NETENRICH.COM/SOLUTIONS/CYBER-RISK-OPERATIONS