

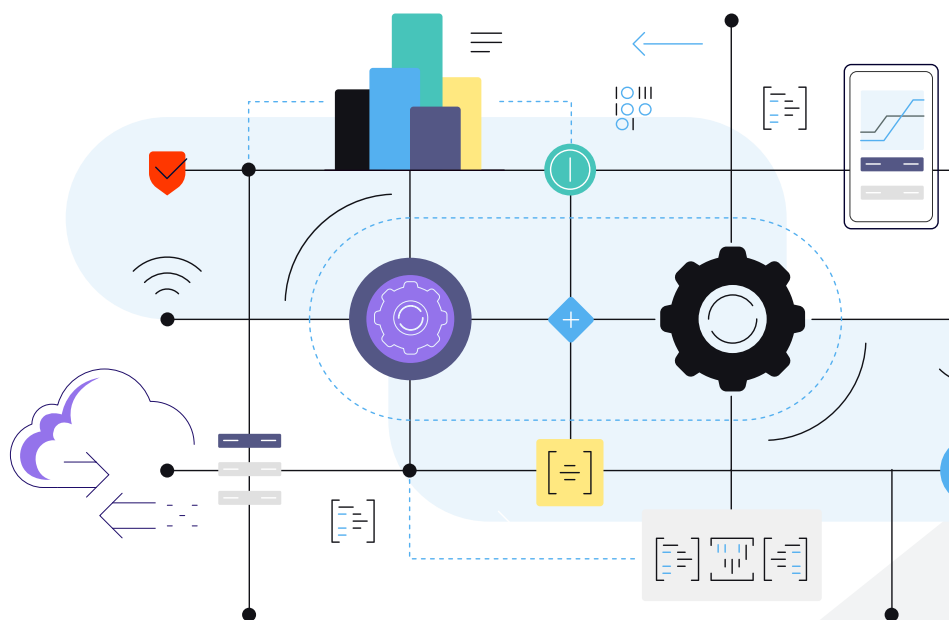


Resolution Intelligence™ for Threat Detection: Managed Security for Microsoft Defender for Endpoint & Office 365

Improve readiness, response and resilience – all with one platform

Built-in cybersecurity adds an invaluable layer of protection against today's rampant ransomware, supply chain, and business email compromise (BEC) attacks – if your team has time to apply the benefits. Netenrich Resolution Intelligence™ offloads administration and enhances the value of Microsoft Defender for Endpoint and Microsoft Defender for Office 365 so you can easily achieve less risk with less effort.

