ExtraHop

SCALEABLE LONG-TERM

PCAP Repository

Speed Investigation and Forensics Evidence Collection

ExtraHop dramatically reduces the time, effort, and money required to perform packet-level incident investigations. With a modularly extensible PCAP repository, you have the definitive packet data for root-cause analysis while fulfilling chain-of-custody evidence collection.

Effective Incident Response Need Packets

Packet capture plays a vital role in incident response, forensic investigation, and threat hunting, but it hasn't been easy to get in hybrid cloud environments. Historically, collecting and analyzing packets was a complex, time-consuming, manual process that often involved multiple tools.

One PCAP Repository for On-premises and Cloud Environments

Reveal(x) scalable PCAP retention unlocks ground truth network forensics with streamlined and guided investigation. By capturing every packet across all your hybrid environments, Reveal(x) provides definitive insights and immediate answers, reducing the time and effort to perform packet-level analysis.

Even cloud-focused security teams now have the forensic detail they need to pinpoint root cause and eradicate intruders while fulfilling evidence chain-of-custody requirements.

Futureproof PCAP Retention Investment

Modularly extend Reveal(x) 360 PCAP archive as your requirements grow, up to 24 petabytes (PB) of storage.

Save Time with an Integrated Workflow

Whether starting from a global view or investigating a single transaction, get to the packets you need in a few clicks.

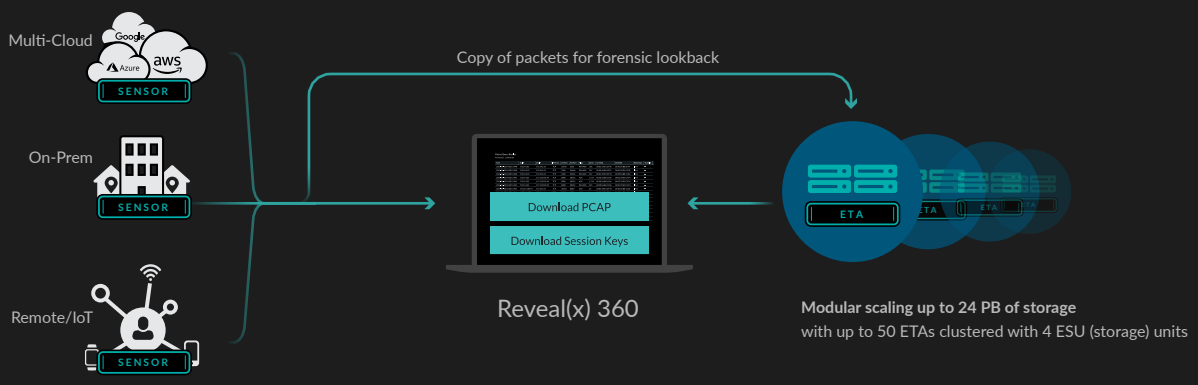
Eliminate Encryption Blindspots

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

Maximize Security Analyst Capabilities

Fast visual query and global search get answers without being an expert.

HOW IT WORKS



Appliance Selection

Modular scaling is achieved with ExtraHop Trace Appliance (ETA) and ExtraHop external Sotruate Units (ESU) working with Reveal(x) 360. ETA can be deployed singly or as a cluster for increased traffic ingestion rates. A cluster of four ETA 8250 appliances can ingest up to 100 Gbps of sustained throughput. Similarly, ESU can be added to each ETA for increased storage capacity, up to 480 TB in total. Each Reveal(x) 360 tenant can incrementally add up to 50 ETA to scale up 24 PB* of available storage.

**19.6 PB available for use based on RAID configuration*

PHYSICAL	ETA 8250	ESU 96TB
PACKET INGEST	10 Gbps (ETA only)	
- Thoughput	25 Gbps[1] (ETA+1 or more ESU)	N/A
NETWORK PORTS		
- Packet Capture	2 x 10 G / 25 G ports	N/A
- Management	2 x 10 G ports +2 x 1 G ports	N/A
- Disks	12 x 8 TB (96 TB total)	12 x 8 TB (96 TB total)
- RAID Configuration	RAID 6	RAID 6
Rack Units	2U	2U
Power Supply	2 x 1100W	2 x 750W

[1] Up to 12.5M packets/sec

VIRTUAL	ETA 6150v	ETA 1150v
PACKET INGEST		
- Capture Thoughput	10 Gbps[2]	1Gbps
HARDWARE REQUIREMENTS		
- vCPU	18	2
- RAM	64GB	16GB
- Firmware Disk	4GB	4GB
- Packet Store Disk	Up to 25TB[3] (min is 1TB)	Up to 4TB (min 500GB)
VIRTUAL NETWORK		
-Management vNIC	Up to 3	1 (Up to 1Gbps capture rate)
-Capture vNIC	2 x 1100W	2 x 750W
-Capture modes	Port Mirror, ERSPAN, RPCAP, VXLAN	Port Mirror, ERSPAN, RPCAP, VXLAN
Platforms	VMware	VMware, Azure, AWS

[2] Up to 800K packets/sec using two capture interfaces
[3] The packetstore virtual disk must support a write throughput of 10Gbps. ExtraHop recommends dedicated storage and I/O channels for the packetstore

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 can compromise your business. When you don't have to choose betweenprotecting your business and moving it forward, that's security, uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com