EXTRAHOP

DATASHEET

Packet-Level Visibility Speeds Forensic Investigations and Evidence Collection

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 lack definitive evidence mid-response, you may never be able to reconstruct the actions intruders made inside your network.

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 their midst. That's why experienced responders recognize that network packets provide you with the unalterable ground truth.

The ExtraHop Packet Forensics module provides visibility across your hybrid environments that attackers can't evade. Your network is forensics-ready with continuous packet capture, a scalable PCAP repository, in-product packet viewer, built-in file carving, and a streamlined investigation workflow with end-to-end packet analysis.

Accurate, actionable data is the only accelerant to recovery and closing security gaps quickly. With ExtraHop Packet Forensics and RevealX™, you can jump into action with context-enriched alert timelines, continuous packet capture, and PCAP evidence repositories to eradicate intruders and recover faster.

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

> “With ExtraHop, I can tell you what every packet is doing anywhere on the network at any given time: where it's going, where it came from, and what is being said across both sides of the conversation. This enables my team to make accurate, informed, and effective decisions about optimization, security, and troubleshooting on the network.”
>
> **Lee Chieffalo, Technical Director, Viasat**

KEY BENEFITS

Integrated Workflow

With detections, transaction records, and packets all indexed and searchable, you can expedite MTTR.

Decryption Capabilities

Uncover damaging activity 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.

Packet Viewer

Analyze and dissect packet data without leaving the platform.

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.

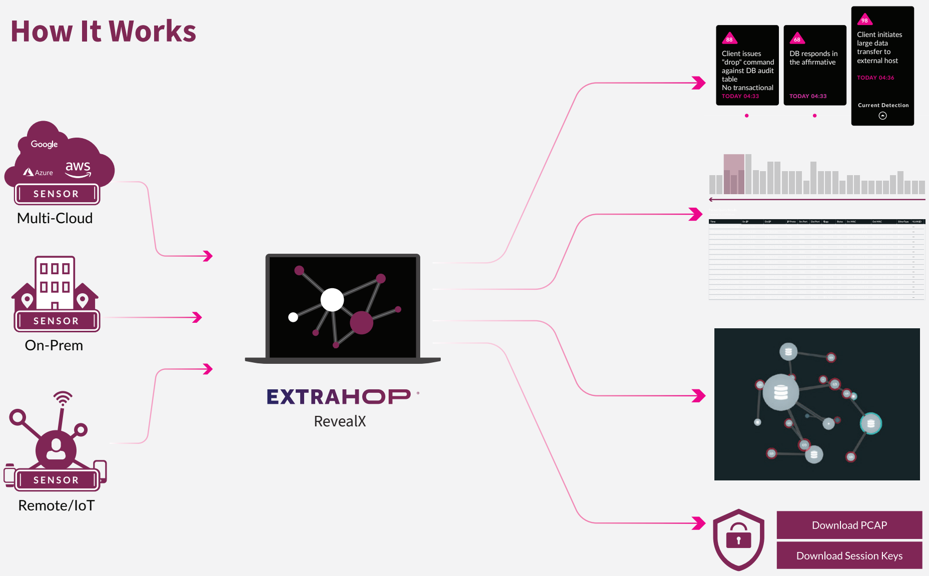
Horizontally Scalable Solutions

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

On-Demand File Carving

Securely extract and recreate files directly from PCAPs within the RevealX platform for faster investigations.

