NETENRICH

RESOLUTION INTELLIGENCE CLOUD™ FOR MANAGING BUSINESS RISK

TABLE OF CONTENTS

Resolution Intelligence Cloud is a cloud-native data analytics platform for managing risk and optimizing overall operations, with the scale and speed of Google Chronicle built in.

Maximize Efficiency & TCO

10x
more efficient

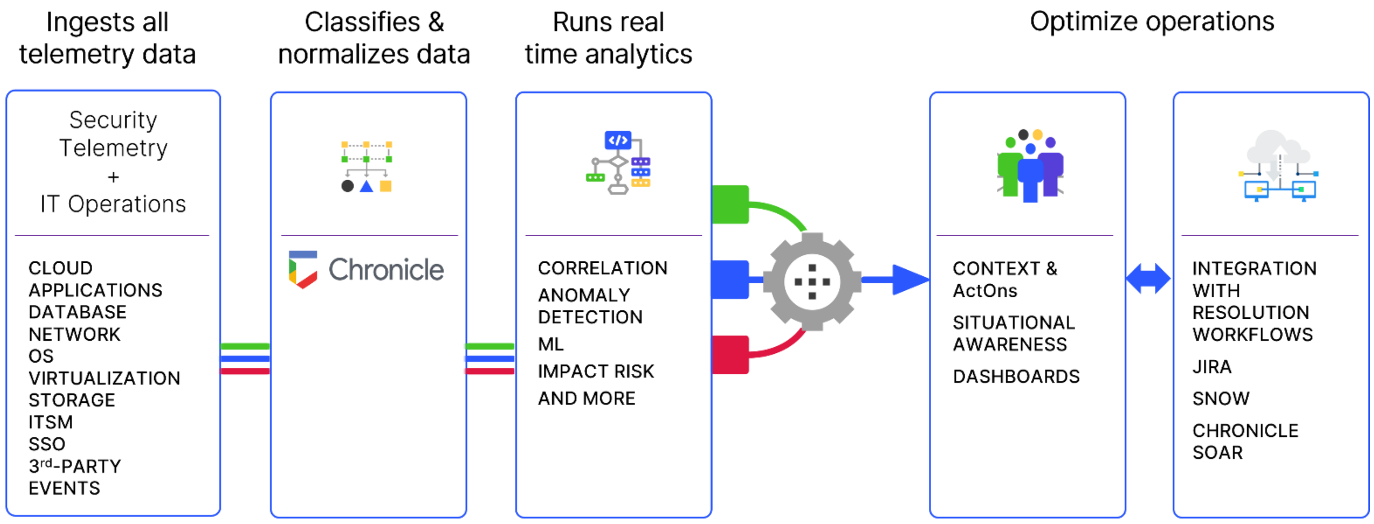
100%
visibility

90%
toil reduction

<3%
false positives

40%
TCO reduction

How Resolution Intelligence Cloud works



Ingests all telemetry data

Security Telemetry + IT Operations

CLOUD
APPLICATIONS
DATABASE
NETWORK
OS
VIRTUALIZATION
STORAGE
ITSM
SSO
3rd-PARTY EVENTS

Classifies & normalizes data

Chronicle

Runs real time analytics

CORRELATION
ANOMALY DETECTION
ML
IMPACT RISK
AND MORE

Optimize operations

CONTEXT & ActOns
SITUATIONAL AWARENESS
DASHBOARDS

INTEGRATION WITH RESOLUTION WORKFLOWS
JIRA
SNOW
CHRONICLE SOAR

Key scenarios

- **Respond fast to what matters most, aligned to the business**: Respond fast with enriched context, automation, and collaboration. Prioritize action based on business-aligned risk scoring. Over time, machine learning improves detection and automated responses.

- **Get comprehensive visibility and insights across environments and multiple tenants**: Have situational awareness across hybrid infrastructures. Get actionable insights that drive improvement and opportunities with multitenant analytics across all assets, clouds, data centers, and more. Provide end customers with visibility into metrics and trends that highlight the value you provide.

- **Find and fix vulnerabilities proactively**: Continuously monitor your dynamic attack surface. Automatically tag assets. Identify missing log coverage based on the MITRE ATT&CK framework and the tactics and techniques of known threat actors.

- **Detect unknowns and anomalies with behavioral analytics**: Detect anomalous behavior based on any attribute, not just user behavior and entity behavior. Run "what if" analyses to simulate situations and observe outcomes. Investigate with conversational AI.

- **Threat hunt**: Hunt for and uncover lurking supply chain attacks with one year of hot data and sub-second search on petabytes of data in Chronicle.

Have context you can act on, with ActOns™

ActOns correlate the events, users, and assets that matter. They're prioritized by a business-aligned risk score based on likelihood, impact, and confidence. A single ActOn console in the platform shows correlated detections, user and asset data, evidence, MITRE ATT&CK® mapping, and graphs, saving hours of research time. Instantly create a war room to securely collaborate on ActOns with colleagues, customers, and other third-party stakeholders.

Top security features

Observe: Common operational view across IT, Cloud, and Security

- Chronicle built in as its infinitely scalable, fast security data lake, with hot data for a year
- Multi-level multi-tenancy with discretionary RBAC (role-based access control)
- Data ingestion from anywhere (cloud, hybrid, on-prem)

Detect: Monitor everywhere, detect anomalies, reduce noise, threat hunt

- Behavioral analytics based on any attribute, not just user behavior and entity behavior
- Attack surface management and automatic asset tagging
- Netenrich threat intel, threat models, and ability to import your own threat feeds

Understand: Get situational awareness and extensive context for analysis

- Alert correlation and prioritization based on business risk
- No-code dashboards with insights across tenants
- MITRE ATT&CK mapping

Act: Resolve faster, proactively

- Automation and AIOps: Reduce workloads
- ActOns: Fix faster with extensive context, correlated alerts, collaboration war rooms
- Integration with existing resolution workflows: SOARs, ServiceNow, Jira, and more

To learn more, visit www.netenrich.com