EXTRAHOP

ExtraHop RevealX™: Cloud-Scale AI-Powered NDR Detects Advanced Threats and Accelerates Investigations

SOLUTION BRIEF

KEY CAPABILITIES

ExtraHop provides cloud-scaled ML/AI for superior threat detection.

AI-powered triage and investigation features accelerate response times.

Integrated packet capture and decryption enhance ML/AI visibility into encrypted threats.

Natural language AI search simplifies data retrieval and analysis for analysts.

The Challenge

As a cybersecurity professional, you face a daunting challenge due to the ineffectiveness of your current threat detection mechanisms. Despite significant investment in numerous security solutions, 41% of attacks successfully bypass your existing defenses.

The problem is compounded by the fact that:

- Initial access is becoming faster and stealthier; adversaries increasingly favor highly personalized social engineering, compromised credentials, and trusted relationship abuse over traditional malware.
- Legitimate remote monitoring and management (RMM) tools are now frequently used by prominent threat groups like Scattered Spider and Conti for lateral movement and command and control within your environment.
- Encrypted channels deliver 87% of network traffic, up from 78.1%, making detection even more difficult for you without proper decryption capabilities.
- The threat landscape continues to evolve with increasingly advanced threats designed to evade threat detection tools and dodge response efforts during investigations.

However, an often overlooked issue is that too many NDR vendors rely on on-device analysis to detect malicious or anomalous activity. The sheer volume of data generated by modern IT environments, with a single 10Gbps link generating 105TB/day, overwhelms the processing power of an individual sensor.

Your detection technology needs to be able to analyze at today's speeds, and it can't do that on a security appliance. Performing analysis on local sensors (physical or virtual) can't keep up with either north-south or lateral, east-west traffic volumes. In 2024, the average attack breakout time from initial threat actor access to lateral movement was 48 minutes, with the fastest breakout observed at just 51 seconds, underscoring the critical need for accelerated investigation and response.

