EXTRAHOP

The Indispensable Value of Full Packet Capture

Executive Brief

For investigating security threats and network performance troubleshooting, having access to your packet data is invaluable. Full packet capture (FPC) provides the deepest, most detailed view of network traffic, helping your operations teams resolve security threats and unusual network behaviors before they disrupt operations and spike costs.

With packet data integrated into their NDR platform, ExtraHop customers saw faster threat detection and resolution worth nearly $592,000 and decreased time to threat detection by 83% and time to threat resolution by 87%. In total, time to remediate decreased from 11 hours to 1.5 hours, saving a total of 9.5 hours on each threat detection and resolution process.*

By giving your teams access to all the data within a packet, including headers and payloads, you'll give them the forensic visibility they need to do their jobs. Tools limited to header analysis alone are often insufficient for precise event identification, thorough investigations, or comprehensive and defensible evidence collection. ExtraHop is unique in delivering full, continuous packet capture integrated with a modern network detection and response (NDR) platform that puts the intelligence of your network at your operations teams' fingertips.

The Need for Real-Time Packet Capture

Always-on, or continuous, packet capture records all packets that traverse your network. This approach ensures that you have a complete record of network traffic, including payload data from internal server communications to traffic destined for external websites or applications. Your operations teams can use these full records to recreate network sessions when they are investigating security alerts or troubleshooting network or application issues and end-user inquiries.

Capturing entire packets, including headers and payloads, offers a comprehensive record of every part of that communication between those two points, which facilitates thorough analysis for threat detection, incident response, and network forensics. This detailed insight allows you to reconstruct network events with precision, aiding in identifying and mitigating security breaches.

Another strength of full packet capture lies in its versatility; it proves invaluable not only in incident response and forensics, but also in compliance monitoring. The ability to capture complete communication flows ensures you can adhere to regulatory standards by maintaining a detailed record of network activities.

Additionally, in troubleshooting network issues, full packet capture (PCAP) becomes a valuable diagnostic tool for optimizing performance. By examining the entire packet content, you can identify complex malicious activity that may be hidden within encrypted traffic or disguised by normal network patterns.

Is "Smart PCAP" Smart Enough?

To offer more affordable and targeted products, some vendors are pitching triggered or "selective" packet capture, also referred to as Smart PCAP, as an alternative to always-on capture. This type of reactionary triggered capture allows you to selectively capture packets under certain conditions. Other tools might trigger packets only when specific protocols are detected on your network, such as file transfer (FTP). These practices will certainly reduce the total amount of data storage you consume with packet capture.

However, this approach requires you to know ahead of time what to look for and often misses unexpected or unplanned incidents. Therefore, "Smart PCAP" is not a robust and reliable enough approach for many organizations. Triggered packet capture often does not meet the standards for highly regulated industries, in which a full record of all packets is required by regulators and auditors. Many federal government agencies and departments are mandated to capture and retain all packet data that traverses their networks, both on-premises and in the cloud. The reason is simple — you often have to go back because you miss the initial attack in real time.

Forensic Visibility Into Encrypted Data

Encryption presents an additional security challenge, relating to both endpoint detection response (EDR) and even network detection and response (NDR). For years, you focused on encrypting as much of your network devices and traffic as possible, only to discover that encryption also provides cover for bad actors with nefarious intentions as they move throughout your network. As a result, much of the threat landscape today is hiding in encryption. In many cases, encryption makes it easier for attacks to happen because it makes these attacks harder to identify and prevent.

