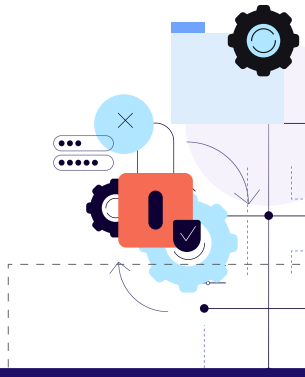
NETENRICH

SOLUTION OVERVIEW

Resolution Intelligence™:

Analytics to Improve Threat Detection



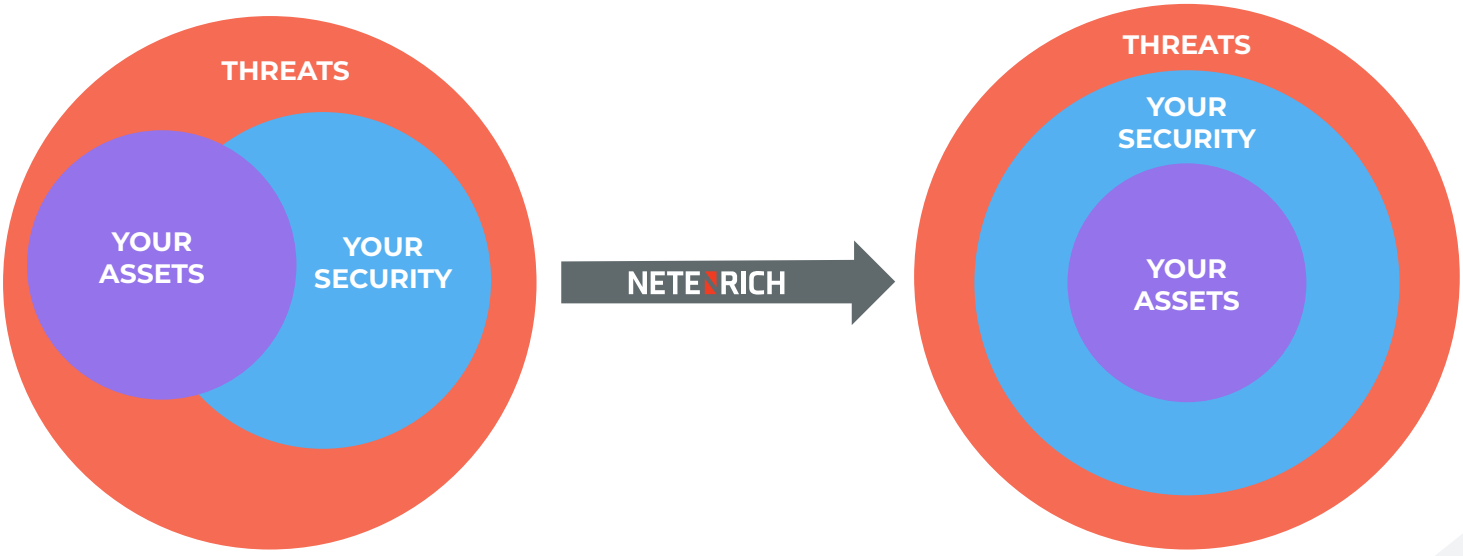
"Can we prioritize threats and act quickly without adding to our ops challenges?"

Yes, you can. Netenrich Resolution Intelligence™ delivers analytics for threat detection through a powerful platform to improve your security monitoring, speed the right response, and strengthen resilience as you scale.

The legacy approach to security operations (SecOps) — throwing more tools and specialists at the problem — adds to perennial challenges with managing tools, maintaining skills, and battling the deafening noise. Resolution Intelligence offloads these challenges from your team and adds context to drive the right action based on risk to the business.

