NETENRICH

Unleash the potential of Chronicle with

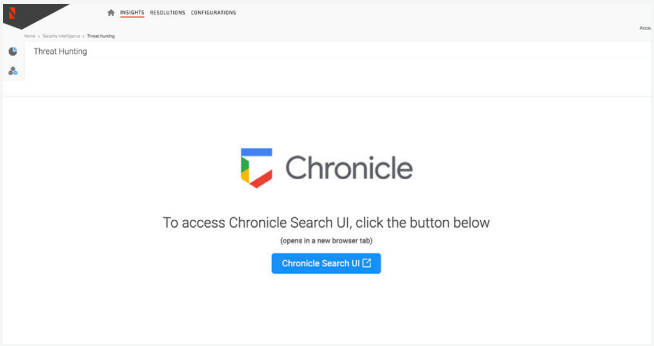
Analytics to innovate, scale, transform

Resolution Intelligence®: The data-driven ops platform for service providers

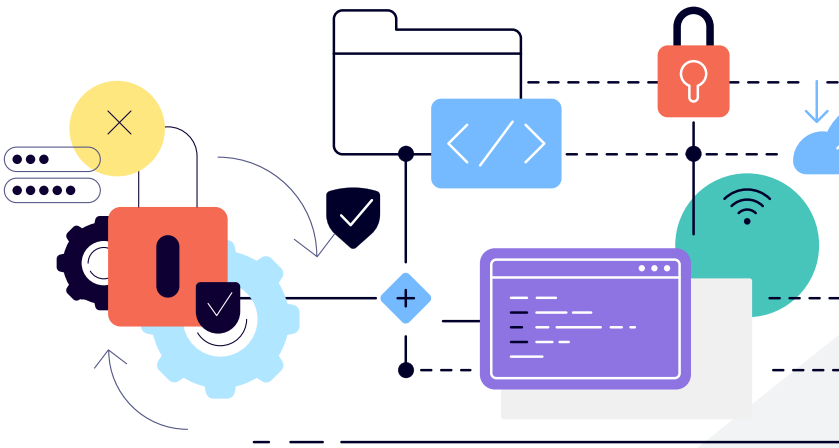
Chronicle unlocks the power of big data. Netenrich's Resolution Intelligence (RI) platform from Netenrich unlocks the full power of Chronicle to generate game-changing analytics.

Resolution Intelligence makes it easy for providers of managed services—MSPs, MSSPs, VARs—and enterprises to build and scale analytics-driven services. The platform fully operationalizes Chronicle to bring you Google-scale insights and context that save time, speed resolution, and keep all your digital ops aligned to risk.

Achieve rapid time-to-value with built-in multitenancy and task automation to improve response, situational awareness, and collaboration out of the box. Resolution Intelligence handles the challenging work of operationalizing Chronicle so your IT, cloud, and security teams don't have to.



Grow with better data. Resolution Intelligence brings everything your IT, cloud, and security teams need to drive Google-scale insights and efficiencies across your managed services environment using a single UI.



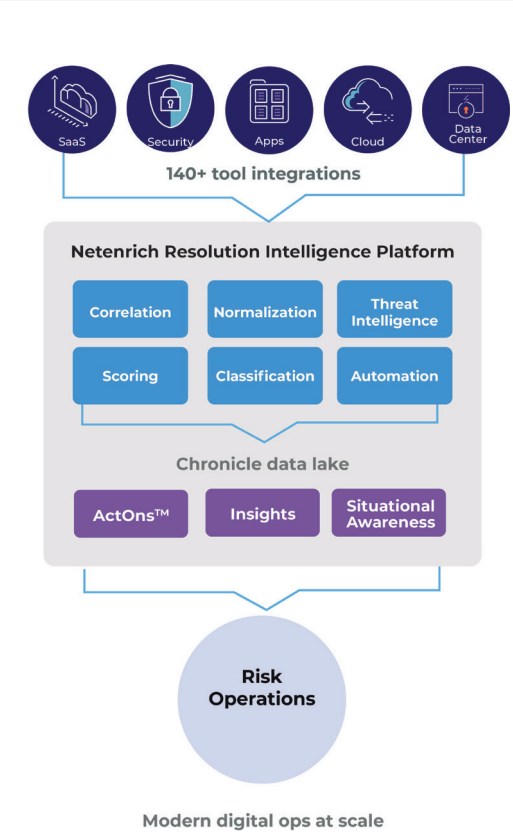
Scale operations, drive opportunities

Netenrich brings the analytics horsepower needed to scale managed detection and response services and bring innovative, insight-based offerings to market, without becoming tool or SOAR experts. Automation streamlines rule-building, case management, and threat analytics based on historical and contextual data.

