ExtraHop

Network Packet Forensics Speeds Investigations and Forensic Evidence Collection

INTRODUCTION

When it comes to incident response and network forensics, response time is critical. The weeks spent by your most skilled security analysts, and the downtime and cost attributed to recovery from data breaches and ransomware add up. Unfortunately, time isn't on your side: If you realize you are missing definitive evidence mid-response, you may not be able to fully capture the actions intruders made toward your data until it's too late.

EXPERIENCED RESPONDERS DEPEND ON THE NETWORK FOR THE CYBER TRUTH

Attacker obfuscation tactics have taught seasoned incident responders to be suspicious of server and endpoint logs when an intruder is in the midst. That's why experienced responders recognize that network packets provide you with the unalterable ground truth.

The ExtraHop Network Forensics module provides incident responders visibility across hybrid environments that attackers can't evade. Your network is forensics-ready with continuous packet capture, a scalable PCAP repository, and a streamlined investigation workflow to eradicate intruders faster.

Accurate, actionable data is the only accelerant to recovery and closing security gaps quickly. With ExtraHop Network Forensics and Reveal(x), incident responders can jump into action with context-enriched alert timelines, continuous packet capture, and PCAP evidence repositories to eradicate intruders and recover faster.

KEY BENEFITS

INTEGRATED WORKFLOW

With detections, transaction records, and packets all indexed and searchable, analysts can expedite speed to resolution.

DECRYPTION CAPABILITIES

Uncover damaging attacker's actions hiding in encrypted traffic, including TLS 1.3 PFS.

MAXIMIZE SECURITY ANALYST RESOURCES

Fast queries and global search with an easy-to-use interface get answers without needing to be an expert.

HYBRID CLOUD ENVIRONMENTS

Capture packets across hybrid environments and provide definitive evidence and immediate answers for cloud security teams.

CHAIN-OF-CUSTODY COLLECTION

Remove manual processes and the need for multiple products for root-cause analysis and fulfill evidence collection requirements.

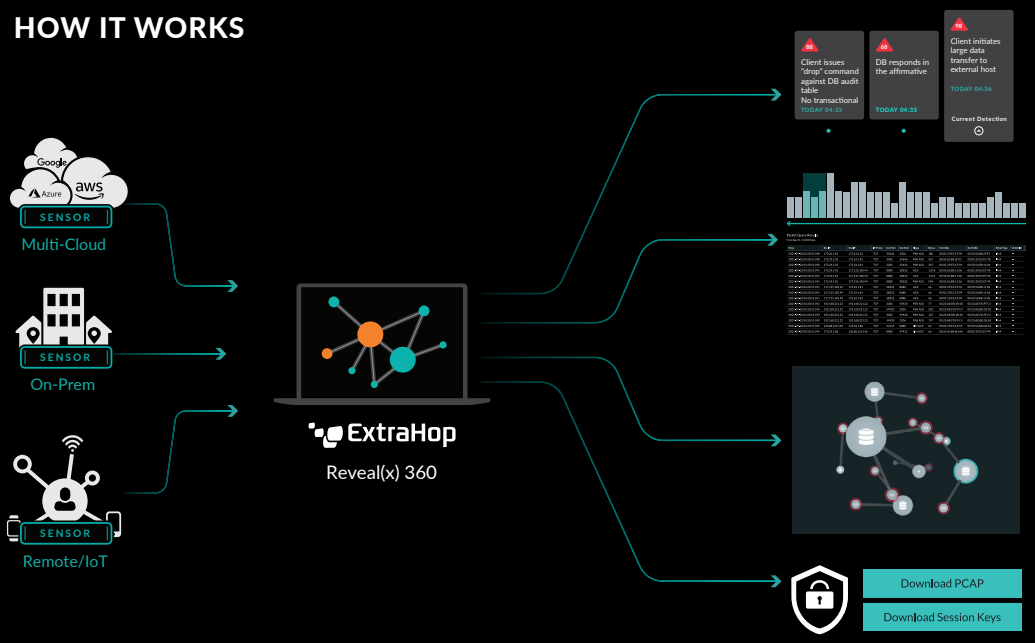
HORIZONTALLY SCALABLE SOLUTION

Modularly extend your PCAP archive as your requirements grow, up to petabytes of storage.

ATTACKERS CAN'T EVADE NETWORK EVIDENCE

ExtraHop Network Forensics includes horizontally scalable PCAP repository, up to Petabytes, for use in regulatory and legal recourse.

HOW IT WORKS



Incident Responders jump into action with contextualized alerts with attacker timeline

Quickly identify the packets needed and collect with full-chain of custody confidence

Scope all impacted systems and compromised data

Long term packet evidence retention

Use Cases

ESTABLISH CYBERSECURITY RESILIENCE

Build resilience against the inevitable attack. Empower incident responders to make informed decisions quicker to eradicate intruders faster using ground-truth traffic data.

ACCELERATE ZERO TRUST

Effectively gather critical evidence for insider threat investigations.

APPLICATION TROUBLESHOOTING

Reduce the MTTI (Mean Time To Innocence) and troubleshoot application issues faster.

HYBRID CLOUD INCIDENT RESPONSE

Provide incident responders cloud-native network forensic evidence.

ABOUT EXTRAHOP NETWORKS

ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the attack. The ExtraHop Reveal(x) 360 platform is the only network detection and response solution that delivers the 360-degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they can see more, know more, and stop more cyberattacks. Learn more at **www.extrahop.com**.

info@extrahop.com
www.extrahop.com

ExtraHop