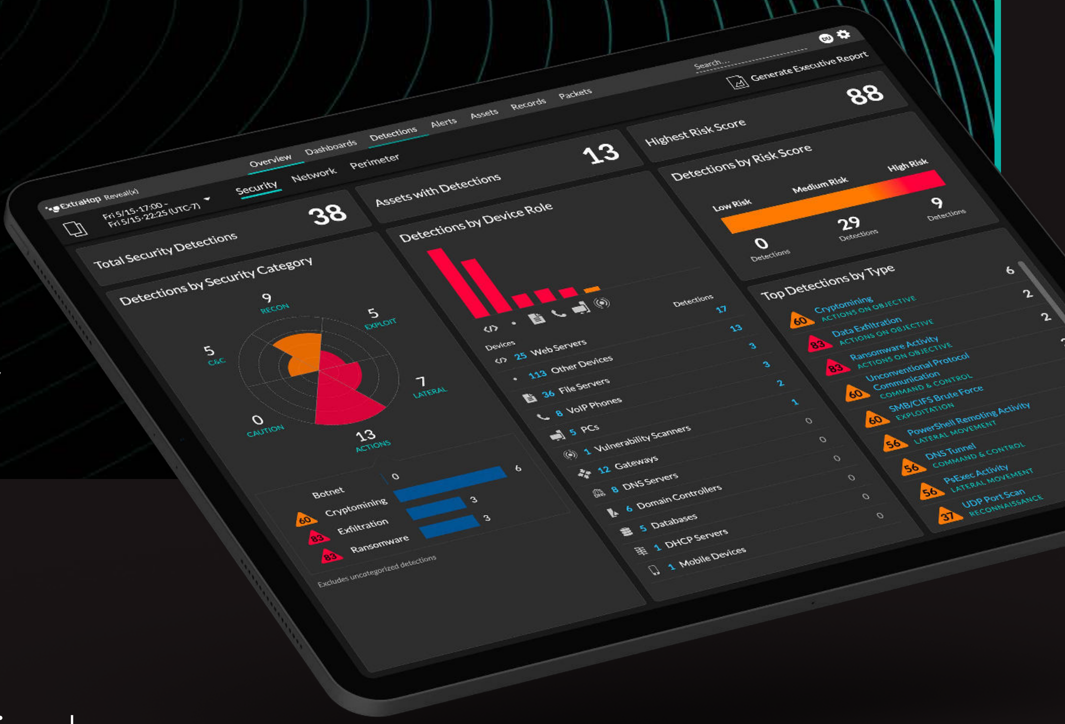
ExtraHop

Reveal(x) 360

aws partner network | competency



Security Uncompromised for the Hybrid Enterprise

Securing the hybrid enterprise means defending against advanced threats in on-premises, multicloud, and remote workforce environments. However, many organizations are finding that their current tooling and processes introduce friction and create coverage gaps. SaaS-based ExtraHop Reveal(x) 360 unifies hybrid and multicloud security in a single management pane, so you can stop ransomware, software supply chain attacks, and more—no matter where you find them.

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

Advanced AI 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 clicks with streamlined investigation and response integrations 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.

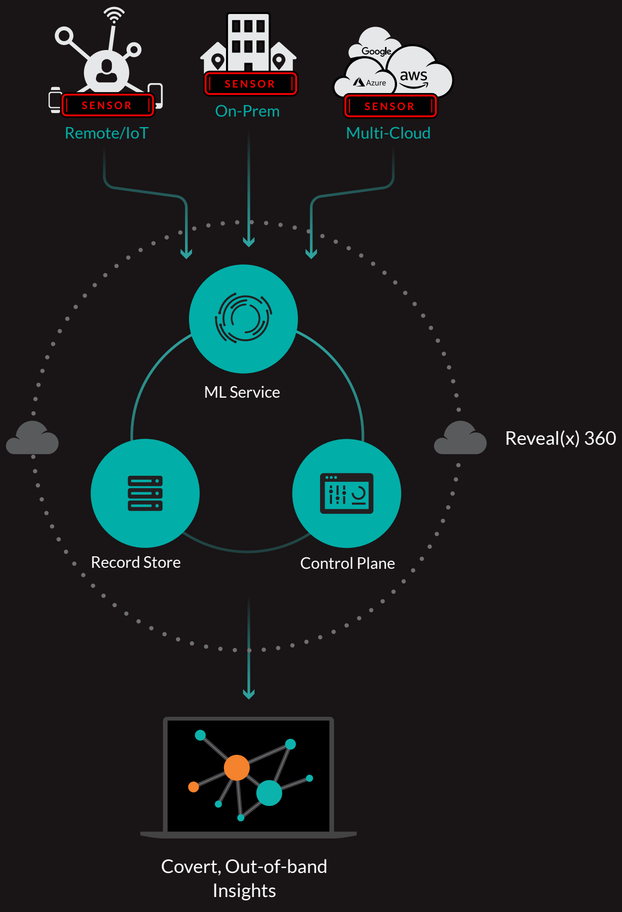
In public cloud environments, Reveal(x) 360 integrates with Amazon VPC Traffic Mirroring, Google Cloud Packet Mirroring, and the announced Microsoft Azure vTAP to deliver agentless, highly elastic NDR that scales up or down to meet your needs.

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.

