



# NETENRICH RESOLUTION INTELLIGENCE CLOUD™: TRANSFORM TO AUTONOMIC SECURITY OPERATIONS

---





# TABLE OF CONTENTS

---

<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">Neterich Resolution Intelligence Cloud Key Benefits</a>	<a href="#">3</a>
<a href="#">Neterich Resolution Intelligence Cloud Plans – Enterprise</a>	<a href="#">5</a>
<a href="#">Plan Features</a>	<a href="#">6</a>
<a href="#">Available Add-Ons</a>	<a href="#">6</a>
<a href="#">Features</a>	<a href="#">7</a>





Netenrich Resolution Intelligence Cloud™ brings risk management, data analytics, and machine intelligence to enable organizations to transform to an Autonomic Security Operations (ASO) approach.

Organizations gain complete situational awareness to better detect and prioritize patterns that indicate risk — even before critical events occur. By distilling large volumes of alert noise down to ActOns — which represent context and information about related events, assets, and users and are ranked based on impact, likelihood, and confidence — the platform pinpoints the alerts that pose the most critical risk and that need immediate resolution.

Unique to the Resolution Intelligence Cloud platform are advanced features, including behavioral analytics, customizable machine learning (ML) models, and predictive threat management and response. The platform builds the foundation for a modern cybersecurity mesh architecture (CSMA) while leveraging existing security systems for increased scale and speed.

Moreover, Resolution Intelligence Cloud platform operationalizes Google Chronicle, a next-gen cloud SIEM, for scale and speed, while adding multi-level multi-tenancy, easy-to-use content management for rules and parsers, and much more. The platform also integrates with Chronicle SOAR and other ITSM tools to speed resolutions. It prioritizes risk and converges operations while optimizing SIEM, SOAR, UEBA, and various data sources to improve overall operational efficiency.

## Netenrich Resolution Intelligence Cloud Key Benefits:

- **Competitive advantage:** By adopting an ASO approach sooner rather than later, you gain a competitive advantage through scaling risk management to align better with the business and by reducing operational costs.
- **Advanced behavioral analytics:** Advanced behavioral analytics help discover, quantify, prioritize, and resolve risks across cybersecurity, digital, and development operations (DevOps).
- **Predictive intelligence:** Artificial intelligence (AI) engines not only quickly process events, analyze data, and detect anomalies, but their ability to continuously learn also helps prevent cyberattacks.
- **Machine learning:** Machine learning (ML) models identify threats that may otherwise go missed, helping you stay ahead of threats and protect your organization from cyberattacks.



- **Large language models:** Training data for customizable ML models allows you to converse with data with a sub-second response.
- **Intelligent SOC routing:** Intelligent routing capabilities direct pressing incidents to the right people for resolution.
- **Multi-tenant scalability:** Multi-level, multi-tenant support enables scale to accommodate the needs of businesses, both large and small, without imposing unnecessary financial burdens.
- **SOC and threat collaboration:** Enhanced collaboration features facilitate cross-organizational communication and coordination to speed incident resolution.
- **Automation:** Automation of low-level investigation tasks helps streamline processes, save time, and boost productivity.
- **Unified visibility:** A single pane of glass for all cybersecurity and digital operations data provides a holistic view into your environment to speed threat detection and response.
- **Flexible packages and pricing:** Flexible options are available to meet the needs of your organization — no matter your size and where you are in your security journey — today and into the future.



# Netenrich Resolution Intelligence Cloud Plans — Enterprise

Wherever you are on your ASO journey, we have a plan to meet your needs.

<b>Resolution Intelligence Cloud ESSENTIALS</b>	<b>Resolution Intelligence Cloud STANDARD</b>	<b>Resolution Intelligence Cloud PREMIUM</b>
<p>A perfect fit for your enterprise if you are just establishing a SOC.</p>	<p>A perfect fit for your enterprise if you already have a SOC but are operating it in a traditional manner. Your organization might be heavily reliant on manual processes and thus, could greatly benefit from the introduction of ML models to enhance your security operations.</p>	<p>Designed for your enterprise if you have an advanced mindset towards risk and the adoption of automation and ML systems. Your organization has already embraced the power of ML but is now looking for ways to prioritize and manage risk better while optimizing your SOC operations.</p>
<p>This plan serves as a stepping stone for you to establish a SOC and provides you with the necessary tools and support for threat detection.</p>	<p>This plan serves as a stepping stone for your enterprise to transition from traditional methods to a more modern, ML- and behavioral analytics-based approach. It provides the necessary tools and support to help you navigate this transition smoothly, while enhancing your threat detection capabilities and improving your overall security posture.</p>	<p>This plan offers advanced ML models and automation tools that can help your enterprise prioritize and manage risks better, detect and respond to threats faster, and achieve higher efficiency.</p>

All plans offer you a range of valuable opportunities and benefits to prioritize and manage risk better while your organization adopts ML and automation. Your choice depends on your specific needs and requirements. With any plan, you can prioritize and reduce your risk exposure, improve your ability to detect and respond to threats, and greatly improve your overall security posture.



