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 blindspots, detect lateral movement, and respond to advanced threats other tools and in-house staff can miss. As a result, ExtraHop mNDR is able to stop breaches 84% faster, provide agentless visibility, packet-level granularity, and security at scale.

NDR- An Essential Security Tool for Your Organization

NDR is a key component in a modern security program. It examines all traffic, clear and encrypted including TLS v1.3 that crosses the wire and doesn't suffer from blind spots like solutions that rely on less- than-complete content. NDR offers the most accurate insight into the attack chain, to provide an aggregate picture and reduce response time.

ExtraHop's technology uses cloud-based machine learning to analyze network wire data, exposing Layer 2-7 threats and threats hiding in encrypted traffic. Our solution:

- Identifies threats by analyzing every packet and network activity on-premises or in the cloud
- Identifies anomalous or malicious activity and potentially lateral movement
- Automates investigations and drives incident response with more complete data, resulting in higher confidence remediation

For many companies, the three core cybersecurity issues are limited funding, time and in-house expertise. Companies both large and small are over-tasking their security operations (SOC) staff, leading to missed opportunities to stop attacks, staff burnout, and in some cases attrition. 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 Extrahop, have continuous east-west and north-south network visibility which allows them to identify difficult-to-spot insider threats, including "low-and-slow" attacks. Using advanced behavioral analytics and context-rich investigative workflows, ExtraHop mNDR delivered by Binary Defense can optimize effective threat detection and response faster and more effectively than most in-house teams.

Highly Scalable, Machine Driven Security Insights

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. Whether it's unmanaged OT devices, unconfigured or unmanaged hosts, or other unknowns in your infrastructure, ExtraHop virtually eliminates blind spots so security teams can have confidence in their security posture without relying on agents which can be evaded or logs that can be altered.

In a post-compromise world, the combination of human analysis enabled by powerful analytics is essential to rapidly identifying and remediating threats to minimize their impact. ExtraHop mNDR provides peace of mind and a sense of trust for security leaders.

ExtraHop mNDR Key Benefits

- 24/7 monitoring, analysis and remediation support
- 12-minute average response time, 30-minutes guaranteed
- Rapidly accelerated time to value of ExtraHop platform purchase
- Expertise on demand – no need to hire additional staff
- Product expertise – eliminating the learning curve and skills gap
- Immediate threat protection for a post-compromise world
- Ongoing security posture improvement identifying weaknesses in the customer infrastructure
- Business engagement – monthly reports and quarterly business reviews
- Integrated service – ExtraHop NDR integrated into Binary Defense SOC
- Predictable operating expense

World Class Product and Expertise, Delivered by Binary Defense

ExtraHop mNDR is operated and managed by Binary Defense, recognized as a Leader 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.

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.

Extend Your Team's Expertise and Capabilities Without Adding Staff

Our goal is to be an extension of your team, supporting existing or adding new Security Operations Center (SOC) capabilities, 24x7x365, against increasingly sophisticated adversaries. You can rest a little easier knowing the combination of ExtraHop and Binary Defense is working hard to identify, investigate, and remediate threats before they can critically impact your business.

Proven Detection and Response Process

Onboarding

Dedicated project manager and technical leader assigned during onboarding

Detection engineers conduct detection assessments and tune as required

Binary Defense detection strategy deployed

Detection/Notification

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 30 minutes for critical events.

Average notification time is 12 minutes

Investigation

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

Escalation

Completed investigations with tactical and strategic mitigation recommendations 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

Remediation

In the event of a breach, the SOC team works with customers to help develop a strategic plan to remedy the attack and prevent additional damages

Why ExtraHop Managed NDR

The industry's leading NDR, an essential tool for visibility and threat detection, plus world-class security expertise from Binary Defense. This powerful combination of technology and expertise is now delivered as a service.

Binary Defense brings deep technical knowledge of the ExtraHop platform coupled with offensive-focused security expertise, applying the Cyber Kill Chain methodology to detect, identify, investigate, and remediate threats to your business with powerful precision. High confidence, rapid detection of threats, with precise and timely remediation guidance reduces the damage a threat actor can have on your company, period.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats–before they compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

Request a Free Trial **extrahop.com/request-free-trial** | Take the Demo **extrahop.com/demo/cloud**

ExtraHop

info@extrahop.com

www.extrahop.com