Jumpstart Google Chronicle with Resolution Intelligence Cloud™ Foundation

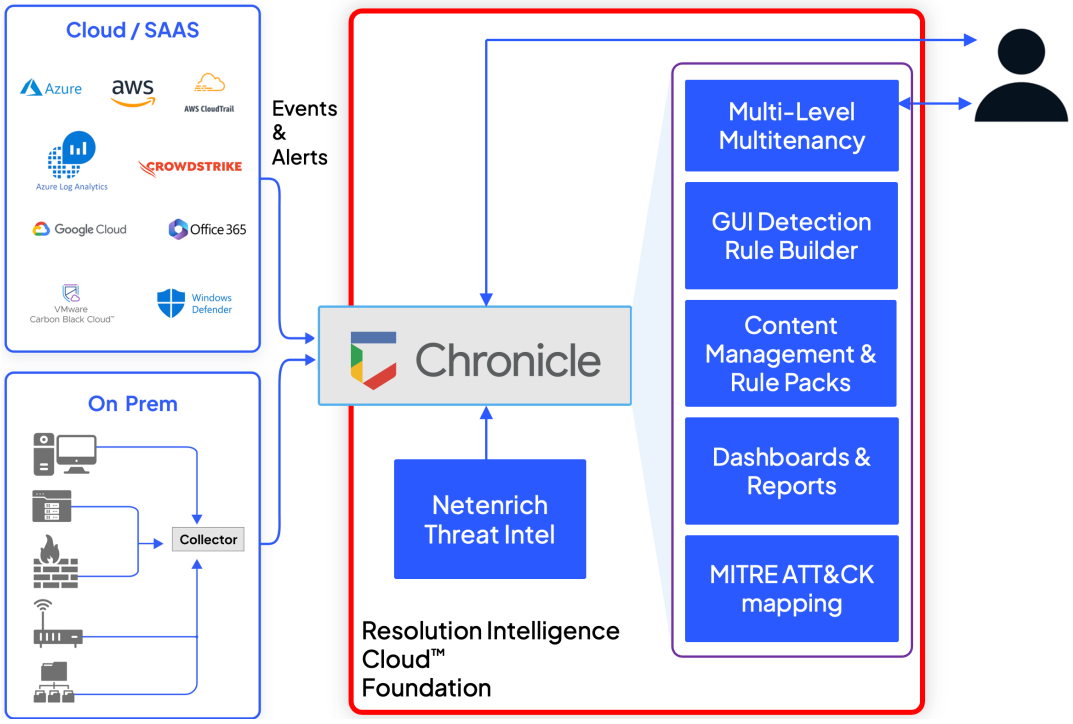
The entry-level subscription plan for Resolution Intelligence Cloud lays the foundation for using security data at petabyte scale in Google Chronicle. Resolution Intelligence Cloud (all plans) uses Chronicle as its security data lake. You get all the functionality of Chronicle plus ease of use, content, and services for success at service-provider scale. Plus, you'll have the customer support you need to get started and succeed.

Harness Chronicle power with Resolution Intelligence Cloud usability

Chronicle is a powerful engine. Resolution Intelligence Cloud Foundation harnesses and operationalizes it with functionality that improves success and effectiveness, such as:

- **Multi-level multitenancy of Chronicle instances**
- **GUI detection rule builder that simplifies YARA-L rule development**
- **Content Management System plus rule and parser packs**
- **Configurable dashboards and reports (built on Big Query)**
- **MITRE ATT&CK mapping**

Plus, Netenrich provides implementation services, a customer success manager, and customer support for ongoing success. Upgrade anytime to Resolution Intelligence Cloud Analytics and Resolutions for alerts correlated with context, intelligence, automation, user entity behavior analytics to find unknowns, and more to speed detection and response while up-leveling staff.



v.01312023

NETENRICH

Chronicle

Resolution Intelligence Cloud Foundation + Chronicle Capabilities

Resolution Intelligence Cloud builds on the power of Google Chronicle. Capabilities listed below are available in Resolution Intelligence Cloud Foundation.

Capability	Chronicle	Resolution Intelligence Cloud Foundation
Data ingestion, search, retention	Ingestion at petabyte scale (multi-cloud, on-prem, data center). Unified Data Model. Super-fast search. Twelve months hot data.	All benefits of Chronicle plus pivot seamlessly from Foundation GUI to Chronicle to search and threat hunt.
Multi-level multitenancy		**Purpose-built to manage multiple Chronicle tenants** from one place. Cross-tenant visibility. Secured with role-based access control (RBAC) and SSO.
Detection rules	Write and edit rules in YARA-L.	**GUI detection rule builder:** create and edit YARA-L rules without code. Rules run directly in Chronicle. Includes **rule testing**.
Content Management		**Manage/package sets of rules** for one or more Chronicle instances. Example: sets of rules for Compliance, or specifically for PCI Compliance.
Rule and parser packs	Comes with detection rules and parsers.	**Additional rule and parser packs**. Netenrich can, optionally, create custom rules and parsers.
Dashboards and reports	Default dashboards for analysis and reporting. Dashboards built on Looker and Big Query.	**Additional dashboards and reports** plus **no-code configurable dashboard builder** on BigQuery. Run dashboards and reports on one, some, or all Chronicle tenants.
MITRE ATT&CK mapping	Google Cloud Threat Intelligence provides and manages a set of YARA-L rules to help customers identify threats to their enterprise.	**Maps alerts to MITRE ATT&CK framework**. Dashboards display MITRE ATT&CK tactics. At higher subscription levels, correlated alerts are mapped to MITRE ATT&CK for context in ActOns.
Threat intelligence	VirusTotal. Google Cloud Threat Intelligence (GCTI) customers get GCTI alerts.	**Netenrich Threat Intelligence** adds third-party threat intelligence, vulnerability disclosures, reference lists of threat intelligence, advisories.

Visit netenrich.com/platform/foundation-chronicle for more information and to contact us. Learn more about Resolution Intelligence Cloud at netenrich.com/platform.

We're on Google Cloud Marketplace.