NETENRICH

RESOLUTION BRIEF

Managed Endpoint Detection & Response (EDR)

Keep the Odds in Your Favor with Smarter Detection & Response

Where do most of today's cyberattacks originate (hint: it's not from the cloud)? Same as it's been for decades — endpoints — because leveraging endpoints to launch malware and ransomware into your environment is simple, and adversaries like things simple.

To stack the odds in your favor, *Managed Endpoint Detection and Response* makes defending your various endpoints against attack much simpler as well. Whether you have EDR solutions in place or not, our managed solution equips your IT and Security experts to monitor, intercept, and respond to suspicious activity before it can damage assets or your brand.

Endpoints as starting points

66% of organizations surveyed incurred huge revenue losses through ransomware attacks and more than half suffered damage to their brand.

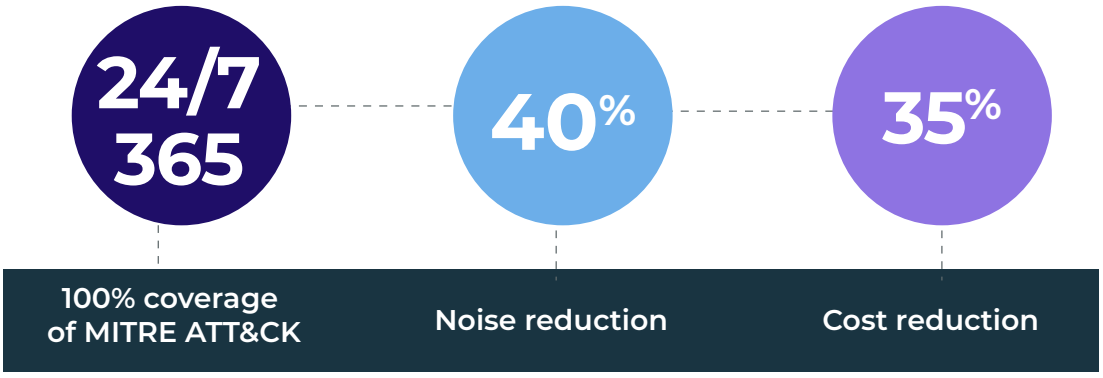
Tech Republic

68% of organizations fell victim to endpoint attacks within the past 12 months.

Ponemon

"The most common source of hacks are compromised credentials used to establish a beach head on user endpoints."

Security Week

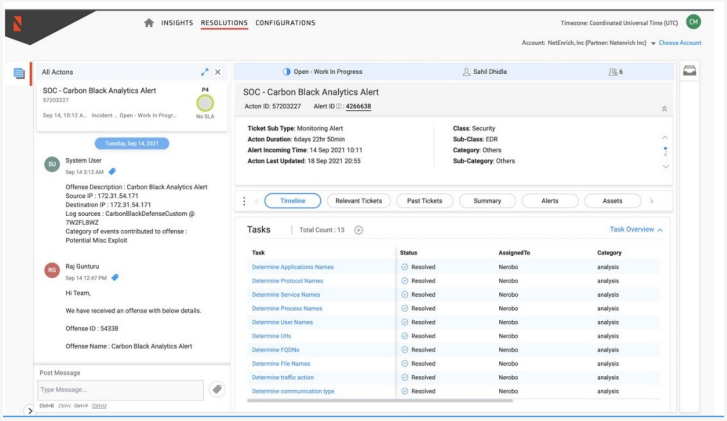


Netenrich's advanced AI platform and digital operations experts manage tool configuration, eliminate false positives, and investigate real alerts so defenders can mount the right response quickly. Round-the-clock coverage and rich contextualization makes it easier to prioritize security operations (SecOps) efforts around high-impact threats to your business — without bombarding your team with noise.

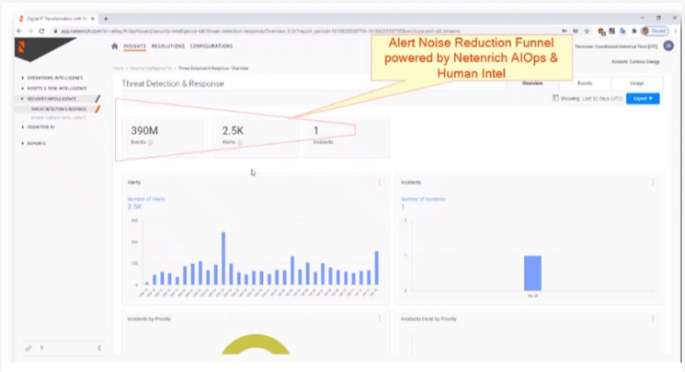
Know and act on what matters

Netenrich Resolution Intelligence delivers full cyber-situational awareness to defenders on an ongoing basis. We offload and automate the time-consuming process of correlating endpoint data with threat and attack surface intelligence to assess risk. The result: managed EDR that equips responders to take the right steps at the right time, faster and with less effort.

