ExtraHop

Reveal(x) Cloud

In the cloud, clarity is key. ExtraHop Reveal(x) Cloud is a cloud-native SaaS-based Network Detection and Response (NDR) solution. Reveal(x) Cloud helps provide SecOps teams with complete visibility in their cloud environment, including real-time threat detection, rapid investigation, and automated response.

COMPLETE VISIBILITY

ExtraHop Reveal(x) Cloud provides deep and continuous visibility from the inside out, enabling SecOps teams to analyze every piece of data, transaction, and application to protect their investment in the cloud. Without native network visibility in the cloud, enterprises have been limited to log or agent centric tools, making it difficult to detect and investigate complex threats in a timely manner.

REAL-TIME DETECTION

A completely passive solution that turns raw packets into metadata, ExtraHop Reveal(x) Cloud makes everything searchable. Combining automated discovery and asset classification with full payload analysis and machine learning for high-fidelity threat detection, ExtraHop Reveal(x) Cloud gives cloud-focused SecOps teams the power to proactively monitor and respond to threats.

GUIDED INVESTIGATION

Reveal(x) Cloud will take you from a cloud security event to associated packet in a few clicks, erasing hours spent collecting and parsing log and agent data. Native integrations with AWS EC2, S3, Amazon CloudWatch and CloudTrail, and Amazon VPC Flow Logs along with partnerships with orchestration and ticketing platforms like ServiceNow and Phantom dramatically speed up mitigation and response.

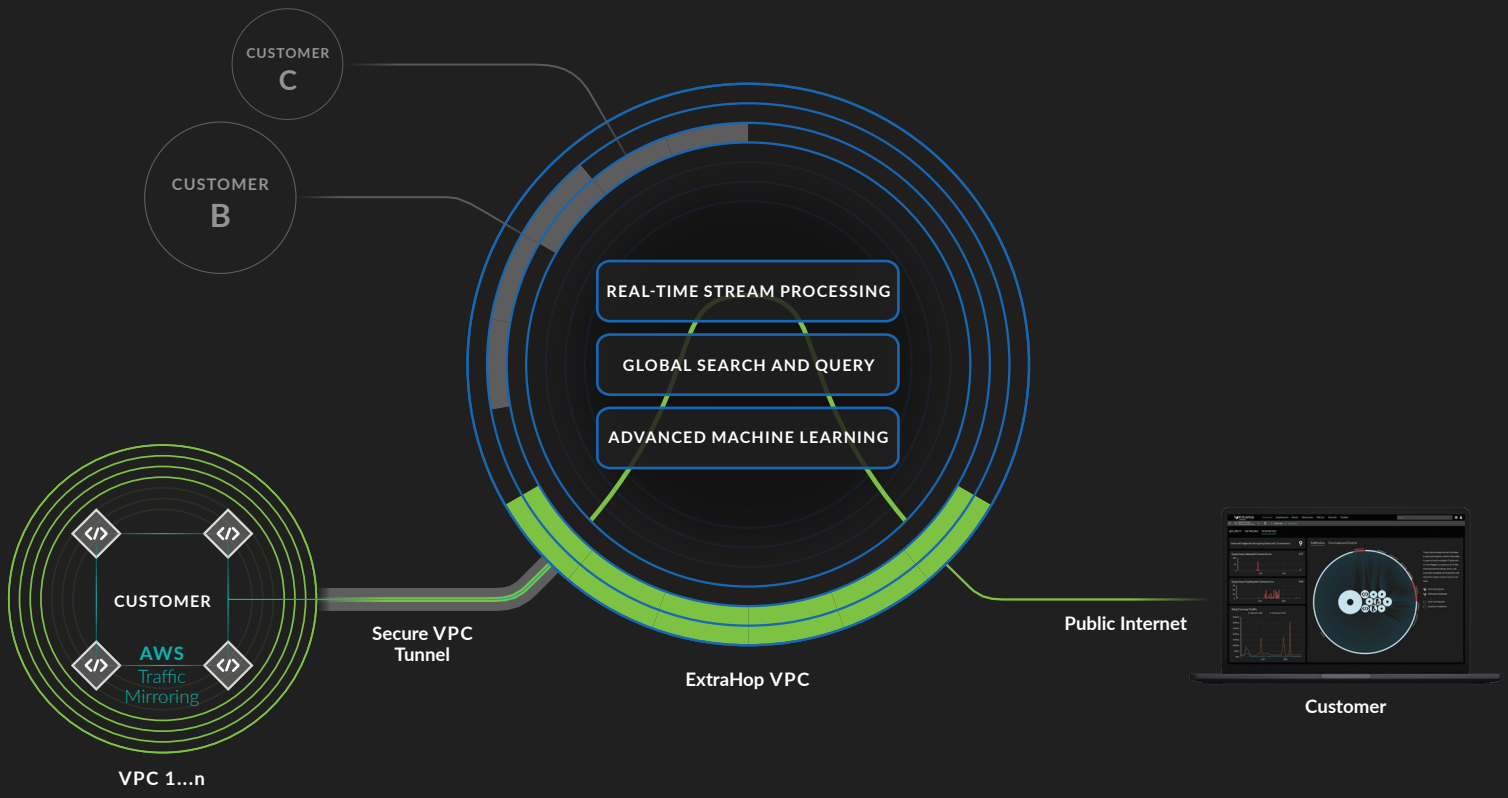
CLOUD-NATIVE SECURITY FOR THE HYBRID ENTERPRISE