MSPs can wield the same analytics capacity to create and monetize new services based on delivering new business insights to customers. Our SaaS-based, multitenant approach lets MSSPs stand up services without steep investments in licensing, multiyear contracts, and specialized talent. The ability to drive and scale new opportunities promotes higher retention and annual recurring revenues (ARRs) for MSPs while helping customers improve uptime, availability, and resilience.

Highlights

- Fully operationalize Chronicle
- Built-in multitenancy
- Build and scale MSP services
- Faster time to market, time to value



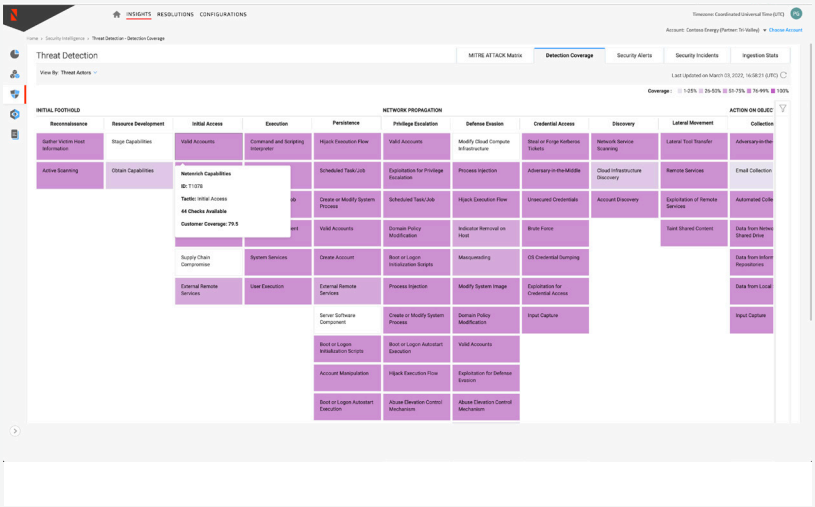
"Insight to action" at the speed and scale of Google. Chronicle and RI offer one-step, one-stop solutions for scaling modern digital operations. Automation, awareness, and analytics promote smarter workflows, faster resolution, and stronger ops and business resilience.

Manage multitenant environments with a single UI

Running operations customer by customer simply doesn't scale. Instead, log into the Netenrich platform to streamline rule-building, threat analytics, and event tracking across your entire base. Built from the ground up around three tiers of multitenancy, Resolution Intelligence lets MSSPs conveniently extend access and transparency to demonstrate value to customers.

Act on what matters in real time

Real-time analytics and rich contextual intelligence let analysts see the big picture—what needs protection, or attention, and who's doing what, where, and when—to predict risk and avoid problems. RI unifies and normalizes input from your data sources and threat detection tools and maps it to the MITRE ATT&CK model so you can find and fill gaps in coverage and understand how attacks happen.

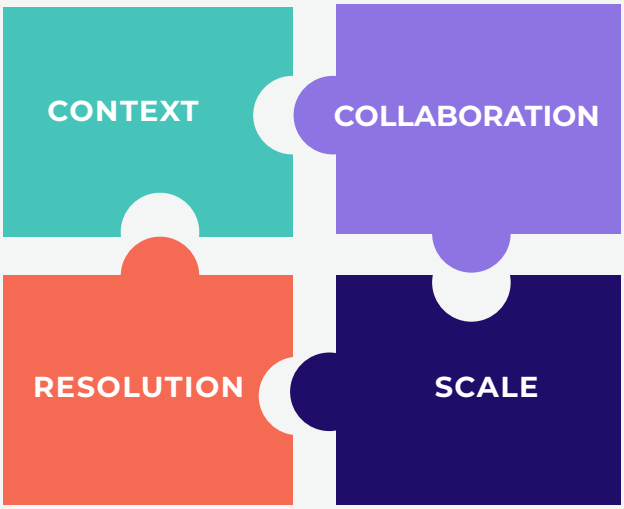


"Are we watching the right things?" RI distills user, endpoint, network, and cloud data into a single view so analysts can manage detection and understand adversary behaviors – without becoming tool experts. Full transparency and long-term retention of telemetry let you spot trends and keep operations aligned to risk.