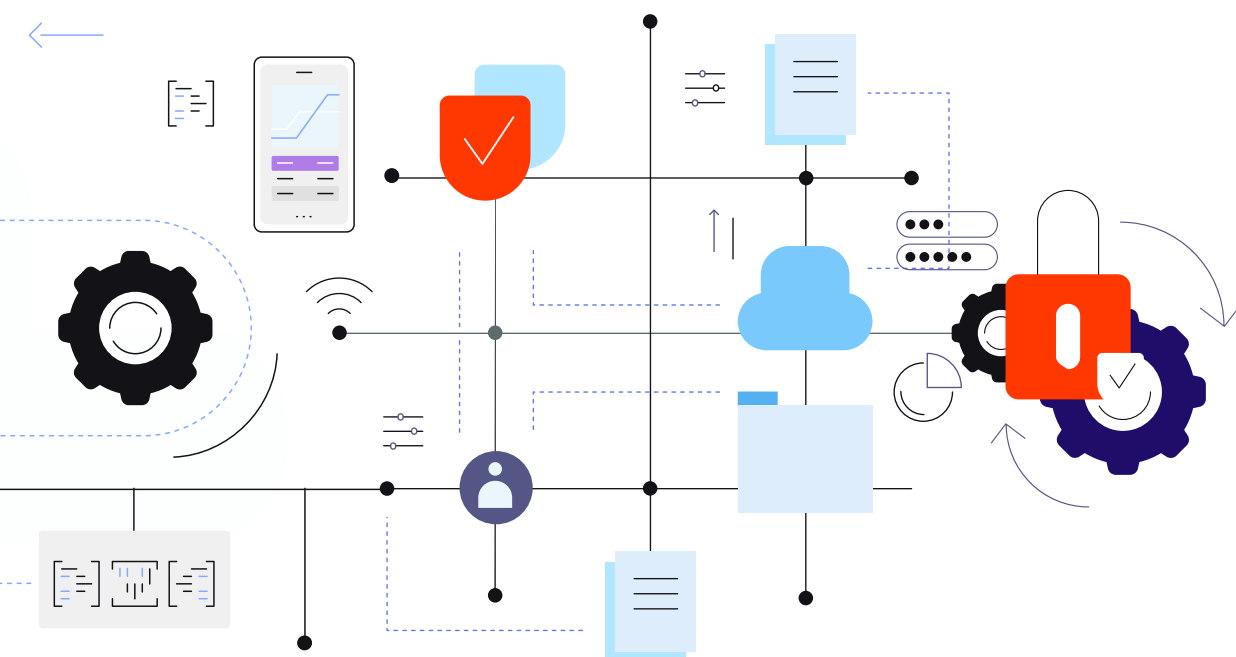
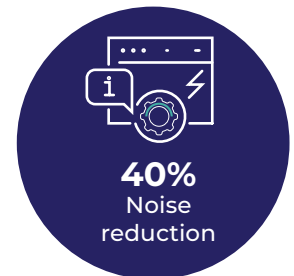
Microsoft Defender delivers automated detection and response capabilities to deflect cyberattacks and optimize security operations (SecOps). Netenrich Resolution Intelligence lets MSP/MSSP partners onboard and manage diverse customers using a single platform to deliver incident management, perform triage, and correlate with other threat vectors (network, cloud, SaaS). Our platform ingests, correlates, and investigates Defender alerts to provide SecOps with fully contextualized and actionable incidents.



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 ops 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.



Here's how our platform combines with Microsoft security controls to protect your business and IT environments from breaches and make your cyber risk posture stronger.

Microsoft Defender for Endpoint

The majority of cyber threats still originate from endpoints. Resolution Intelligence combines with Microsoft Defender for Endpoint to achieve complete endpoint security across Windows, macOS, Linux, Android, iOS, and network devices.

Microsoft Defender for Endpoint supports vulnerability management, endpoint detection and response (EDR), mobile threat defense, and threat hunting in a single, unified platform. The Netenrich platform integrates with Microsoft Defender for Endpoint for easy onboarding and configuration.

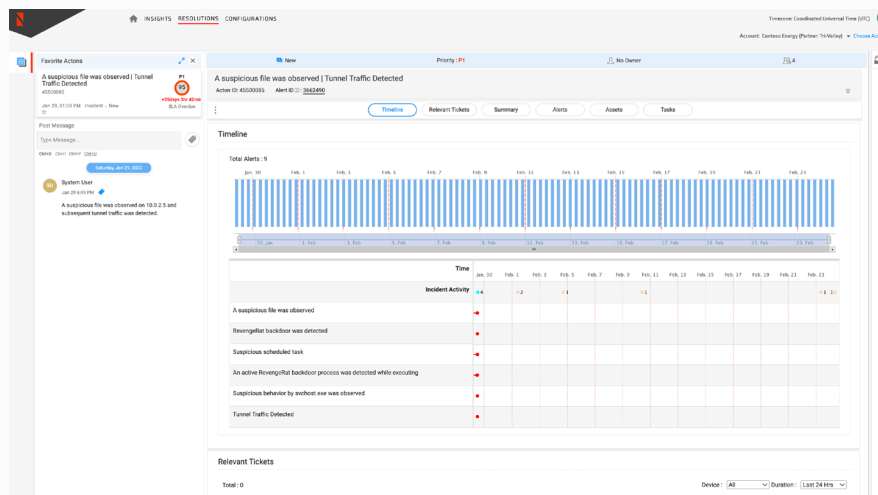
Netenrich Managed EDR creates a comprehensive, intelligent hub for data collection, correlation, and analysis to secure desktops, laptops, and servers. MSSPs can:

- Launch threat hunting services
- Create and push custom detection rules to all or a subset of customers based on risk
- Focus vigilance on critical assets and threat actors exploiting known exposures
- Integrate with leading IT Service Management (ITSM) systems

Microsoft Defender for Endpoint delivers industry-leading endpoint security . . . to rapidly stop attacks, scale your security resources, and evolve your defenses. It's delivered at cloud scale, with built-in AI that reasons over the industry's broadest threat intelligence.