SaaS-based Threat Detection and Response

While the cloud has proven to be a force multiplier for business and IT, for SecOps teams the cloud dramatically expands the attack surface and exposes the organization to new and unknown risks. Despite these challenges, many organizations choose to embrace the scale and flexibility of the cloud but find the limitations of existing security tool sets – which typically rely on logs or agents – make it difficult to detect and investigate complex threats in a timely manner due to lack of continuous visibility across all Virtual Private Clouds.

With ExtraHop Reveal(x) Cloud, organizations can adopt a cloud-native approach to protecting their hybrid attack surface. Reveal(x) Cloud provides inside-the-perimeter threat detection, investigation, and response across AWS workloads, allowing SecOps to track rogue instances and eliminate risks created by misconfigurations, insecure APIs, and unauthorized access. ExtraHop Reveal(x) Cloud is a Saas-based solution that deploys instantly and without agents, delivering immediate asset discovery, real-time threat detection, and ML-powered response.

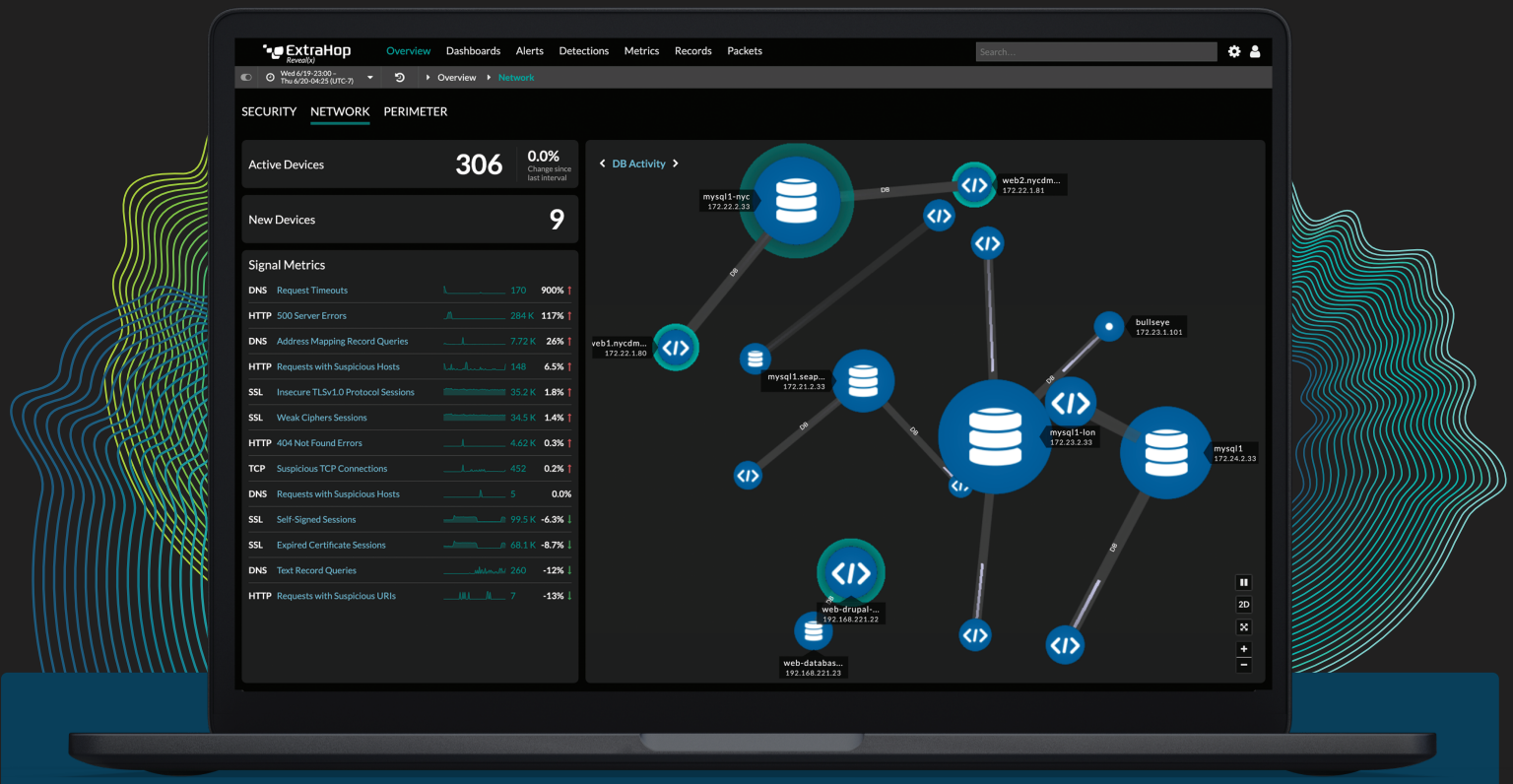
How it Works



REVEAL(X) CLOUD USE CASES

From a single platform, security teams can apply controls to both on-prem and cloud workloads and implement unified threat detection and security policies.

- **Breach Detection**
- **Dependency Mapping**
- **Threat Detection**
- **Encrypted Traffic Analysis**
- **Compliance & Audit**
- **Forensic Analysis**
- **Inventory & Config**
- **Vulnerability Assessment**
- **Threat Hunting**



EXTRAHOP REVEAL(X) CLOUD FEATURES

Hygiene and Compliance
Correlate between malicious activity and asset criticality to deliver high-fidelity alerts which keep teams focused on the highest-risk threats.

Automated Investigations & Response
