ExtraHop

SCALEABLE PACKET CAPTURE

Accelerate Compliance and Modernize Network Visibility

Scalable packet capture (PCAP) is the foundation for network security and observability:
It supplies diverse data sources that help teams understand what is happening inside a network. Information from PCAP enables you to hunt for cyber threats, speed forensic investigations, and respond to sophisticated attacks. This is why PCAP is a core requirement to comply with U.S. federal government cyber-modernization mandates, including Executive Order 14028 and OMB M-21-31.

Packet Capture Challenges

To be effectively used in cyber operations, network packet capture requires a daunting amount of time and effort to capture, analyze, and retain packet data. Hybrid environments, petabytes of daily network transactions, and encrypted network traffic quickly overwhelm traditional PCAP tools. Recent federal mandates establishing new retention requirements further exacerbate these shortcomings, leaving Executive Branch departments and agencies in need of an efficient, cost-effective, and scalable way to achieve compliance.

Reduce Time, Effort, and Cost

ExtraHop Reveal(x) is an extensible PCAP repository that provides definitive packet data. This speeds root-cause analysis and helps fulfill mandated data retention and information sharing directives.

Reveal(x) combines packet-level data with advanced network intelligence to find threats in real-time. With powerful investigative workflows and forensics capabilities—including visibility into encrypted network traffic—federal government agencies using ExtraHop are well-positioned to meet current and future cyber maturity requirements.

Scaleable Network Forensic Collection

Continuously capture packet data across your agency's hybrid environment—including cloud, datacenter, and IoT—with ingestion up to 100 Gbps of sustained throughput.

Futureproof PCAP Investments

Modularly extend Reveal(x) packet data retention periods as your requirements grow, up to 24 petabytes (PB) of storage.

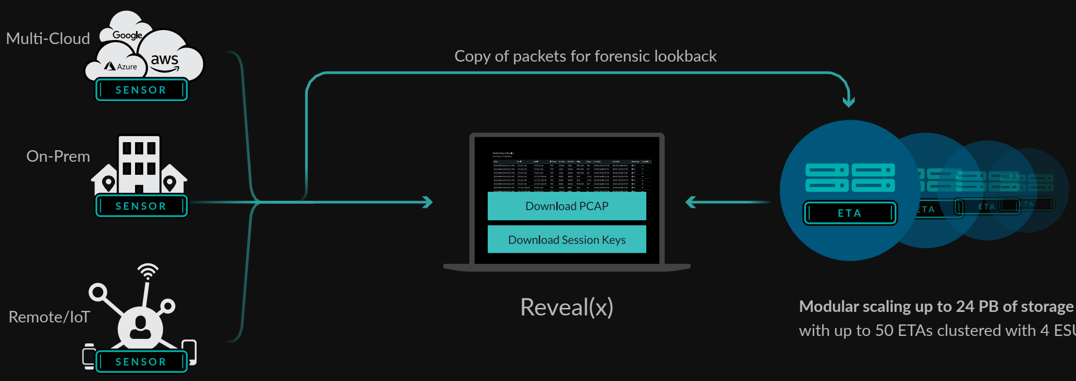
Eliminate Encryption Blindspots

Uncover advanced threats and malicious activities hiding in encrypted traffic—even those invisible to traditional packet-capture tools—with out-of-band SSL/TLS 1.3 decryption.

Maximize Security Analyst Capabilities

Get immediate answers without having to be an expert with an integrated workflow, fast visual query, and global search.

HOW IT WORKS



Modular scaling up to 24 PB of storage
with up to 50 ETAs clustered with 4 ESU (storage) units

USE CASES

LOG ALL NETWORK TRANSACTIONS

Meet OMB M-21-31 event logging requirements for network device infrastructure, cloud environments, and application transactions categories. Reveal(x) continuously captures network transactions across multiple cloud providers and on-premises, all in one tool.

PRESERVE FORNSIC EVIDENCE

Fulfill chain-of-custody and full packet data retention obligations with cost-effective storage. Reveal(x) provides the scale and flexibility to achieve retention periods beyond 72 hours with BYO storage options.

DETECT ATTACKS IN ENCYRPTED TRAFFIC

Securely decrypt traffic for inspection to detect and investigate the origin of malicious activity. Reveal(x) can be configured to store a session key with packets for a safer approach than sharing long-term private keys with analysts.

APPLY ADVANCED ANALYSIS TO PACKET DATA

Uncover sophisticated advanced persistent threats lurking in network data. Reveal(x) reclaims the cyber advantage by combining packet-level granularity, visibility, and situational intelligence to detect advanced threats other tools miss.

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