The Netenrich platform integrates with market-leading EDR solutions such as VMWare Carbon Black, CrowdStrike, Microsoft Defender for Endpoints, and SentinelOne for easy onboarding and configuration. Managed EDR creates a comprehensive, intelligent hub for data collection, correlation, and analysis to secure all your endpoints — desktops, laptops, and servers (Windows, Mac, Linux).



Transparent incident management, full EDR context, AI/ML-scored act-ons, and ChatOps collaboration capabilities are standard through the integration of Managed EDR with the Netenrich Resolution Intelligence® platform.



A better "day in the life": Easy-to-read dashboards depict steadily increasing noise and workload reduction achieved with Managed EDR.

Netenrich offers managed security service providers (MSSPs) and enterprise IT teams full transparency from detection through resolution. We equip your defenders to:

See the right data
Software agents monitor and collect endpoint data such as executions, cross processes, network connections, software inventory and registry/file modifications.

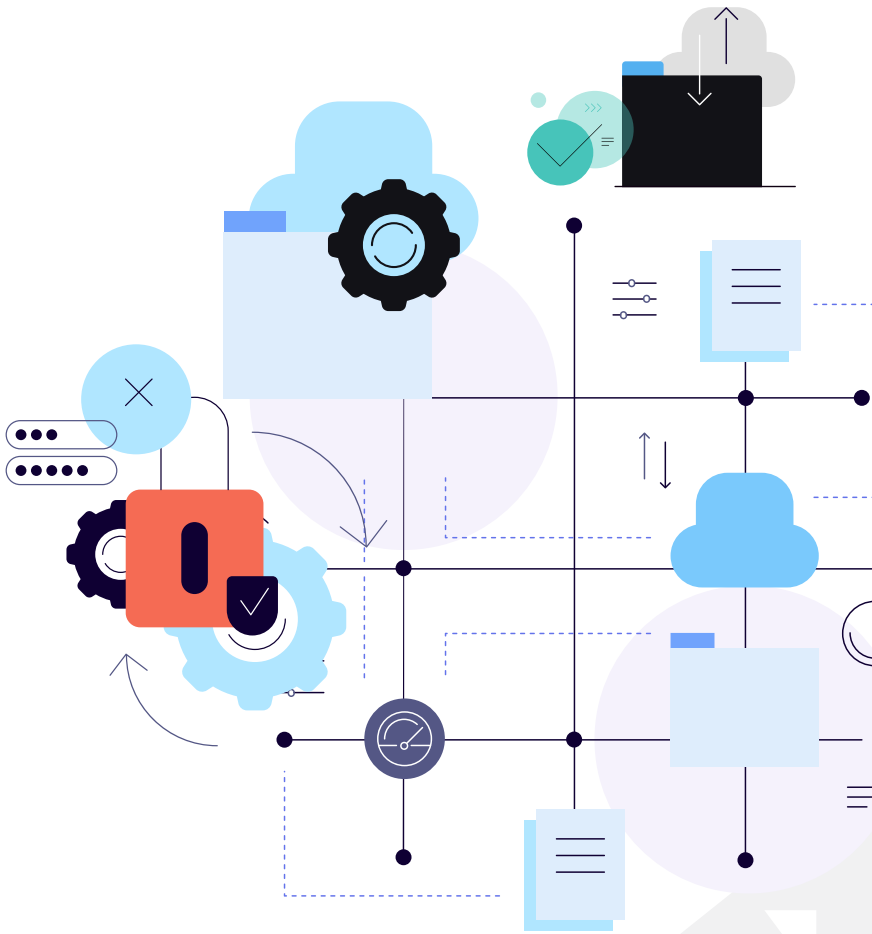
View threats in context
Our proprietary big data platform performs event correlation across people, problems, processes, and historic context. We generate recommendations based on dynamic machine and expert intelligence.

Know what to do first
Preconfigured rules, correlation, and analytics recognize when endpoint data indicates a known security breach or an incident triggers a valid alert.

Find threats before they find you
Managed EDR digs deeper to find malicious actors that have slipped past your endpoint security defenses. We work closely with you to understand your environment and inform threat hunting, threat modeling, adversary emulation, and other SecOps efforts.

Automate and speed response
Upon spotting patterns, our AI and machine learning (ML) engines can initiate automated responses to quarantine endpoints or intercept potential threats. For those that cannot be auto-resolved, we up-level tickets with full context and insights to mitigate risk faster. The platform also enables powerful chat-ops collaboration capabilities to break down silos and speed resolution.