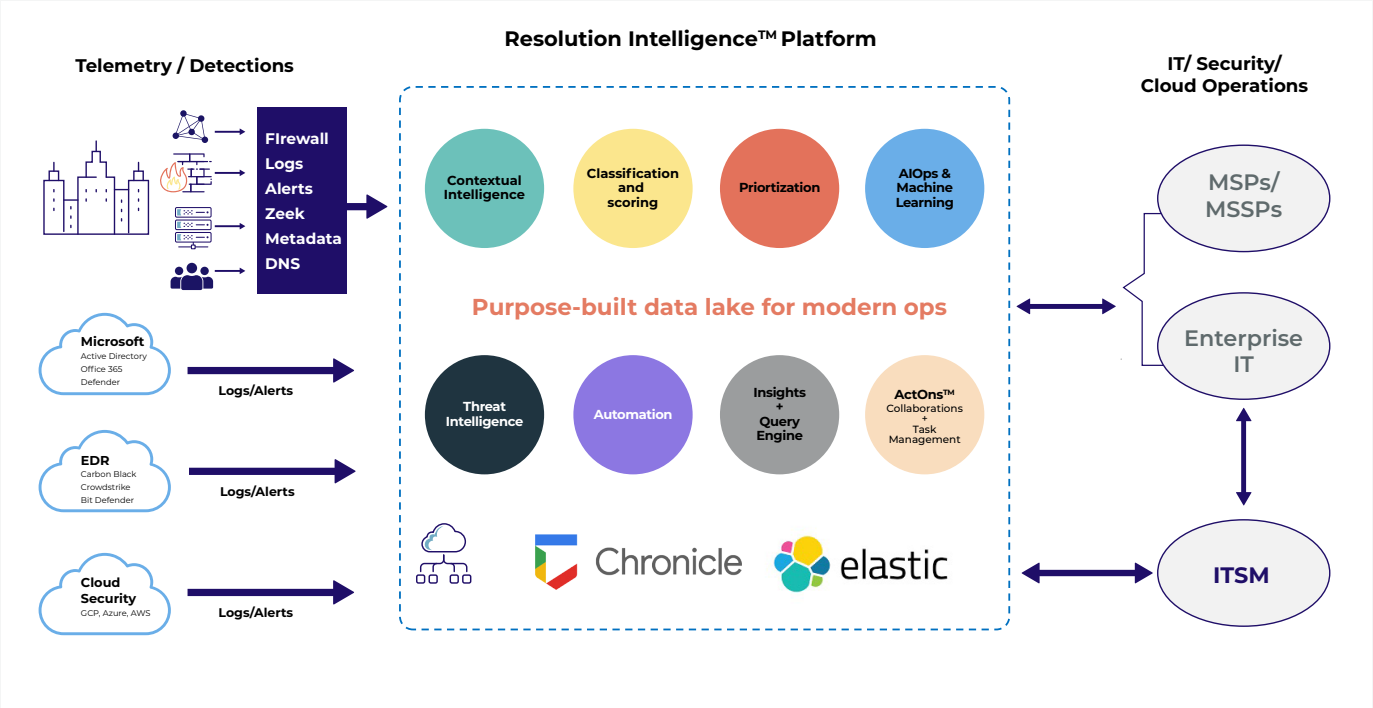
Highlights

- Safeguard uptime
- Maximize value from tool investments
- Always know what matters – and what to do about it
- Improve readiness, response, resilience
- Keep SecOps aligned to business risk