Collaborate and resolve—faster

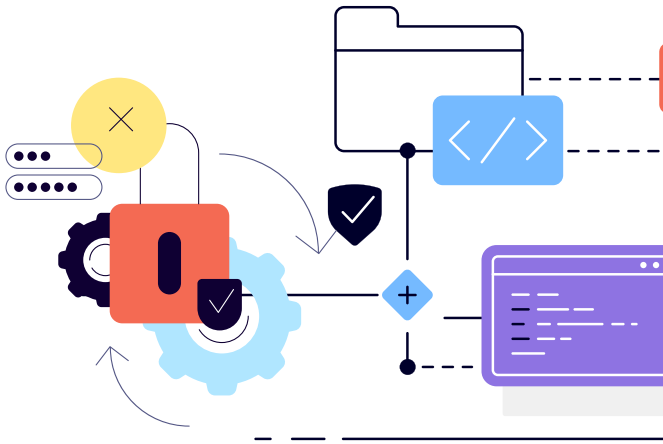
The faster the right people know what's happening, the faster issues get resolved (with five people on a bridge call instead of 30). Task automation, contextualization, and full transparency let your teams (and your customers' teams) see the same data, and the bigger picture.

Collaborate through the platform to drive resolution, lower cost, and conserve cycles while improving outcomes for customers.

