Netenrich
Resolution Intelligence Cloud™

Chronicle

# Resolution Intelligence Cloud™ + Chronicle

## The challenge: Unclear and present danger

Constantly reacting to alerts doesn't work or scale. Cyberattacks are intensifying in frequency and sophistication, while your infrastructure is increasing in complexity. Siloed security tools generate zillions of alerts — your security team is stressed from alert fatigue, and your budget is stressed too. You simply can't hire enough people. It's time for a new, proactive approach to cybersecurity operations.

## The solution: Secure operations with Resolution Intelligence Cloud + Chronicle

Run secure operations aligned with your business. Resolution Intelligence Cloud puts data analytics to work, correlating events from multiple detection sources and using behavioral analytics to make SOC teams dramatically more effective. Resolution Intelligence Cloud delivers intelligence you can act on to proactively strengthen your security posture and speed response.

### Key benefits

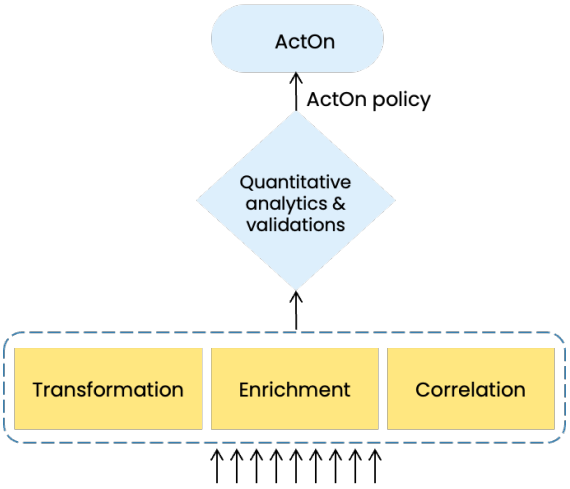
- **Strengthen cybersecurity risk posture** with risk-based cybersecurity aligned to the business. Address areas of vulnerability that matter most — before exploits occur. Resolution Intelligence Cloud's open architecture works with your tech stack now and later, so you can continuously improve without disruption.
- **Boost analyst productivity and effectiveness by 80% or more**. Resolution Intelligence Cloud minimizes and automates tedium to cure alert fatigue. It eliminates redundant work and fills gaps by breaking down silos between security and digital ops, streamlining processes. Everyone is on the same page, focused on solving the most critical confirmed issues first, improving security and operational metrics.
- **Cut costs**. Chronicle delivers a 3.9x – 6x savings over other SIEM solutions.[1] Resolution Intelligence Cloud further slashes TCO with integrations with Siemplify, ServiceNow, and Jira and features that enable you to streamline your security and digital ops tech stacks.

### Sprint from SOC-as-usual to secure operations

Resolution Intelligence Cloud applies real-time analytics, context, and correlation across security and digital ops data. You have the situational awareness and data confidence you need to take action, prevent issues, and mitigate damage if an issue occurs.

### Context you can act on, with ActOns™

Beyond signals and noise, know if situations require attention. **ActOns™** correlate events, tickets, users, and assets. Resolution Intelligence Cloud scores each ActOn's risk based on likelihood, impact, and confidence. A single ActOn console 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 collaborate on ActOns with colleagues and customers. Click on any event to investigate directly in Chronicle with sub-second search.




[1] ESG, Analyzing Economic Benefits of Google Chronicle Security Analytics Platform, by Jack Poller, August 2020

Netenrich
Resolution Intelligence Cloud™

Chronicle

## Manage multiple Chronicle tenants in one place

Enterprises, MSPs, MSSPs, and GSIs: support your customers more effectively using Resolution Intelligence Cloud's multi-level multitenancy. Use role-based access control and an easy-to-use rules editor and rules manager to create rules in Chronicle and apply them to one, some, or all tenants, all from one place.

## Key scenarios

- **Visibility and situational awareness:** Analysts have situational awareness across hybrid infrastructures from one console. Detect and respond proactively with analytics that identifies patterns and anomalies across security and ops data. Over time, machine learning improves detection and automated responses.
- **Monitor and detect threats without alert fatigue:** ActOns correlate related event, user, and asset data with tickets in one console, reducing noise by 80%. ActOns are prioritized based on risk and impact to the business, so analysts know where to focus when.
- **Find and fix vulnerabilities before attacks occur:** Forecast cyber risk and proactively respond to situations that could be a threat with attack surface management. Identify where log coverage is missing based on the MITRE ATT&CK framework, so your defenses are ready.
- **Accelerate threat investigations with ActOns**: Click on events to investigate directly in Chronicle with sub-second search. Find lurking supply chain attacks with one year of data in Chronicle.
- **Improve case management**: Integrate with Siemplify/SOAR, ServiceNow/ITSM, OpsRamp/ITOM to manage response following your workflows.
- **Manage security for your customers**: Manage multiple Chronicle instances in one place. Get visibility across all or a subset of tenants. Apply detection rules to one, some, or all tenants, all from one console.

## Key features

**Situational awareness & prevention**

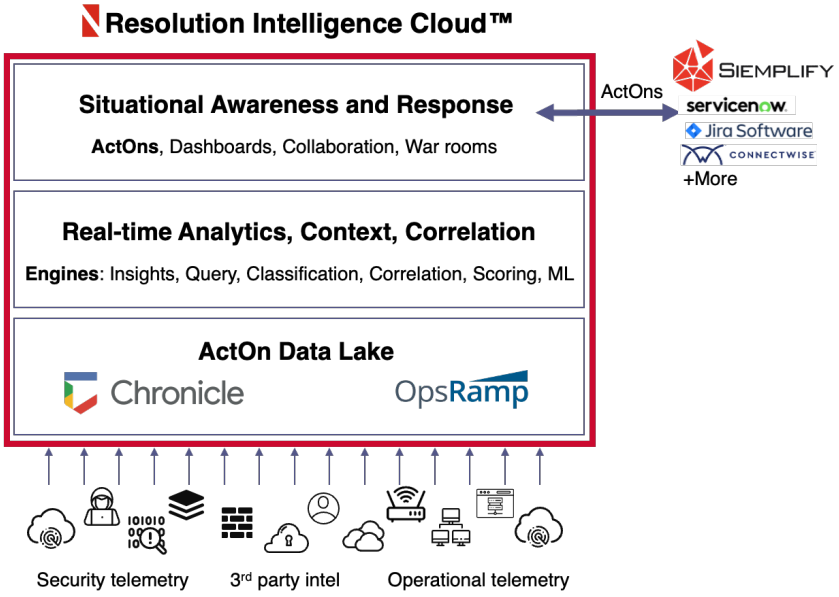
- Analytics, context, and correlation across security and operations data
- ActOn Console
- Advanced risk scoring
- Attack surface management
- Multi-level multitenancy
- Discretionary RBAC

**Detection**

- Threat intelligence
- Detection rules management
- MITRE ATT&CK mapping

**Response**

- Collaboration war room
- Automation
- Sub-second search on petabytes
- Integration with SOARs and ITSMs




## Learn more

Visit www.netenrich.com for more information.