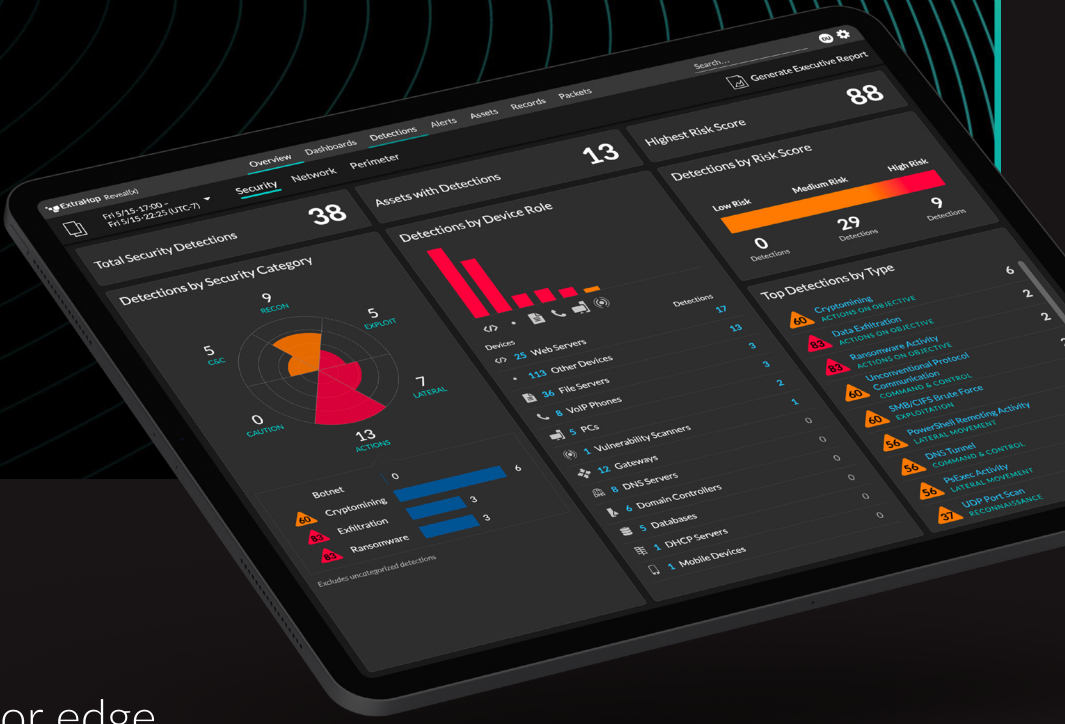
ExtraHop

Reveal(x) 360


ExtraHop Reveal(x)
Fri 5/15-17:00 - Fri 5/15-22:25 (UTC-7)
Overview
Dashboards
Detections
Alerts
Assets
Records
Packets
Search...
Security
Network
Perimeter
Generate Executive Report
Total Security Detections 38
Assets with Detections 13
Highest Risk Score 88
Detections by Security Category
9 RECON
5 EXPLOIT
5 C&C
7 LATERAL
0 CAUTION
13 ACTIONS
Botnet 0
60 Cryptomining 6
83 Exfiltration 3
83 Ransomware 3
Excludes uncategorized detections
Detections by Device Role
Devices
Detections
25 Web Servers 17
113 Other Devices 13
36 File Servers 3
8 VoIP Phones 3
5 PCs 2
1 Vulnerability Scanners 1
12 Gateways 0
8 DNS Servers 0
6 Domain Controllers 0
5 Databases 0
1 DHCP Servers 0
1 Mobile Devices 0
Detections by Risk Score
Low Risk
Medium Risk
High Risk
0 Detections
29 Detections
9 Detections
Top Detections by Type
60 Cryptomining ACTIONS ON OBJECTIVE 6
83 Data Exfiltration ACTIONS ON OBJECTIVE 2
83 Ransomware Activity ACTIONS ON OBJECTIVE 2
60 Unconventional Protocol Communication COMMAND & CONTROL
60 SMB/CIFS Brute Force EXPLOITATION
56 PowerShell Remoting Activity LATERAL MOVEMENT
56 DNS Tunnel COMMAND & CONTROL
56 PsExec Activity LATERAL MOVEMENT
37 UDP Port Scan RECONNAISSANCE

SaaS-based security for edge, core, and cloud deployments.