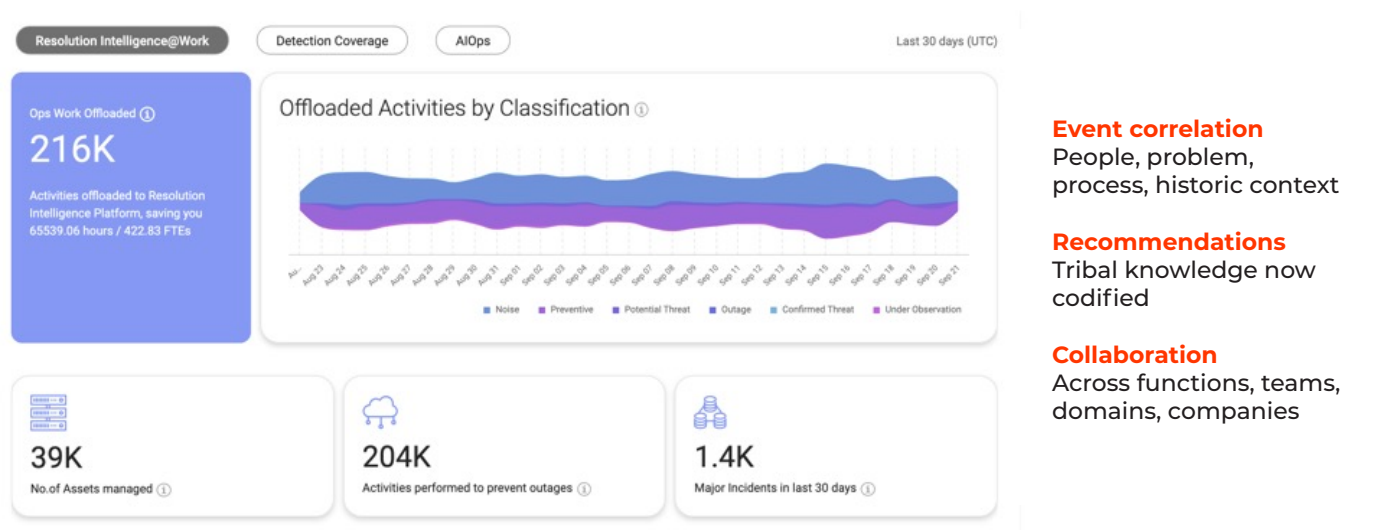


Do more with the data you have

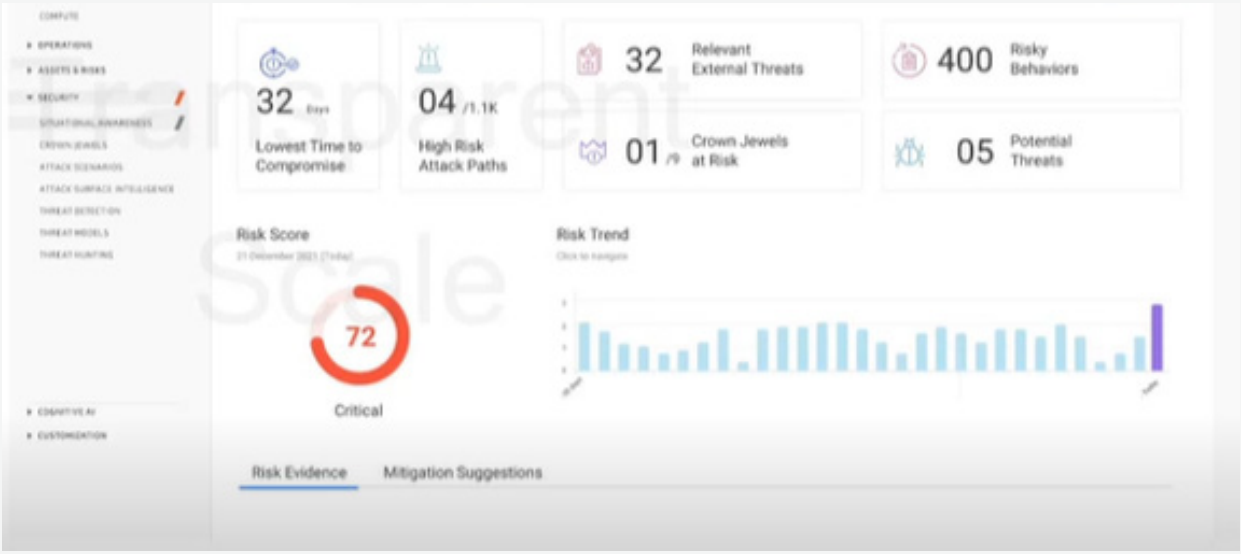
Combining Netenrich's analytics-as-a-service platform with Chronicle, the industry's premier security data lake, lets your teams access, retain, and realize greater value from data generated by existing detection and monitoring tools. Architected from the ground up to deliver real-time operations data, the platform generates actionable insights—awareness, fully contextualized "ActOns™," and analytics—so you can make data-driven decisions with ease and consistency.



Multitenancy, data sharing, and collaboration optimize your analyst-to-customer ratio as you consistently meet SLAs.



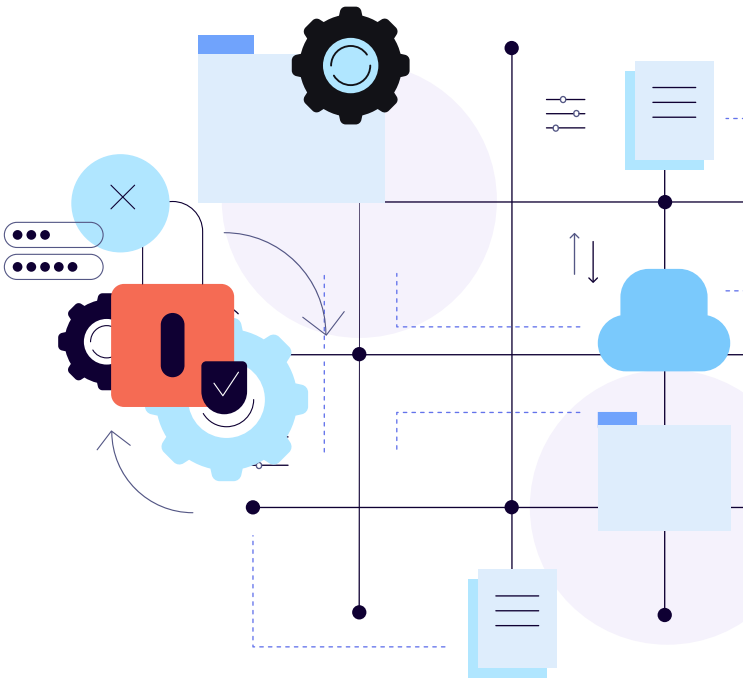
Optimize your analyst to customer ratio. RI and Chronicle bring the right technology, tribal knowledge, and processes to scale your services and customer base without scaling resources.



