EXTRAHOP

ExtraHop Managed Network Detection and Response

Managed by BINARY DEFENSE

ExtraHop Managed Network Detection and Response (mNDR) provides the ExtraHop industry-leading network detection and response platform, Reveal(x) 360, as a managed service. Cybersecurity experts, in a U.S. based 24x7x365 security operations center, utilize the power of ExtraHop to eliminate blind spots, detect lateral movement, and respond to advanced threats other tools and in-house staff can miss. As a result, ExtraHop mNDR can help stop breaches 84% faster, provide agentless visibility, packet-level granularity, and security at scale.ExtraHop NDR, managed by Binary Defense, excels here, providing peace of mind in a turbulent and uncertain world.

Optimize Your Security Posture

The core cybersecurity issue for many companies is the limited number of resources, time and in-house experts available to protect their organization in a post-compromise world. This means the question is not if you will be breached, but when, and how will your stretched IT or security team be able to deal with this incident?

Cybersecurity experts, utilizing Binary Defense managed Extrahop, have east-west and north-south visibility 24/7 into your network which allows them to identify insider, rogue and low-and-slow attacks. Using advanced behavioral analytics and context-rich investigative workflows, we can optimize effective threat detection and response faster and more effectively than most in-house teams.

Human Analysis Enabled By Powerful Analytics

The ExtraHop NDR platform transforms raw network traffic (including SSL/TLS encrypted traffic) into wire data analytics at up to 100 Gbps of sustained throughput, automatically discovering, classifying, and mapping every asset, device, and user in your environment in real time. This means no more visibility gaps, and no means for attackers to disable or evade monitoring as with log, agent or signature-based tools.

In a post-compromise world, human analysis enabled by powerful analytics is essential to identifying and remediating advanced and persistent threats. ExtraHop mNDR excels here, providing peace of mind in a turbulent and uncertain world.

ExtraHop mNDR is managed by Binary Defense

ExtraHop mNDR is operated and managed by Binary Defense, recognized as a Strong Performer in Managed Detection & Response by Forrester, a Top 250 MSSP by MSSP Alert, and a representative vendor in the Gartner Market Guide for Managed Detection & Response.

When you partner with ExtraHop and Binary Defense you get a team of experts that includes Security Operations Center (SOC) Analysts, Shift Leads, a SOC Manager, Chief Security Officer, Client Support, Product Development, Threat Hunting,

EXTRAHOP MNDR KEY BENEFITS

- 24x7x365 monitoring, analysis and remediation
- Access to a team of security experts
- 12-minute average response time, 30-minutes guaranteed
- Ongoing security posture improvement with monthly reports and quarterly business reviews
- No learning curves
- No technology implementations
- No SOC build out
- No skill gaps
- No new hires
- Immediate threat protection for a post-compromise world
- Predictable operating expense

World Class Product and Expertise, Delivered by Binary

As a customer of ExtraHop mNDR delivered by Binary Defense, your company benefits from unmatched expertise and experience in detection engineering, analysis, investigations, remediation guidance, and incident support around the clock. Technology, security operations, and expertise – all so your precious and limited resources can focus on more important things.

An Extension of your Team

Our goal with every customer is to be an extension of your team, providing 24x7x365 protection against increasingly sophisticated adversaries. Binary Defense SOC analysts are skillfully trained to monitor for malicious behavior and provide instructions on the best way to remediate a threat before it causes damage.

Proven Detection and Response Process

Onboarding	Detection/Notification	Investigation	Escalation	Remediation
Dedicated project manager and technical leader assigned during onboarding Detection engineers conduct detection assessments and tune as required Binary Defense detection strategy deployed	24x7x365 Security Event Monitoring Event Triage and Dispositioning. SOC analysts validate the alerts, false positives become tuning candidates SOC Analysts prioritize alerts by time and severity SOC Analysts call client within 30min for critical events, average time is 12min	SOC Analysts conduct full Kill Chain analysis, attack reconstruction and synthesis SOC Analysts identify key IOCs across the Kill Chain New IOCs deployed to client environment Defense in depth approach to protecting	Investigations include tactical and strategic mitigation recommendations and are escalated within established SLAs True positives are escalated reducing the quantity of alarms through tuning and analysis Personalized service and customized escalation procedures by ticket severity	SOC Analysts conduct full Kill Chain analysis, attack reconstruction and synthesis SOC Analysts identify key IOCs across the Kill Chain New IOCs deployed to client environment Defense in depth approach to protecting

Why ExtraHop Managed NDR

ExtraHop mNDR managed by Binary Defense, is an easy path to complete visibility, advanced threat detection and intelligent response in a post compromise world. An offensive-minded service, security analysts investigate threats using full Cyber Kill Chain analysis to provide deep contextual insights with tactical and strategic mitigation recommendations for your team. As a result, we can discover and prevent threats early in the attack lifecycle.

An extension of your team, ExtraHop mNDR provides 24x7x365 eyes-on-glass detection and response capabilities that improve your security posture and keep your team focused on their mission-critical objectives.

The combination of security experts, a curated technology stack featuring the industry-leading, cloud-native ExtraHop network detection and response platform, and a U.S. based 24x7x365 security operations center, provides a scalable, turnkey security solution at a fraction of the cost, time and resources needed for an enterprise SOC.

ABOUT EXTRAHOP AND BINARY DEFENSE

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX network detection and response (NDR) platform uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

Binary Defense is a trusted leader in security operations, supporting companies of all sizes and industries to proactively monitor, detect and respond to cyberattacks. The company personalizes a Managed Detection and Response solution, including advanced Threat Hunting, Digital Risk Protection, Phishing Response, and Incident Response services, helping customers mature their security program with confidence.

EXTRAHOP™

info@extrahop.com
extrahop.com

BINARY DEFENSE™

sales@binarydefense.com
binarydefense.com