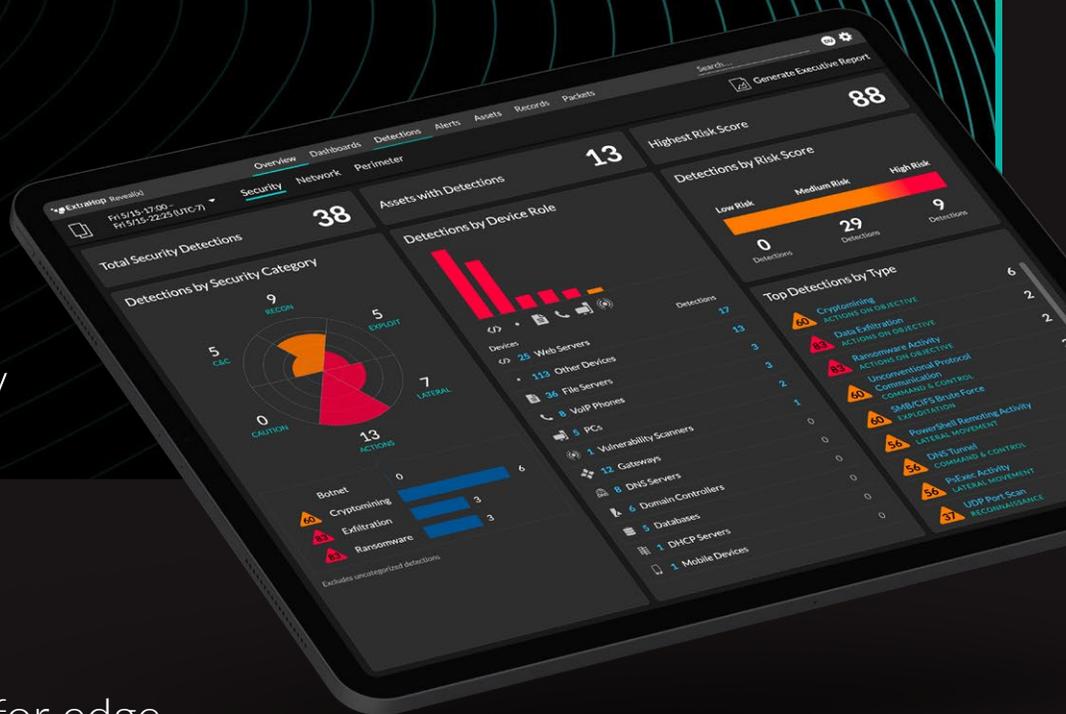




Reveal(x) 360



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. However, many organizations find their existing security processes and on-premises tools don't translate well to a hybrid infrastructure, leaving gaps and struggling to provide visibility into containerized environments. 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.

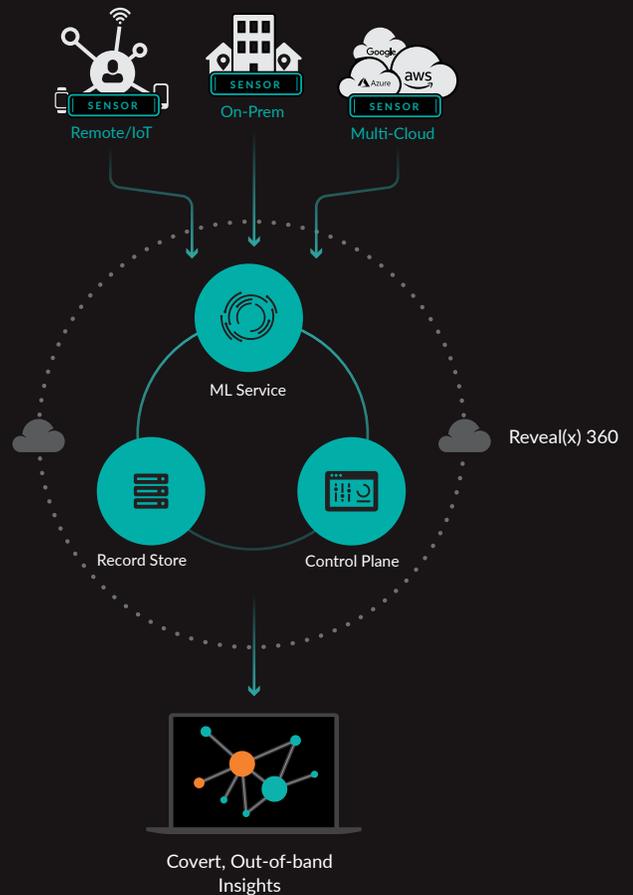
In public cloud environments, Reveal(x) 360 integrates with Amazon VPC Traffic Mirroring, Google Cloud Packet Mirroring, and the announced Microsoft Azure vTAP to deliver agentless, highly elastic NDR that scales up or down to meet your needs.

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/



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

USE CASES

Detect Advanced Threats

Monitor Sensitive Workloads

Incident Response

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

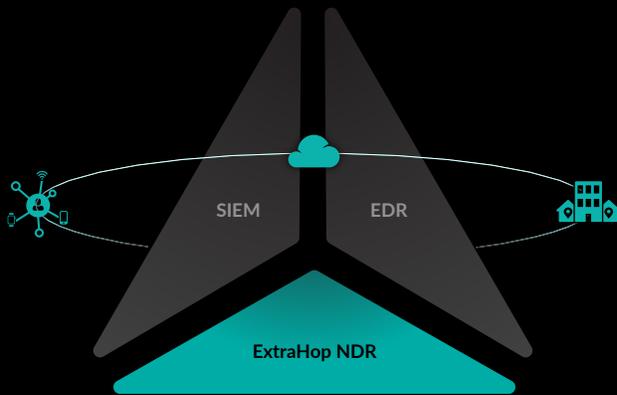
Decrypts SSL/TLS 1.3-encrypted traffic, including cipher suites that support perfect forward secrecy (PFS).

Global Intelligence

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

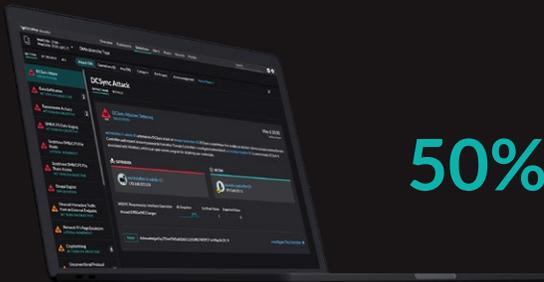
Automated Inventory

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



NDR IS FOUNDATIONAL SECURITY

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.



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



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. Learn more at www.extrahop.com



info@extrahop.com
www.extrahop.com