Let your experts do more expert things. Resolution Intelligence delivers Cyber Situational Awareness (CSA) and threat detection analytics to pivot security operations from reactive and event driven to proactive and risk driven. Faster time to insight helps IT and security teams resolve risk from endpoints, network, cloud, and user behavior before it leads to breaches.

Advance and modernize SecOps

As a cloud service, Chronicle adds as a specialized layer of security insight to core Google infrastructure. Providers can search, analyze, and retain massive amounts of security and network telemetry to improve cybersecurity posture. Chronicle normalizes, indexes, correlates, and analyzes data for instant analysis by those responding to incidents and proactively seeking to avoid risk.



Insight and research

Google Cloud's research surfaces highly actionable alerts in Chronicle environments based on Google's collective insight and research into Internet-based threats.

Google speed

Surface important indicators across high-volume and value sources like EDR, NDR, proxies, firewalls, and more with Google speed. Gain faster time to value.

Google scale

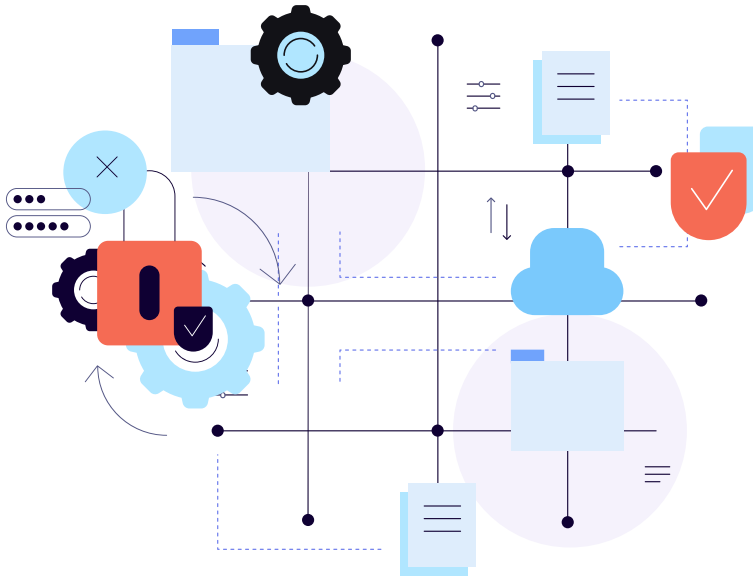
Planet-scale system for storing and analyzing all enterprise security telemetry.

Why Chronicle? Why Netenrich?

Chronicle and Resolution Intelligence have a lot in common. Both were built to help internal teams accelerate value and scale operations before being made available to partners and customers.

Architected to support managed service business models, Resolution Intelligence embodies 12+ years' experience resolving issues and driving efficient operations across 6,000 end customers worldwide.

Together, best-in-class data lake and operations analytics capabilities free you to transform, innovate, and scale digital ops and business at your own desired pace.