Microsoft





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

Microsoft Defender for Office 365

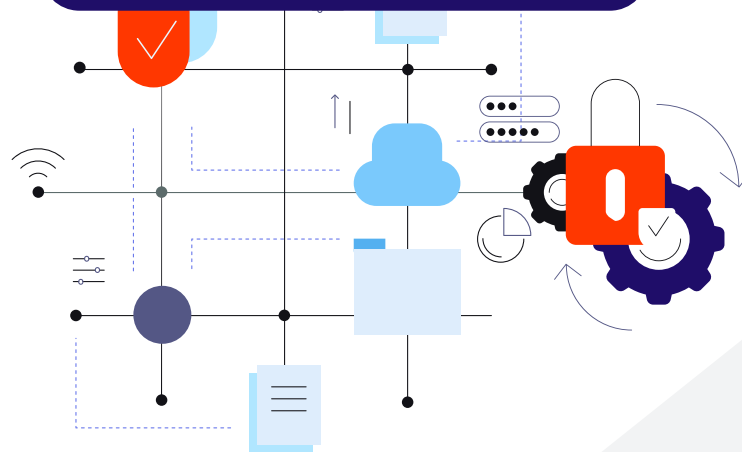
Email now represents the primary attack vector for cybercrime. Netenrich combines with Microsoft's integrated threat protection for Office 365 to prevent a variety of volume-based and targeted attacks including business email compromise, credential phishing, ransomware, and advanced malware.

Microsoft Defender for Office 365 builds on the core safeguards offered by Exchange Online Protection (EOP) available in any subscription featuring Exchange Online mailboxes. The solution automatically investigates and remediates attacks.

Offloading multi-tenant management to the Netenrich Resolution Intelligence Platform simplifies administration, speeds alert handling, and improves incident response. Integrated Microsoft-Netenrich security solutions track attacks across Office 365 with advanced hunting capabilities that help identify, prioritize, and investigate threats and attacks.

In The Forrester Wave™: Enterprise Email Security, Q2 2021 analysis, Microsoft Defender for Office 365 received the highest possible score in the incident response, threat intelligence, and endpoint and endpoint detection and response (EDR) solution criteria.

