# Resolution Intelligence Cloud™

## Real-time data analytics for secure operations at scale and speed

Resolution Intelligence Cloud is a native cloud data analytics platform for managing security and digital operations at scale. The platform transforms security and digital operations by ingesting all data across security and operations, identifying pre-incident  situations and incidents, ranking them by business risk, and correlating extensive context for proactive resolution.

CIOs and CISOs face increasing infrastructure complexity and an onslaught of threats. Multiple monitoring tools, siloed teams, and the growing need for hard-to-find talent busts budgets, doesn't scale, and isn't working. Leading CIOs and CISOs need to proactively manage risks to the business based on data, not react to low-level events. They need to make existing teams more effective.

It starts with data at scale, the more the better. Resolution Intelligence Cloud applies advanced analytics and machine learning across real-time operations *and* security data. It detects patterns that indicate risk - before incidents occur. So security and ops teams have situational awareness, context, and a common operational picture that optimizes their effectiveness.

The platform automates low-level investigation tasks and uses machine learning to reveal situations that may be malicious – depending on context – and may require resolution. ActOns present information you can act on: highly correlated information about related events, assets, and users. Priority scoring based on impact, likelihood, and confidence indicates where you should focus first to minimize business disruption. Analysts have a single place to collaborate with context and make decisions with data for fast resolution.

Resolution Intelligence Cloud leverages and operationalizes Google Chronicle for scale and speed, adding multi-level multitenancy, easy-to-use content management for rules and parsers, and more. The platform integrates with Chronicle SOAR and ITSMs to speed resolutions.

## Resolution Intelligence Cloud subscriptions

Resolution Intelligence Cloud plans fit wherever you are on your journey to secure operations at scale:

- **Foundation** - Ingest all your data without penalty. Jumpstart Google Chronicle for security data and threat detection at Google speed and scale. Foundation provides multi-level multitenancy, role-based access control (RBAC), single sign on (SSO), detection rule and parser management, detection rule and parser packs, Netenrich threat intelligence, real-time dashboards and reports, and more.
- **Analytics** - Get situational awareness and be proactive with real-time data analytics and machine learning that reveal risky behaviors and pre-incident situations. Situations are scored by business risk, and they present information you can act on: highly correlated information about related events, assets, and users. Up-level staff by automating Tier 1 and Tier 2-level tasks.
- **Resolutions** - Resolve situations quickly and effectively with data and Actons™: highly correlated information about related events, assets, and users. Analysts, colleagues, ops, customers, even third-party experts can collaborate with context and see what happened when. Two-way integration at the ActOn level with Google's Chronicle SOAR (formerly Siemplify) and ITSMs speeds resolution and enriches existing resolution workflows.

See reverse for features in each plan.[1]

Contact us and find more information at netenrich.com. Buy now on Google Cloud Marketplace.

[1] Plans and pricing are subject to change. For the latest information, see netenrich.com/platform/pricing.

## Resolution Intelligence Cloud subscriptions

Pricing starts at $45 per covered personnel per year with a one-year contract. Contact us if you already have Chronicle licenses.

| | Foundation | Analytics | Resolutions |
|---|---|---|---|
| **Base Platform** | | | |
| Multi-level multitenancy, RBAC, SSO | ✓ | ✓ | ✓ |
| **Google Chronicle** | | | |
| Google Chronicle licenses from Netenrich | ✓ | ✓ | ✓ |
| Integration with Chronicle SOAR | ✓ | ✓ | ✓ |
| **Data ingestion** | | | |
| Cloud, Hybrid Cloud, On-prem | ✓ | ✓ | ✓ |
| **Content Management** | | | |
| Parser packs & parser management | ✓ | ✓ | ✓ |
| Detection rule packs & rules management | ✓ | ✓ | ✓ |
| **Netenrich Threat Intelligence** | | | |
| Curated, enriched threat intelligence feeds | ✓ | ✓ | ✓ |
| **Signal Browser** | | | |
| Listing of alerts | ✓ | ✓ | ✓ |
| **Dashboards and Reports** | | | |
| Out of the box and DIY | ✓ | ✓ | ✓ |
| **Support** | | | |
| Customer success manager (CSM) | ✓ | ✓ | ✓ |
| Customer support | 24/7 (Web) | 24/7 (Web) | 24/7 (Web) |
| **Analytics and Situational Awareness** | | | |
| Analytics workbench | | ✓ | ✓ |
| Attack surface intelligence | | ✓ | ✓ |
| Threat detection mapped to MITRE ATT&CK | | ✓ | ✓ |
| Indication of Compromise intelligence | | ✓ | ✓ |
| Vulnerability intelligence | | ✓ | ✓ |
| External threats | | ✓ | ✓ |
| Threat models | | ✓ | ✓ |
| AIOps | | ✓ | ✓ |
| **Automation** | | | |
| Tier 1+ SOC automation | | ✓ | ✓ |
| Tier 1+ NOC automation | | ✓ | ✓ |
| **Asset Intelligence** | | | |
| For cloud assets (GCP, AWS, Azure) | | ✓ | ✓ |
| **Situations** | | | |
| Scoring: likelihood, impact, confidence | | ✓ | ✓ |
| Situational analytics | | ✓ | ✓ |
| **Resolution with ActOns** | | | |
| Timelines | | | ✓ |
| War room for collaboration | | | ✓ |
| ActOn policy | | | ✓ |
| ActOn integrations: Chronicle SOAR, ITSMs | | | ✓ |