Insight to “ActOns” in a Fraction of the Time

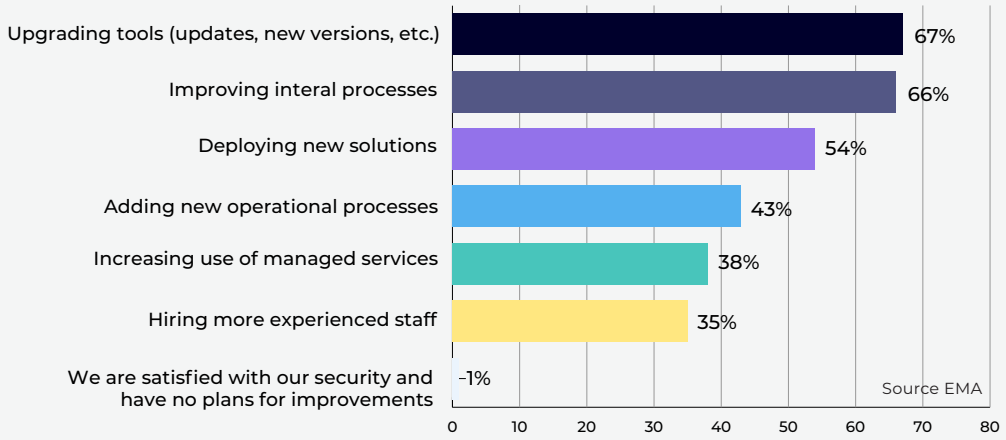
With too many tools generating too many alerts and false positives for L2/L3 teams to process, Netenrich automates and offloads integration and management to drive efficiencies across monitoring, detection, and response. While offloading tool administration, the Netenrich solution correlates input on threats arising from endpoints, applications, hybrid infrastructure, and user behavior. The platform ingests and enriches security telemetry with threat feeds, OSINT data, CVE information, and expert insights to provide granularity and context for investigation and triage.



Netenrich Resolution Intelligence Threat Detection Platform

The Resolution Intelligence Platform uses AIOps to reduce noise and automatically applies 12+ years’ codified ops expertise to prioritize and fully contextualize ActOns for cyber-defenders. The platform bridges skills gaps by automatically engaging the right responders and equipping them with exactly the right insights to resolve risk quickly, or even proactively. Flexible options support managed service provider (MSP) and hybrid SecOps models now gaining in popularity at every-size enterprise.

How is your company planning on improving its cybersecurity posture?



"More" is not the answer. While two-thirds of survey respondents planned to buy more security tools, more than half also reported issues with integration and management. With threats on the rise and security budgets flat, 30% plan to increase use of managed services to offload the burden of maintaining specialized systems and skills.

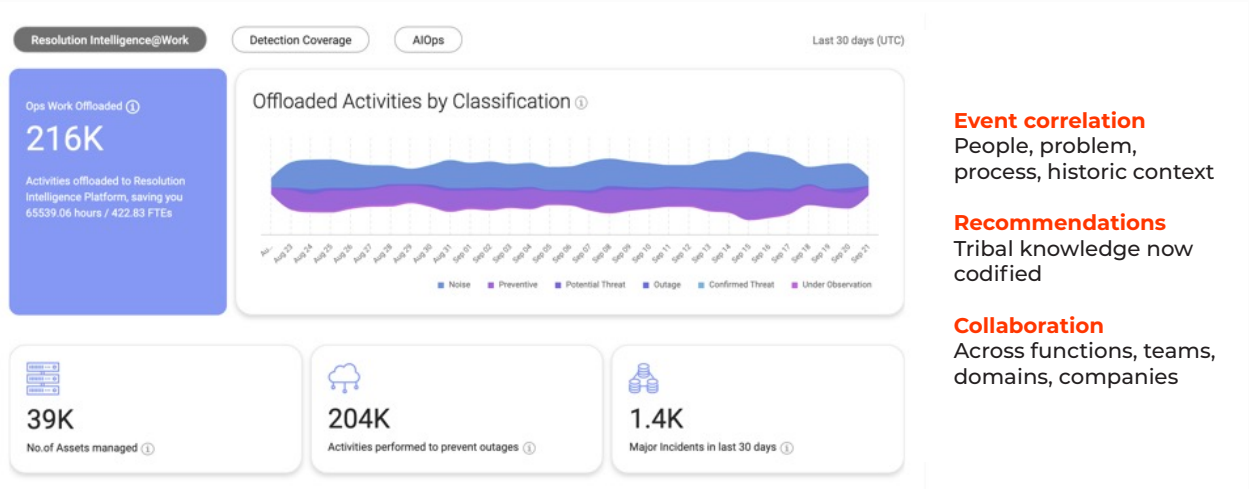
Prioritization + context = Smarter response, resolution, resilience

The Netenrich platform automatically focuses your efforts on mitigating internal and external risk that requires immediate action. Continuous validation of threat detection keeps you a step ahead of serious attacks actually targeting your assets.