How It Works

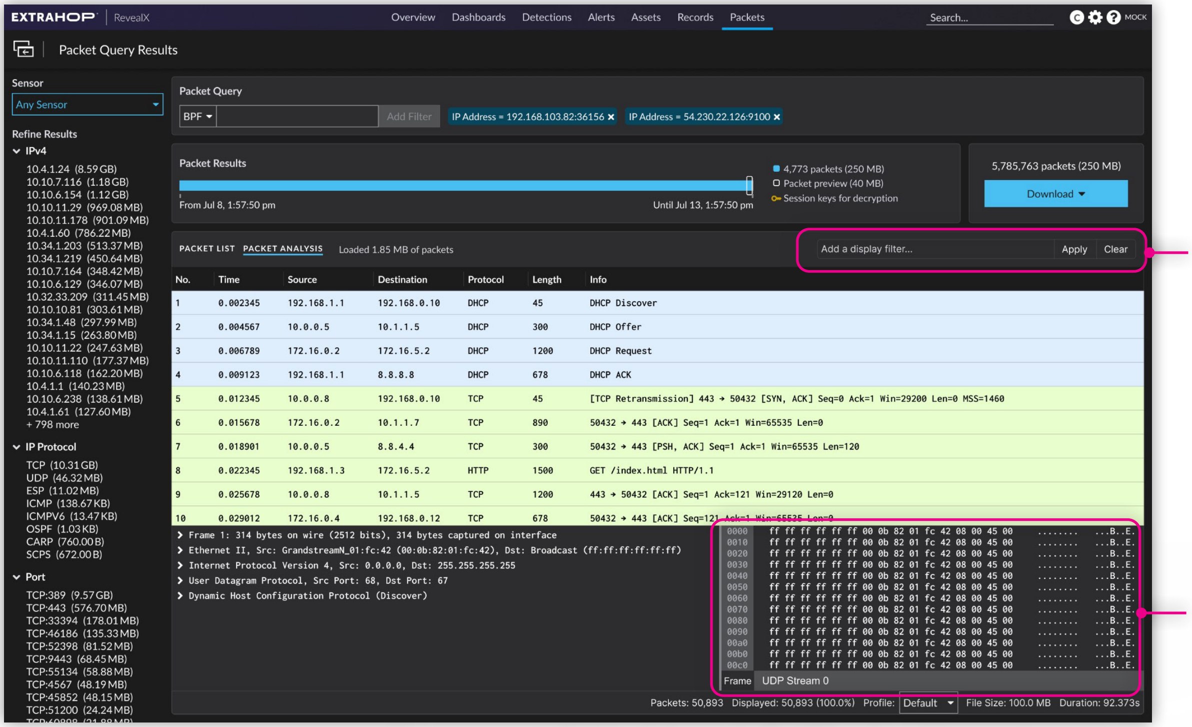


Incident Responders jump into action with contextualized alerts with attacker timeline

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



Packet Query Results

Sensor: Any Sensor

Refine Results

IPv4
10.4.1.24 (8.59 GB)
10.10.7.116 (1.18 GB)
10.10.6.154 (1.12 GB)
10.10.11.29 (969.08 MB)
10.10.11.178 (901.09 MB)
10.4.1.60 (786.22 MB)
10.34.1.203 (513.37 MB)
10.34.1.219 (450.64 MB)
10.10.7.164 (348.42 MB)
10.10.6.129 (346.07 MB)
10.32.33.209 (311.45 MB)
10.10.10.81 (303.61 MB)
10.34.1.48 (297.99 MB)
10.34.1.15 (263.80 MB)
10.10.11.22 (247.63 MB)
10.10.11.110 (177.37 MB)
10.10.6.118 (162.20 MB)
10.4.1.1 (140.23 MB)
10.10.6.238 (138.61 MB)
10.4.1.61 (127.60 MB)
+ 798 more

IP Protocol
TCP (10.31 GB)
UDP (46.32 MB)
ESP (11.02 MB)
ICMP (138.67 KB)
ICMPV6 (13.47 KB)
OSPF (1.03 KB)
CARP (760.00 B)
SCPS (672.00 B)

Port
TCP:389 (9.57 GB)
TCP:443 (576.70 MB)
TCP:33394 (178.01 MB)
TCP:46186 (135.33 MB)
TCP:52398 (81.52 MB)
TCP:9443 (68.45 MB)
TCP:55134 (58.88 MB)
TCP:4567 (48.19 MB)
TCP:45852 (48.15 MB)
TCP:51200 (24.24 MB)

Packet Query

BPF | Add Filter | IP Address = 192.168.103.82:36156 ✕ | IP Address = 54.230.22.126:9100 ✕

Packet Results

From Jul 8, 1:57:50 pm — Until Jul 13, 1:57:50 pm

■ 4,773 packets (250 MB)
□ Packet preview (40 MB)
Session keys for decryption

5,785,763 packets (250 MB)

Download ▾

PACKET LIST PACKET ANALYSIS Loaded 1.85 MB of packets

Add a display filter... Apply Clear

No.	Time	Source	Destination	Protocol	Length	Info
1	0.002345	192.168.1.1	192.168.0.10	DHCP	45	DHCP Discover
2	0.004567	10.0.0.5	10.1.1.5	DHCP	300	DHCP Offer
3	0.006789	172.16.0.2	172.16.5.2	DHCP	1200	DHCP Request
4	0.009123	192.168.1.1	8.8.8.8	DHCP	678	DHCP ACK
5	0.012345	10.0.0.8	192.168.0.10	TCP	45	[TCP Retransmission] 443 → 50432 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
6	0.015678	172.16.0.2	10.1.1.7	TCP	890	50432 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
7	0.018901	10.0.0.5	8.8.4.4	TCP	300	50432 → 443 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=120
8	0.022345	192.168.1.3	172.16.5.2	HTTP	1500	GET /index.html HTTP/1.1
9	0.025678	10.0.0.8	10.1.1.5	TCP	1200	443 → 50432 [ACK] Seq=1 Ack=121 Win=29120 Len=0
10	0.029012	172.16.0.4	192.168.0.12	TCP	678	50432 → 443 [ACK] Seq=121 Ack=1 Win=65535 Len=0

```
> Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured on interface
> Ethernet II, Src: GrandstreamN_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

```
0000   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0010   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0020   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0030   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0040   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0050   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0060   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0070   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0080   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
0090   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
00a0   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
00b0   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
00c0   ff ff ff ff ff ff 00 0b 82 01 fc 42 08 00 45 00   ........   ...B..E.
```

Frame | UDP Stream 0

Packets: 50,893 Displayed: 50,893 (100.0%) Profile: Default ▾ File Size: 100.0 MB Duration: 92.373s

Filter Packets

Traffic Streams

The packet viewer allows you to analyze and dissect packet data without leaving the RevealX platform and supports key analysis capabilities, including filtering TCP, UDP, HTTP streams.

TAKE THE NEXT STEP

To experience RevealX for yourself, request a personalized live demo.

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