Securing the modern enterprise means protecting a complex web of workloads consisting of hardware, applications, and data spread across edge, core, remote workforce, and cloud deployments. SaaS-based ExtraHop Reveal(x) 360 enables you to unify threat visibility across your attack surface with a truly cloud-native network detection and response (NDR) solution. Reveal(x) 360 deploys quickly, removes much of the management burden from security and IT teams, and begins providing immediate value with 360-degree visibility and situational intelligence in real time.

COMPLETE VISIBILITY

Gain deep and continuous visibility into east-west and north-south traffic from the data center to the cloud to the user and device edge.

REAL-TIME DETECTION

Cloud-scale machine learning uses more than 1 million predictive models to detect anomalous and suspicious behaviors as soon as they occur.

INTELLIGENT RESPONSE

Pivot from detection to forensic evidence in seconds with streamlined investigative workflows. Leverage integrated response automation to immediately act on threats.

CLOUD-NATIVE SECURITY FOR THE HYBRID ENTERPRISE

SaaS-delivered Network Detection & Response

Reveal(x) 360 is the first and only SaaS-based network detection and response solution that provides on-demand, unified visibility across multicloud and hybrid environments as well as distributed workforces and operations.

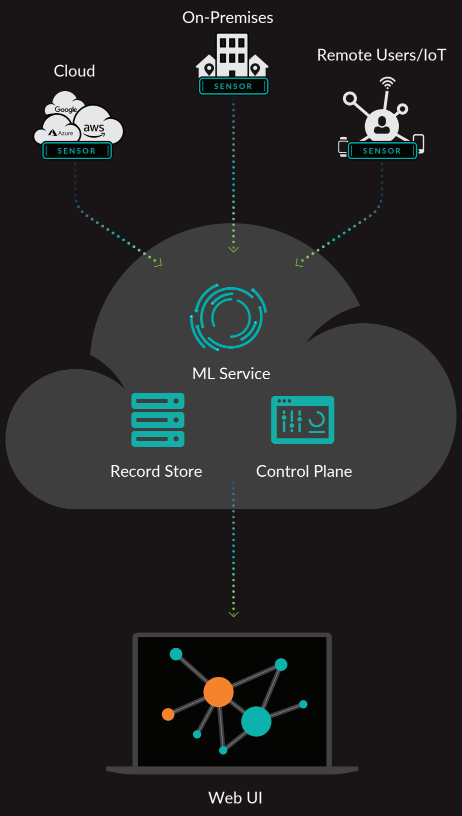
In public cloud environments, Reveal(x) 360 integrates with Amazon VPC Traffic Mirroring, Google Cloud Packet Mirroring, and the announced Microsoft Azure vTAP to deliver agentless, highly elastic NDR that scales up or down to meet your needs.

HOW REVEAL(X) 360 WORKS

Reveal(x) 360 extends cloud-native NDR across hybrid environments by providing full visibility at enterprise scale. Integrated workflows accelerate threat hunting and amplify organizational resources.

ExtraHop sensors deployed locally in data centers, clouds, and remote sites decrypt and process network data, extracting records and de-identified metadata which are sent securely to Reveal(x) 360 for behavioral analysis, real-time threat detection, and investigation.

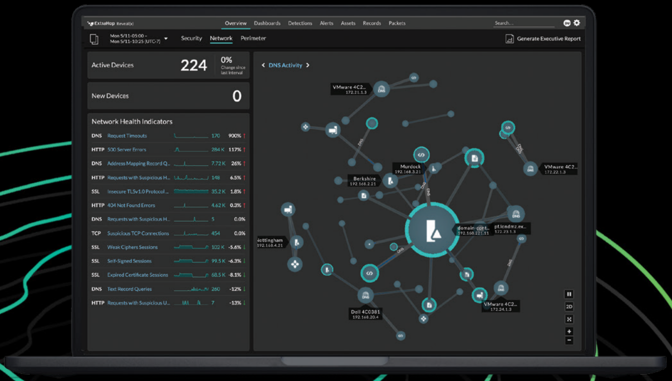
A cloud-based record store with 90-day lookback provides fully hosted and managed search for streamlined incident investigation. A cloud-hosted control plane—accessible from anywhere via the secure web-based Reveal(x) 360 user interface—gives you a unified view of the environments where sensors are deployed.



WHY CLOUD-NATIVE?

Perimeter-focused security tools often rely on fixed agents or logs that can leave visibility gaps, miss critical threats, and add unnecessary friction to DevOps processes. SaaS-based Reveal(x) 360 leverages native integrations with cloud service provider packet mirroring features to provide agentless visibility, packet-level granularity, and security at scale.