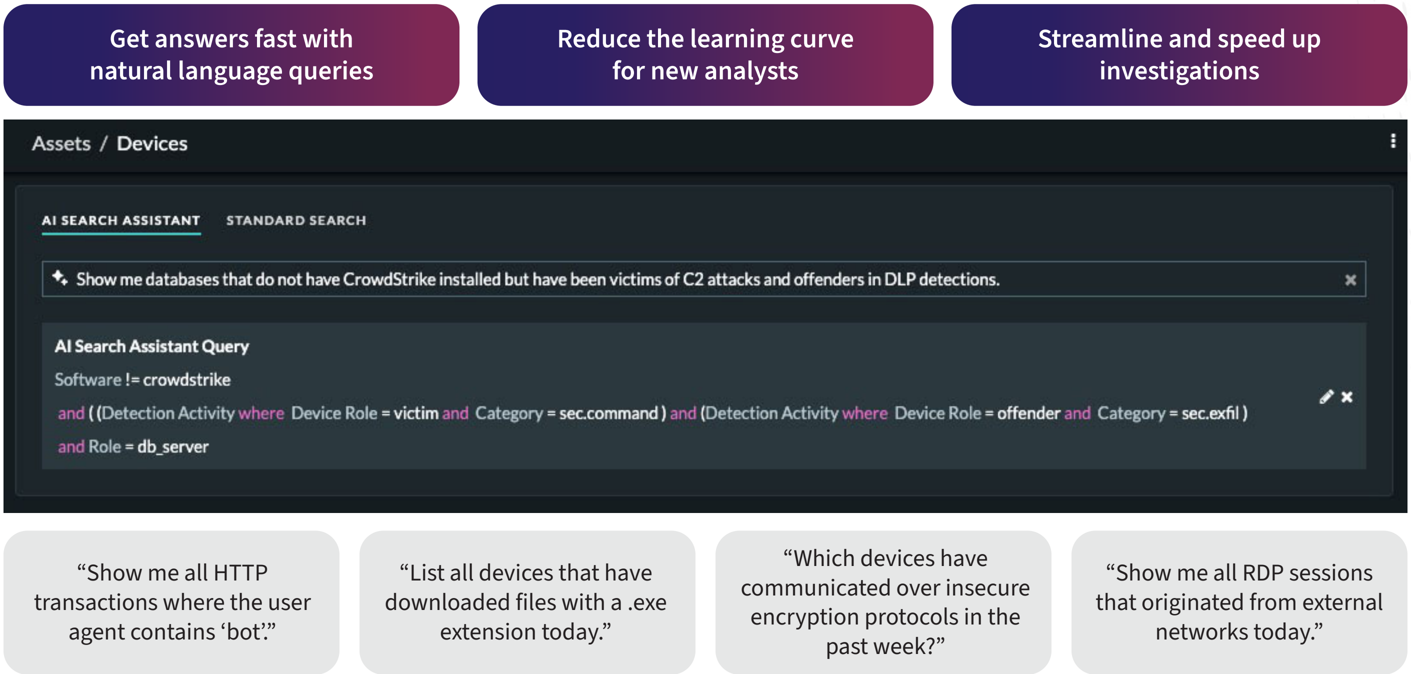
The Solution

With ExtraHop's RevealX platform, you can leverage cloud-scaled ML/AI to revolutionize your network detection and response (NDR). Unlike many solutions that rely on limited on-device machine learning, ExtraHop's cloud-based ML/AI operates with unlimited compute resources. This allows you to apply millions of high-fidelity models for every device, application, and metric, providing significantly more powerful and accurate detections. These models auto-update with no action required from you, and continuously ingest massive threat intelligence datasets, ensuring that ExtraHop stays ahead of evolving threats for you. This cloud-scale approach means

ML/AI analysis is correlated across all your sensors, not isolated to individual appliances, drastically lowering false positives while increasing the accuracy of your detections. ExtraHop's ability to process over 1PB of data daily on a single sensor highlights its unparalleled capacity for handling voluminous data at scale, ensuring high-fidelity detections even in petabyte-scale environments.

A key strength of ExtraHop's ML/AI is direct access to native packet capture and decryption capabilities. Many NDR and similar security tools require you to use additional third-party solutions for full packet capture, or decryption, adding operational complexity and increasing your total cost of ownership. ExtraHop RevealX provides complete packet visibility everywhere and can decrypt over 100 protocols natively. This is critical, as 65% of your internal traffic is encrypted. Without the ability to decrypt, critical lateral movement threat indicators remain hidden, rendering other security tools blind to malicious activity.

By integrating decryption and full packet capture, ExtraHop ensures that its ML/AI analytics have all the necessary information to detect legitimate advanced threats missed by other tools and significantly speeds up your threat investigations. This integrated approach also streamlines workflows, allowing your analysts to move seamlessly from detection to investigation to response within a single UI, with one-click access to months of proof of record and deep packet inspection.



Get answers fast with natural language queries

Reduce the learning curve for new analysts

Streamline and speed up investigations

Show me databases that do not have CrowdStrike installed but have been victims of C2 attacks and offenders in DLP detections.

AI Search Assistant Query

```
Software != crowdstrike
and ( (Detection Activity where Device Role = victim and Category = sec.command ) and (Detection Activity where Device Role = offender and Category = sec.exfil )
and Role = db_server
```

"Show me all HTTP transactions where the user agent contains 'bot'."

"List all devices that have downloaded files with a .exe extension today."

"Which devices have communicated over insecure encryption protocols in the past week?"

"Show me all RDP sessions that originated from external networks today."

Figure 1: ExtraHop's AI Search Assistant transforms the search process to help your analysts get the answers they need fast!

CUSTOMER BENEFITS

The ML/AI analytics in ExtraHop RevealX significantly benefit your organization by transforming how you detect, triage, and investigate cyberattacks. The platform's full packet visibility, combined with cloud-scale ML/AI, ensures more accurate threat detections, catching threats other tools miss. This granular insight also dramatically reduces false positives and speeds threat investigations, freeing up precious analyst time. And by integrating native packet capture and decryption, ExtraHop supports vendor consolidation, eliminating separate third-party tools and reducing management overhead, ultimately simplifying your security stack and lowering operational costs.

ExtraHop's AI/ML-powered features enable RevealX to give you immediate confirmation of malicious activity and breaches, provide "smoking gun" evidence, and supercharge investigations with intelligent, integrated workflows.

- The Smart Triage feature enables your Tier 1 analysts to move quickly from alerts to investigations, quickly focusing their efforts on what matters most.
- The Smart Investigations feature automates context aggregation for your Tier 2 investigations, rapidly creating incident case files for high-risk attack patterns, which combats alert fatigue and accelerates your investigation process.
- Your analysts will conduct forensic investigations faster because of their ability to move seamlessly from detections to records to packets in just two clicks.
- The investigation process will be further streamlined by features like file carving, which filters out only relevant data from packet stores so analysts remain focused.
- The AI Search Assistant, powered by generative AI, allows your analysts to use natural language queries to quickly find what they need, when they need it (see figure 1).

ExtraHop's industry-leading ML and AI capabilities dramatically reduce the learning curve for your less experienced analysts and accelerate overall investigation efforts. The results are visible in key metrics such as faster Mean-Time-To-Detect (MTTD) and Mean-Time-To-Respond (MTTR). This ultimately strengthens your overall security posture, minimizes the impact of even the most advanced cyberattacks, and empowers your security teams to be faster, more effective, and more proactive in defending against modern threats.

TAKE THE NEXT STEP

For more information and to schedule a demo, visit extrahop.com

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management 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.

EXTRAHOP®

info@extrahop.com
extrahop.com