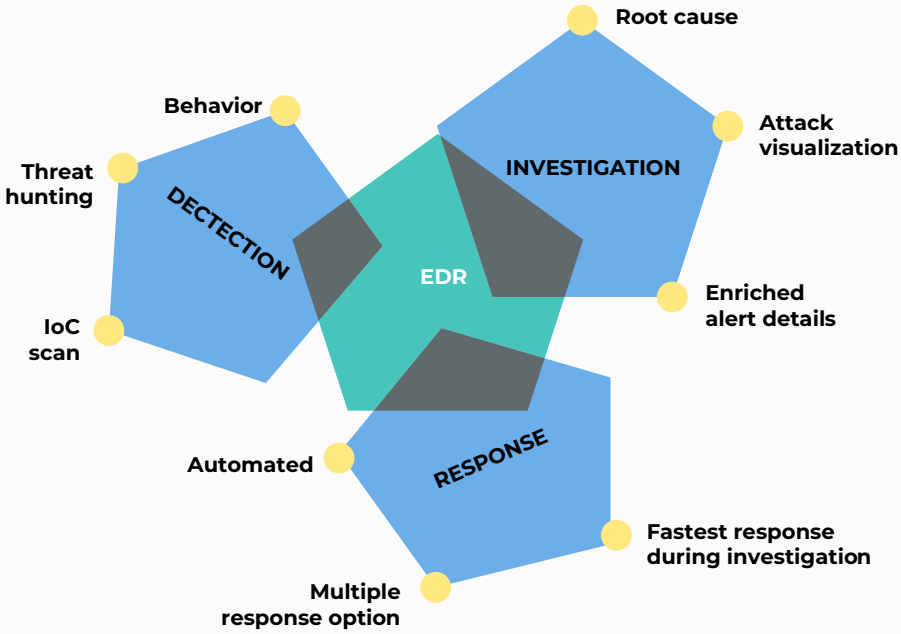
Shrink your attack surface
Netenrich Resolution Intelligence dashboards track trending patterns and efficiency improvements such as noise and workload reduction.



Netenrich Resolution Intelligence® for cybersecurity

Netenrich's Resolution Intelligence embodies 12+ years' digital Ops expertise and best practices. Resolution Intelligence keeps endpoint security aligned to your changing business and IT initiatives such as work from home, cloud migration, and device upgrades. Our unrivaled mix of AI, ML, and codified tribal knowledge frees your analysts to up-level activities to reduce cost and retain top talent.

We modernize digital operations around faster and more proactive resolution, stronger compliance, and next-level digital Ops efficiencies. We equip IT and Security teams to realize higher value from tool investments and scale operations to drive innovation that transforms your business.



Netenrich Resolution Intelligence® delivers a superior customer experience from easy onboarding to proactive investigation to full transparency. Our repeatable, risk-based process generates rich analytics to improve your cybersecurity posture over time.

Try Managed EDR today

Engaging a managed EDR provider should bring more investment flexibility, not less. Act now to experience the agility, responsiveness, and expertise you need to keep risk aligned with security operations.

Managed EDR specifications

CATEGORY	FUNCTION	CAPABILITIES
DETECTION AND MONITORING	MONITORING	• EDR alerts brought into the Netenrich platform and monitored 24/7 • Custom watchlists and use cases created for specific customer environments based on EDR threat detection capabilities
	INCIDENT ESCALATION	• Real-time incident management with tickets created by Netenrich Managed EDR analysts • Tickets escalated to EDR team to perform triage, impact assessment, remediation, and preventive enhancements
	MITIGATION AND CONTAINMENT GUIDELINES	• Detailed mitigation steps provided for each ticket • Option to quarantine infected hosts to avoid lateral movement or data exfiltration
	INCIDENT RESPONSE	• Playbooks support initial automated response • Secure connection for incident responders to remediate infected hosts • Detailed remediation steps for every ticket
INTEGRATIONS	ALERT INGESTION & EDR ADMINISTRATION	• Expert insight into how trending threats affect your business and critical assets
ADVANCED ANALYTICS & REPORTS	REPORTING	• Advanced analytics • Standard and custom reports on EDR performance and incident management in the environment
SUPPORT	SERVICE DESK	• Interfaces with customer IT and Security teams
SERVICE DELIVERY	MANAGEMENT	• Service Delivery Manager (SDM)
STATUS REVIEW SUMMARY CALLS	ONLINE AND WEB MEETINGS	• Monthly call to discuss the security and health trends and top incidents • Managed EDR consulting available
ADD-ON SERVICES		
THREAT HUNTING	ADVANCED	• Custom hypothesis-driven threat hunting • Additional capabilities deployment