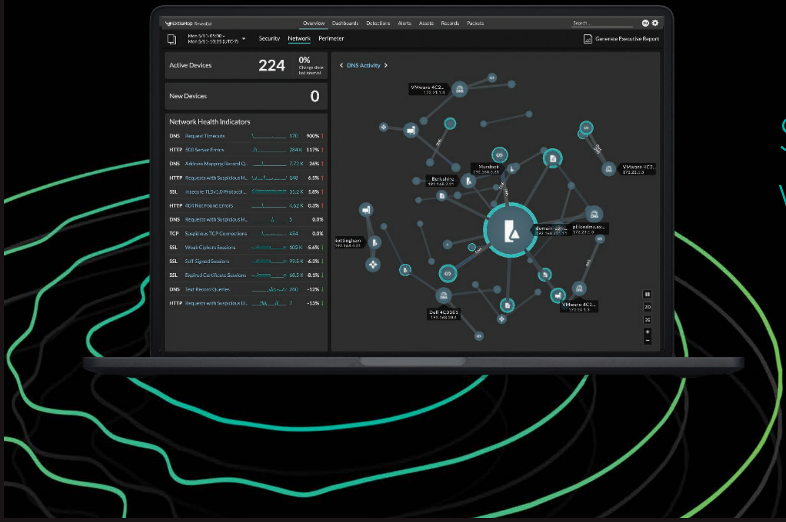
A cloud-based record store with 90-day lookback provides fully hosted and managed search for streamlined incident investigation. A cloud-hosted control plane—accessible from anywhere via the secure web-based Reveal(x) 360 user interface—gives you a unified view of the environments where sensors are deployed.



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%

Stop breaches, not business, with Reveal(x) 360.

USE CASES

Advanced Threat Detection

Workload & Data Monitoring

Container Security

Inventory & Configuration

Forensic Investigation

Vulnerability Assessment

Dependency Mapping

Compliance & Audit

Threat Hunting

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.

Unified Security
Accessible from anywhere via a secure web-based UI for unified security in a single management pane.

Continuous PCAP
Reveal(x) 360 Ultra sensors offer 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.

Managed Services
Augments lean security teams to identify vulnerabilities, detect incidents, and stop adversaries.

LAYERED CLOUD THREAT DEFENSE FOR AWS

Stop Advanced Attacks from the Inside

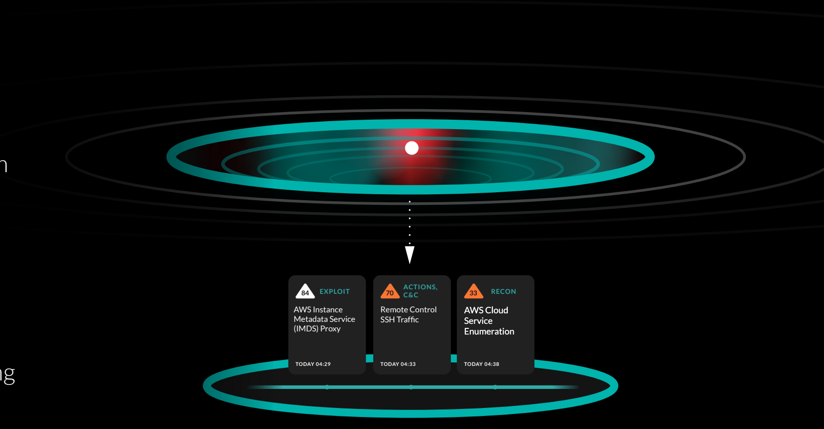
Cloud security teams are outnumbered and traditional tools can't stop advanced threats at the perimeter. As adversaries continue to evolve their attacks on mission-critical applications and workloads, enterprises need Reveal(x) 360 cloud threat defense for AWS.

With Reveal(x) 360, security teams can identify and isolate advanced attacks before they become breaches. Reveal(x) 360 offers frictionless deployment flexibility with broad visibility from VPC Flow Logs and access to packets for deep forensic investigation in a single management pane.

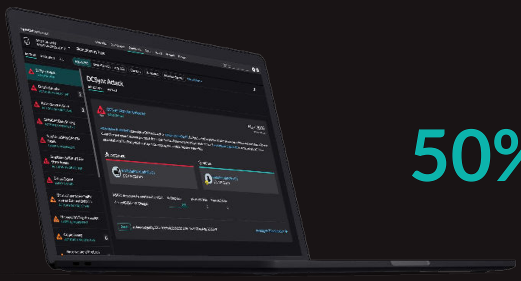
By analyzing all forms of network telemetry with advanced AI, Reveal(x) 360 eliminates coverage and visibility gaps. It also provides security teams with real-time data visualization, enabling them to identify and investigate hotspots of malicious activity. Armed with real-time information, security teams can make fast, informed decisions about what to do when threats arise.

ExtraHop offers several cloud threat defense subscription tiers featuring a cloud-hosted control plane, advanced AI service, and record store with 90-day lookback.

THE BREADTH OF VPC FLOW LOGS


84
EXPLOIT
AWS Instance Metadata Service (IMDS) Proxy
TODAY 04:29
70
ACTIONS, C&C
Remote Control SSH Traffic
TODAY 04:33
33
RECON
AWS Cloud Service Enumeration
TODAY 04:38

AND THE DEPTH OF PACKETS



50% FASTER THREAT DETECTION

84% FASTER THREAT RESOLUTION

99% FASTER TROUBLE-SHOOTING

FORRESTER

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

aws partner network | competency

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 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