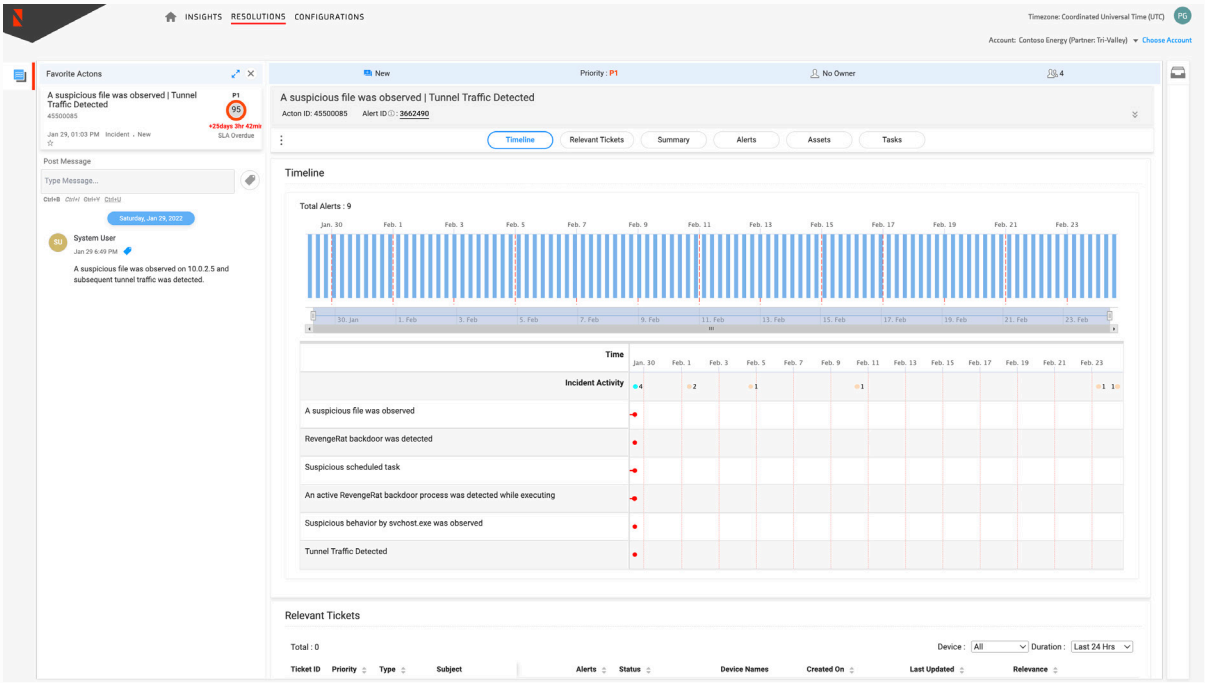
With automated risk scoring and 100% mapping of all alerts to MITRE ATT&CK de facto standards, we spot indicators during all important phases of an attack. For example, signs that an adversary may be evaluating hosts for compromise or trying to use stolen credentials.

Resolution Intelligence enables rapid action and proactive resilience:

- Automated investigation, risk scoring, noise and false positive reduction
- Incident management and war room capabilities
- A converged data set for IT, cloud, Dev-, and SecOps
- Common data lake for all security telemetry
- Threat hunting with built-in threat intelligence
- Single-pane-of-glass visualization
- Support for multi-tenancy



Your tools and teams work smarter and faster. Netenrich Resolution Intelligence enhances threat detection by offloading time-consuming correlation, investigation, and analysis to automate and speed response and resolution. Efficiencies increase over time as the platform leverages AIOps and machine learning (ML) to resolve more incidents and codify tribal knowledge to improve monitoring and detection.