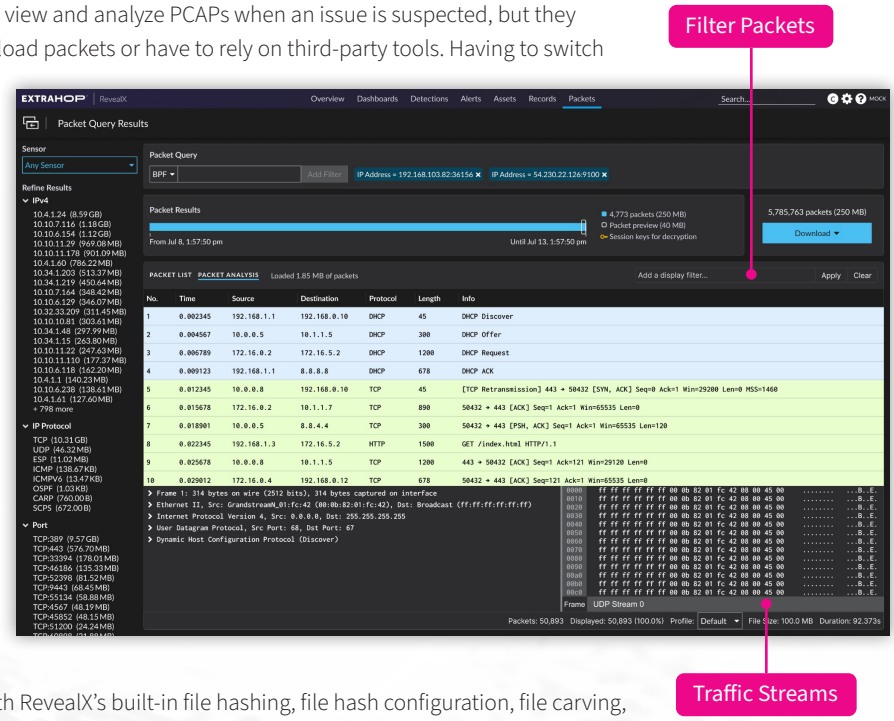
ExtraHop customers have an advantage by not only defending the network but also ensuring line-speed analysis can happen with zero impact on performance. By leveraging full packet capture, capable of SSL, TLS, and Active Directory decryption, ExtraHop gives you control over your full network flows, examining every packet, whether encrypted or not. This comprehensive traffic analysis enables you to build better metadata around your network traffic, leading to more productive investigations, earlier detections, and faster resolutions. By being able to see into encrypted traffic and provide real-time insight and analysis, ExtraHop enables you to stop current attacks and protect against future attempts.

The Evidence You Need, When You Need It

You can make use of collections of PCAPs to investigate and resolve a host of security issues. If you are already getting alerts from an IDS/IPS/SIEM device, or better yet, have IDS capabilities built into your NDR platform, then your ability to quickly analyze the related packets that triggered the alert can reveal exactly what transpired. Having quick access to those packets means a much faster forensics process than using fallible log data. Without those packets, you may never know how a culprit entered the network or the extent of the damage.

Packets at Your Fingertips with End-to-End Analysis

Your network and security teams often need access to view and analyze PCAPs when an issue is suspected, but they often face internal restrictions when needing to download packets or have to rely on third-party tools. Having to switch tools between metadata and drilling down into raw packets can be cumbersome and time-consuming. With an in-product packet viewer, ExtraHop is simplifying your investigation workflow and reducing the need for manual downloads and the use of third-party tools in order to do faster root cause analysis. Having end-to-end network packet analysis within your NDR platform enables you to pinpoint and resolve threats and network performance issues without leaving the ExtraHop RevealX™ platform and improves incident response time.



It's Time for a Modern Approach to NDR

Threats are escalating each year, and forward-thinking organizations know that no matter how well they believe they are positioned against today's threats, tomorrow still beckons. Combined with RevealX's built-in file hashing, file hash configuration, file carving, and malicious file detection capabilities, it provides significant benefits for both you and your network teams. These latest product updates result in a streamlined workflow that helps SOC analysts save hours of arduous investigation time while consolidating more of their mission-critical security functions within a single NDR console. With the ability to identify threats earlier, investigate smarter, and stop them faster, ExtraHop enables you to future-proof your security and stay ahead of the latest risks.

Interested in taking a proactive approach to your threat detection?
Now is the time to reach out to ExtraHop at extrahop.com/contact.

*Forrester Consulting, The Total Economic Impact™ of ExtraHop Reveal(x) 360, January 2023.

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