ExtraHop

ExtraHop Packet Basics

FREE PCAP FOR AWS ENVIRONMENTS

Forensic investigation in cloud environments is more critical than ever. Attacks evolve daily, and the number of advanced threats security teams are forced to confront continues to rise.

ExtraHop Packet Basics is a free network forensics offering that provides incident responders with packet capture (PCAP) for analysis, forensic investigation, threat hunting, and more.

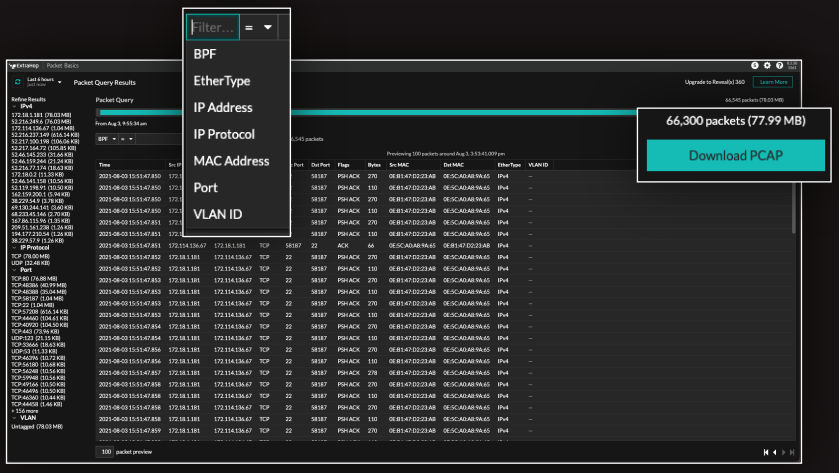
Security Benefits of Packet Capture in Cloud Environments

With ExtraHop Packet Basics, cloud-focused security teams now have access to specific network packets before, during, and after incidents. Armed with richer forensic detail than what is available in logs and data from agents and firewalls, analysts can get to ground truth faster and fulfill chain-of-custody requirements.

Why Choose ExtraHop Packet Basics Free PCAP?

ExtraHop Packet Basics integrates with Amazon VPC Traffic Mirroring to begin providing incident responders and forensic investigators with copies of network packets as soon as it's deployed in an AWS environment. As a free tool, ExtraHop Packet Basics also removes the financial burden of adding PCAP to your existing incident response workflows.

You can select ExtraHop Packet Basics directly from AWS Marketplace, allowing you to deploy PCAP with the click of a button. Additionally, ExtraHop Packet Basics provides three key benefits:



- Enhances incident response workflows with instant access to network packets.
- Enables PCAP for the packets needed for incident response and more.
- Reduces the amount of time and effort required to perform packet capture in the cloud.

Get ExtraHop Packet Basics for Free

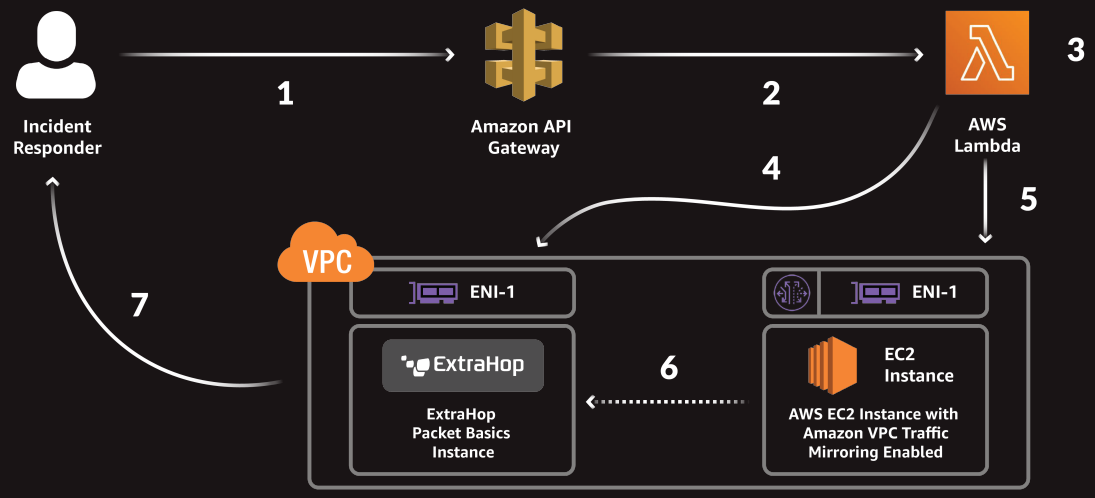
GET IT NOW ›

Start the Reveal(x) 360 Demo

START DEMO ›

EXTRAHOP PACKET BASICS

Incident Response Workflow



Respond intelligently

ExtraHop Packet Basics is designed for frictionless PCAP in AWS environments, helping incident responders make confident decisions about the steps to take to stop a threat. Here is one example of how an incident responder could use network packets from ExtraHop Packet Basics.

1. An incident responder identifies abnormal activity and submits an EC2 instance to investigate
2. The API Gateway interacts with an AWS Lambda
3. Given input, the Lambda triggers an action
4. The Lambda launches an ExtraHop Packet Basics instance
5. The Lambda also enables Amazon VPC Traffic Mirroring
6. Amazon VPC Traffic Mirroring forwards copies of network packets to the ExtraHop Packet Basics instance
7. The incident responder can now analyze packet data on the potentially compromised workload and take their next steps

---

Get ExtraHop Packet Basics for Free

GET IT NOW ⊙

Start the Reveal(x) 360 Demo

START DEMO ⊙

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 between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com