Provide seamless security settings and limit tool sprawl by integrating with AWS CloudTrail, Amazon CloudWatch, VPC Flow Logs, orchestration systems, and more.

Decode Application Layer Protocols
Analyze and decode cloud-based application content and payload at scale.

Move at the Speed of the Cloud
Provide East/West visibility for threat detection and response at up to 25Gbps per VPC.

Identity and Access Management
Analyze Active Directory payloads to automatically flag indicators of credential harvesting and brute force attacks.

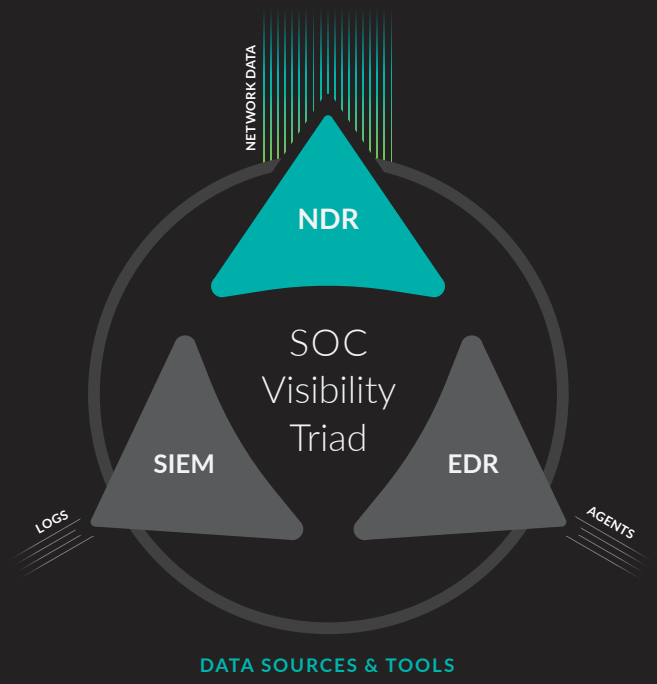
Decryption at Scale
Decrypt all SSL/TLS-encrypted traffic passively and in real-time so you can maintain compliance with full visibility into encrypted threats.

FEATURED INTEGRATIONS

Amazon CloudTrail
Amazon CloudWatch
VPC FlowLogs
QRadar
DEMISTO
A PALO ALTO NETWORKS COMPANY
Phantom

CLOUD-NATIVE NDR COMPLETES SOC VISIBILITY

The missing piece in many enterprise SOCs is network data. Network Detection and Response provides observed ground truth with context, and can't be turned off or evaded by savvy attackers, unlike log and agent-based tools. Because of these traits, the network is the best data source for a truly cloud-native approach to detecting, investigating, and responding to threats in hybrid environments.



CUSTOMER VALUE

IDC

COMPLETE VISIBILITY

95%

Improvement In Time To Detect Threats

REAL-TIME DETECTION

77%

Improvement In Time To Resolve

GUIDED INVESTIGATION

59%

Reduction In Staff Time To Resolve

FREE TRIAL extrahop.com/freetrial

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach analyzes all network interactions and applies cloud-scale machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring the availability of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

ExtraHop

info@extrahop.com
www.extrahop.com