Features, Benefits, Analytics

What we do	What you gain
DATA MODELING	
Big data lake processing of cybersecurity data — unstructured, semi-structured, or structured data	• Model data into data sets based on specialized domain knowledge. Enable navigation by users to analyze business cases without need for technical knowledge
Ingest data from multiple sources (machine, non-machine) in various formats (JSON, XML, unstructured as web logs and app logs)	• Run analytics on big data • Analyze, detect, gather insights, and respond to cybersecurity threats and risks in all forms that they exist in an enterprise • Retain data for 12 months
Gather and analyze data from websites, applications, devices, sensors, etc.	• Eliminate blind-spots in your environment
Enable monitoring for detection and response across endpoints, EDR, hybrid cloud, NDR, users, SaaS apps, IDS/IPS, firewalls	• One-stop-shop visibility for cybersecurity monitoring, detection, response, and resolution • Eliminate swivel-chairing across multiple tools
Integrate with customer tools for log and alert ingestion	• Detect threats embedded in network traffic flows • Stop major incidents before they happen
Support network sensors	• Advanced analytics • Standard and custom reports on EDR performance and incident management in the environment
Integrate threat intelligence	• Leverage threat intel from industry-leading sources including Chronicle • Stay ahead of threat actors
DATA INDEXING	
Normalize, index, correlate, and analyze data to glean instant analysis and context on risky activity in enterprise	• Faster searching and querying on different conditions

Features, Benefits, Analytics

What we do	What you gain
DATA SEARCHING	
Retain, analyze, search, and tag massive amounts of security and network telemetry	• Create metrics, predict future trends, and identify patterns in data
Manage detection rules & use cases (standard and custom)	• Create and manage rules to detect, prioritize, and respond to high-impact threats • Solutions for email, cloud, network security, endpoints, servers, hosts, users • Multilevel rule management for service providers and clients
Perform advanced threat hunting and investigation	• Proactively find risk to stay ahead of bad actors • Search back in time and chronology for threat patterns and correlation
Perform advanced threat detection and response	• Recognize, expose, and shut down malicious operations before they take hold
Manage IP address white and black	• Track friend and adversary activity for more efficient processing
Provide big data lake with advanced analytics processing support	• Run powerful search queries on security, IT, cloud, and Dev ops data
Enable visual workflows of big data	• Increase efficiency, improve SOC outcomes
ALERTS & INCIDENT RESPONSE	
Ease of configuration of alerts and incidents	• Pre-integrated support for popular ticketing systems (such as ServiceNow)
Correlate alerts and incidents using AI/ML	• Trigger emails or RSS upon matching criteria • Reduce noise and alerts • Obtain better insights on alerts and business impact
Enrich alerts and incidents with actionable context and intelligence	• Make better decisions faster
Score alerts and incidents based on AI/ML	• Sort and prioritize incidents easily by metrics that are most important (e.g. risk, impact)
Define notification and escalation paths and workflows	• Configure heirarchy of escalation notifications • Notify via multiple modes – email, phone, SMS
Automate incident resolution (IR) using pre-builtrunbooks	• Speed detection and response with insights from Netenrich Resolution Intelligence database
Provide incident management interface for resolutions	• Eliminate need for heavy-duty ITSM/ticketing systems
Track incident timeline	• View chronology of threat events as they happen
Reduce false positives with analyst-vetted insights and automation	• Eliminate wasted cycles • Prioritize incidents that matter most

Platform Features and Benefits

What we do	What you gain
REPORTS & DASHBOARDS	
Create standard and custom dashboards, insights, reports	• Build custom reports and dashboards without need to code • See search results in chosen format—charts, reports, pivots, etc. • Data organized for intuitive, effective decision making
Classify asset intelligence for noisy and problem assets	• Prioritize threat hunting analysis faster
Create MITRE ATT&CK-based classification and dashboards	• Standardize on industry nomenclature/ format for modeling threats and attacks • Know your detection coverage and blind spots • Reduce training costs • Improve speed, quality of threat response
ACTONS & COLLABORATIONS	
Manage ActOns	• Get AI/ML-prioritized, sequenced, context-rich tasks to “act on” and resolve incidents
Promote collaboration with ChatOps	• Break down silos across IT, Sec, cloud, DevOps to democratize security
PLATFORM	
Flexible deployment model	• MSPs and enterprises can use the platform to create and provide a variety of services to external and internal customers
Achieve cloud security	• Understand security posture from on-premise to cloud
Streamline onboarding and configuration	• DIY / self-service - go at your own pace • Customer, device, and context onboarding wizards
Maintain transparency	• Share cybersecurity insights and track efforts across teams, functions, and service providers
Support multitenancy for service providers	• Onboard and support end-clients’ individual tenant and firewall their data
	• Customer, device, and context onboarding wizards