# Plan Features

Scope	Resolution Intelligence Cloud ESSENTIALS	Resolution Intelligence Cloud STANDARD	Resolution Intelligence Cloud PREMIUM
Tenants	Single tenant	Single tenant	Multi-tenant
ML Models	20	60	120
Domains/Sub-Domains Monitored by Attack Surface Management (ASM)	1 domain; 5 sub-domains	5 domains; 25 sub-domains	Unlimited
Custom Exposures Detections on Attack Surfaces	10	25	100
Security Practitioner Role Users	10	20	30
Hot Storage	12 months	12 months	12 months
Correlation Policies	Unlimited	Unlimited	Unlimited
Notifications (Email, Push, Web, SMS, Phone)	Unlimited	Unlimited	Unlimited
Escalation Policies	Unlimited	Unlimited	Unlimited
General Role Users	Unlimited	Unlimited	Unlimited

## Available Add-Ons:

Additional Tenants	Available	Available	Included
Additional ML Models	Not available	Available	Available
Additional Domains/Sub-Domains Monitored By ASM	Not available	Available	Included
Additional Custom Exposure Detections on Attack Surfaces	Not available	Available	Available
Additional Security Practitioner Role Users	Available	Available	Available
Additional Cold Storage	Not available	Available	Available



Features	Resolution Intelligence Cloud ESSENTIALS	Resolution Intelligence Cloud STANDARD	Resolution Intelligence Cloud PREMIUM
<b>Signal Management</b>			
Signal enrichment engine	Y	Y	Y
Analytics and correlation of enriched Signals to Situations	Y	Y	Y
<b>Risk Intelligence</b>			
ActOns (situational intelligence and adaptive risk prediction based on LIC scoring - Likelihood, Impact, Confidence)	Y	Y	Y
Digital services management module with tagging of HVE (high value entities)	Y	Y	Y
Asset analytics module (prioritization, tagging, service grouping, event routing)	Y	Y	Y
<b>Advanced Analytics and Machine Learning</b>			
Signal analytics — Beta	Y	Y	Y
UEBA use cases — out-of-box models	Y	Y	Y
Behavior analytics (UEBA++) — Limited Beta	Y	Y	Y
Custom behavioral modeling, data science augmentation, and behavior-based detection library	Y	Y	Y
<b>Security Analytics Suite</b>			
Threat detection mapped to MITRE & cyber kill chain	Y	Y	Y
Threat Actor Intelligence mapped to MITRE	Y	Y	Y
Analytics to map security control gap to MITRE	Y	Y	Y
Vulnerability intelligence (formerly KNow)	Y	Y	Y
Out of the box dashboards and no-code custom dashboard builder with visualization	Y	Y	Y



Features	Resolution Intelligence Cloud ESSENTIALS	Resolution Intelligence Cloud STANDARD	Resolution Intelligence Cloud PREMIUM
<b>Threat Detection</b>			
Modern data & detection engineering — parsers, feeds, content mgmt. & integrations	Y	Y	Y
Detection rules library	Y	Y	Y
Threat feed-based detection	Y	Y	Y
Attack surface management — external exposure scanning and vulnerability integration (ASE – Attack Surface Exposures) for higher efficacy	Y	Y	Y
Custom Exposures for ASE	Y	Y	Y
<b>Streamlined Cybersecurity Workflow &amp; Response</b>			
SOC workflow management and optimization	Y	Y	Y
Advanced ITSM integration	Y	Y	Y
On-call schedules	Y	Y	Y
Escalation policies	Y	Y	Y
Email and push notification	Y	Y	Y
SMS and phone notification	Y	Y	Y
War room for collaboration	Y	Y	Y
<b>Data Framework for Autonomic Security Operations</b>			
Next-gen cloud native SIEM (12 months hot storage, threat hunting, powerful detection engine) — Google Chronicle SIEM (free license provided by Netenrich)	Y	Y	Y
Built-in parsers and cloud connectors	Y	Y	Y
Curated, enriched threat intelligence feeds	Y	Y	Y
Best of breed threat feeds from Netenrich and Google	Y	Y	Y
Netenrich's Knowledge Now (Global threat Intelligence)	Y	Y	Y
3 <sup>rd</sup> party threat intel feeds	Y	Y	Y
Chronicle SOAR / 3 <sup>rd</sup> party SOAR integration for risk response	Y	Y	Y
<b>Key Platform Operations Elements</b>			
SSO	Y	Y	Y
Multi-tenancy	Y	Y	Y
RBAC	Y	Y	Y
Cloud hosted datalake (petabyte scalability with sub-second search)	Y	Y	Y





Features	Resolution Intelligence Cloud ESSENTIALS	Resolution Intelligence Cloud STANDARD	Resolution Intelligence Cloud PREMIUM
<b>Customer Support &amp; Customer Success Management</b>			
Customer Support (24x7; Web)	Y	Y	Y
Customer Success Manager	Y	Y	Y

To learn more about how you can prioritize and manage risk better in your environment, as well as increase the efficiency and effectiveness of your security and digital operations, visit [www.netenrich.com](http://www.netenrich.com) or [contact the Netenrich team](#).