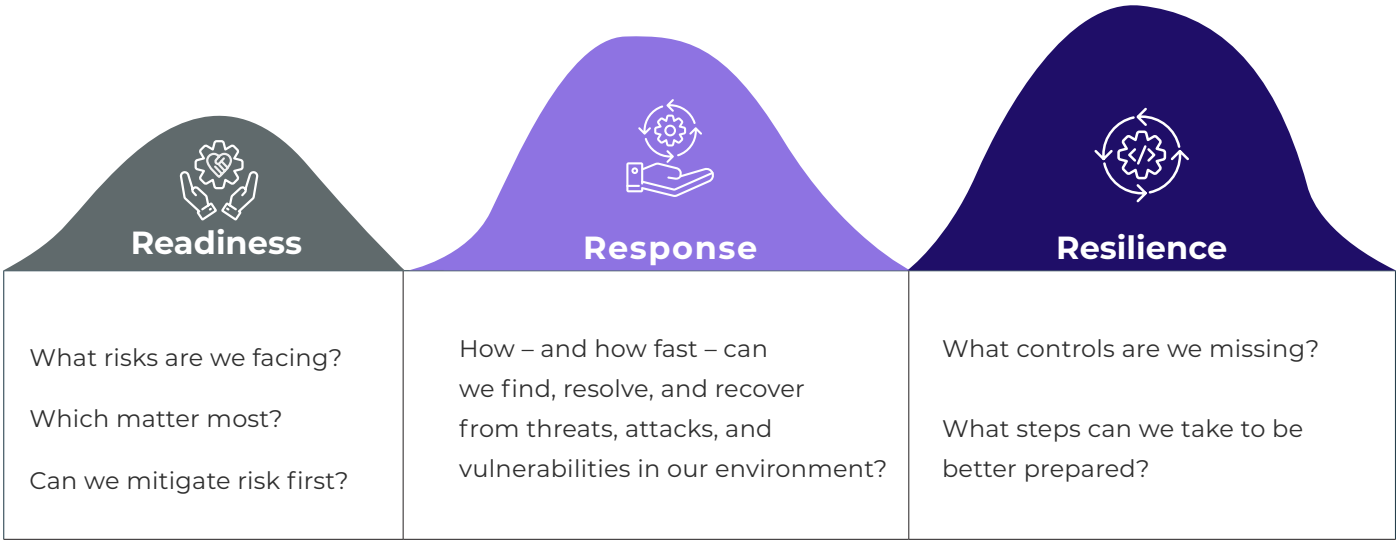


Transparent incident management and scoring. Incidents and relevant resolvers are automatically scored by Netenrich AI/ML engines based on business context. Incident management is collaborative via ChatOps to enhance transparency and break down silos across teams and functions.

Resolve to be Resilient — and Stay Aligned

Built by seasoned cybersecurity veterans with a broad range of skills and specialization across threat detection, incident response, risk management and security research, Netenrich's data-driven Resolution Intelligence Platform keeps operations aligned to risk. A purpose-built user interface (UI) provides visibility into open tickets with guided remediation steps for a lasting advantage over ransomware, malware, and other crippling cyberattacks.

Netenrich delivers transparency, flexibility, and scale to give MSPs and in-house operations teams one trusted source for actionable data and predictive analytics as operations scale. Our platform leverages automation and experience running operations for more than 6,000 organizations in one powerful software-as-a-service (SaaS) platform to drive awareness as or before you need it, and keep ops aligned with risk.



Try It Risk Free

Try Netenrich Resolution Intelligence to streamline SecOps, speed the right response, and strengthen your cyber risk posture.

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 re-sponse 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 • Multi-level 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 DevOps 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 multi-tenancy for service providers	• Onboard and support end-clients’ individual tenant and firewall their data