To see how Reveal(x) 360 helps international fantasy adventure game maker Wizards of the Coast remove layers of security complexity from their DevOps processes and empower developers to create with speed, read the case study and watch the video. **extrahop.com/customers/stories/wizards-of-the-coast/**



Active Devices 224 0% Change since last interval

New Devices 0

Network Health Indicators

DNS	Request Timeouts	170	900% ↑
HTTP	500 Server Errors	284 K	117% ↑
DNS	Address Mapping Record Q...	7.72 K	26% ↑
HTTP	Requests with Suspicious H...	148	6.5% ↑
SSL	Insecure TLSv1.0 Protocol ...	35.2 K	1.8% ↑
HTTP	404 Not Found Errors	4.62 K	0.3% ↑
DNS	Requests with Suspicious H...	5	0.0%
TCP	Suspicious TCP Connections	454	0.0%
SSL	Weak Ciphers Sessions	102 K	-5.6% ↓
SSL	Self-Signed Sessions	99.5 K	-6.3% ↓
SSL	Expired Certificate Sessions	68.5 K	-8.1% ↓
DNS	Text Record Queries	260	-12% ↓
HTTP	Requests with Suspicious U...	7	-13% ↓

Unified security management from edge to core to cloud in a single user interface.

USE CASES

Threat Detection

Hygiene & Compliance

Inventory & Configuration

Monitoring & Diagnostics

Incident Response

Threat Hunting

Forensic Investigation

Vulnerability Assessment

Dependency Mapping

REVEAL(X) 360 FEATURES

Cloud Record Store
Enables 90-day lookback with the ability to purchase additional bands of capacity or leverage on-demand pricing.

Cloud Control Plane
Accessible from anywhere via a secure web-based UI for unified security in a single management pane.

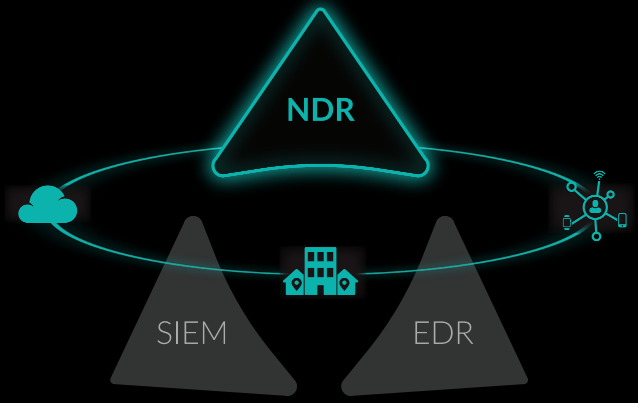
Continuous PCAP
Reveal(x) 360 Ultra offers continuous packet capture for in-depth forensic investigation.

Line-Rate Decryption
Decrypts SSL/TLS 1.3-encrypted traffic, including cipher suites that support perfect forward secrecy (PFS).

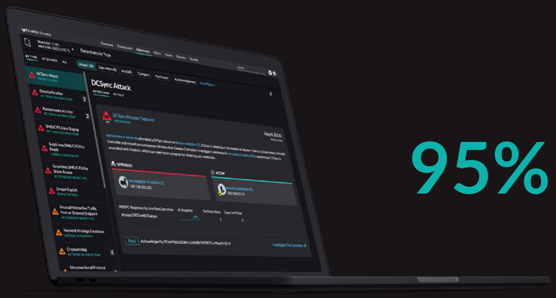
Global Intelligence
Analyzes petabytes of anonymized threat telemetry collected daily from more than 15 million devices and workloads worldwide.

Automated Inventory
Automatic and continuous asset discovery, classification, and dependency mapping across environments.

CLOUD-NATIVE NDR COMPLETES THE SOC VISIBILITY TRIAD



The missing piece in many security operations centers (SOCs) is network data. Network detection and response provides observed ground truth with context, that can't be turned off or evaded by savvy attackers, unlike log and agent-based tools. Because of this resilience, cloud-native NDR is the best approach for detecting, investigating, and responding to threats in hybrid, multicloud, remote workforce, and IoT environments.



95% FASTER THREAT DETECTION

77% IMPROVEMENT IN TIME TO RESOLVE

59% LESS STAFF TIME TO RESOLVE THREATS

IDC

Request a Free Trial **extrahop.com/request-free-trial**
Take the Demo **extrahop.com/demo/cloud**

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. Learn more at www.extrahop.com.

ExtraHop

info@extrahop.com
www.extrahop.com