Microsoft



Resolution Intelligence for Microsoft Defender: Scale and Simplify SecOps

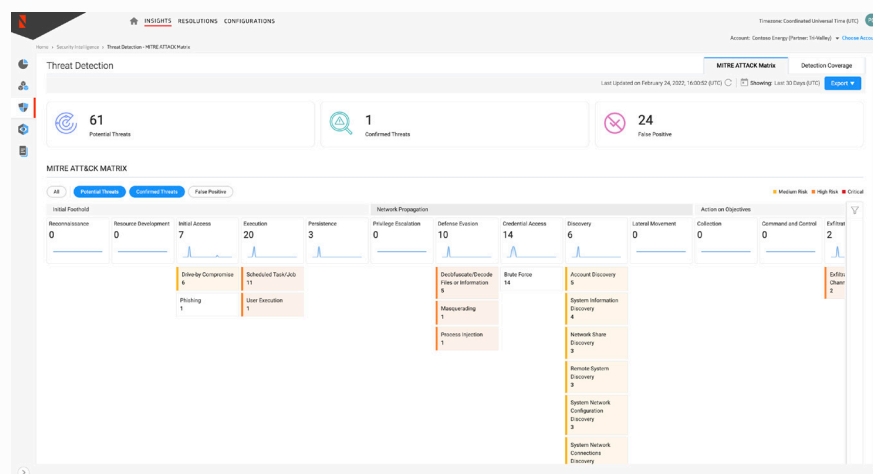
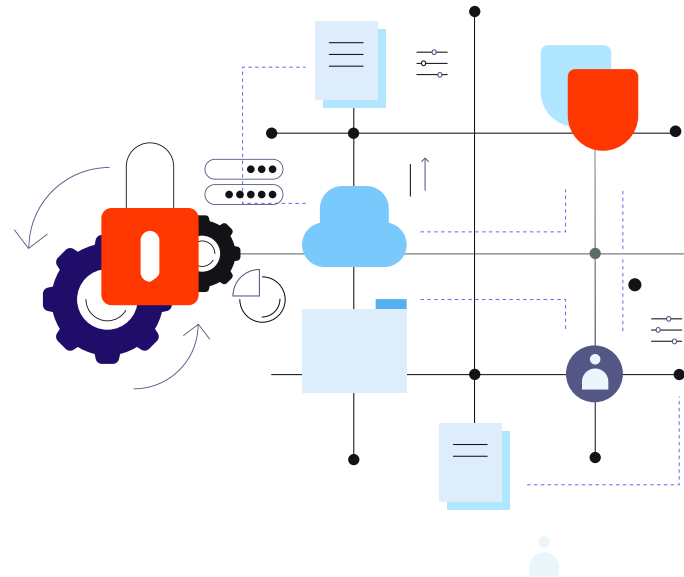
Netenrich equips defenders with more and better context to act while promoting resilience and scale across IT, security, and cloud operations. Full transparency from detection through resolution improves your ability to:

Detect & prevent: Find threats before they find you

Netenrich capabilities for managed threat detection let defenders dig deeper to find malicious actors that have slipped past front-line security defenses. We work closely with you to understand your environment and inform threat hunting, threat modeling, adversary emulation, and other SecOps efforts.

Understand and prioritize risk

Netenrich automates the time-consuming process of correlating endpoint data with threat and attack surface intelligence to assess risk. Our proprietary big data platform performs event correlation across people, problem, process, and historic context. We generate recommendations based on dynamic machine and expert intelligence.



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

Try Resolution Intelligence for Microsoft Defender Today

Stack the odds in your favor to make defending your environment from breaches easier, and your fast-changing risk posture stronger. Act now to experience the power of solutions combining Microsoft Defender with Resolution Intelligence to boost the agility, responsiveness, and depth of your security operations risk free.

Specifications

CATEGORY	FUNCTION	CAPABILITIES
DETECTION AND MONITORING	ENDPOINT MONITORING	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Real-time incident management with tickets created by Netenrich analysts Tickets escalated to response team to perform triage, impact assessment, remediation, and preventive enhancements
	THREAT HUNTING & INTEGRATED INTELLIGENCE	<ul style="list-style-type: none"> Unfiltered telemetry promotes proactive threat hunting Integrates with Netenrich Global Contextual Threat Intelligence platform and supports custom use cases and watchlists to detect attacks in early stages
	MITIGATION & CONTAINMENT GUIDELINES	<ul style="list-style-type: none"> Detailed mitigation steps provided for each ticket Option to quarantine infected hosts to avoid lateral movement or data exfiltration
	INCIDENT RESPONSE	<ul style="list-style-type: none"> Playbooks support initial automated response Secure connection for responders to remediate infected hosts Detailed remediation steps for every ticket
INTEGRATIONS	ALERT INGESTION & ADMINISTRATION	<ul style="list-style-type: none"> Tool integration, setup, configuration, and maintenance
ADVANCED ANALYTICS & REPORTS	REPORTING	<ul style="list-style-type: none"> Advanced analytics Standard and custom reports on EDR performance and incident management in the environment
SUPPORT	SERVICE DESK	<ul style="list-style-type: none"> Interfaces with customer IT and Security teams
SERVICE DELIVERY	MANAGEMENT	<ul style="list-style-type: none"> Service Delivery Manager (SDM)
STATUS REVIEW SUMMARY CALLS	ONLINE & WEB MEETINGS	<ul style="list-style-type: none"> Monthly call to discuss the security and health trends and top incidents Managed EDR consulting available