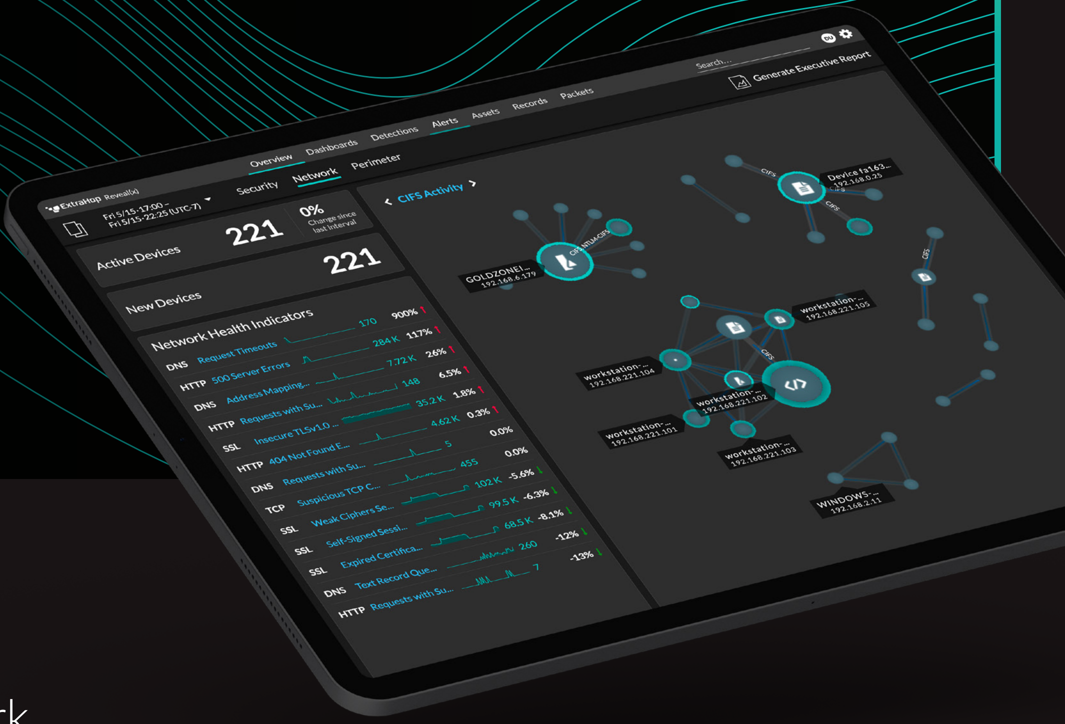
ExtraHop

Reveal(x)



Network Health Indicators

DNS	Request Timeouts	170	900% ↑
HTTP	500 Server Errors	284 K	117% ↑
DNS	Address Mapping...	7.72 K	26% ↑
HTTP	Requests with Su...	148	6.5% ↑
SSL	Insecure TLSv1.0 ...	35.2 K	1.8% ↑
HTTP	404 Not Found E...	4.62 K	0.3% ↑
DNS	Requests with Su...	5	0.0%
TCP	Suspicious TCP C...	455	0.0%
SSL	Weak Ciphers Se...	102 K	-5.6% ↓
SSL	Self-Signed Sessi...	99.5 K	-6.3% ↓
SSL	Expired Certifica...	68.5 K	-8.1% ↓
DNS	Text Record Que...	260	-12% ↓
HTTP	Requests with Su...	7	-13% ↓

Cloud-Native Network Detection & Response

Reveal(x) is the only cloud-native network detection and response (NDR) platform that provides the scale, speed, and visibility required by enterprise security teams to detect and respond to threats in hybrid environments. Reveal(x) combines automated discovery and asset classification with full payload analysis and cloud-based machine learning for threat detection and investigation.

COMPLETE VISIBILITY

With visibility from the data center to the edge to the cloud, you'll understand your enterprise from the inside out. Reveal(x) discovers, classifies, and maps dependencies for every asset communicating across the network. Out-of-band decryption of SSL/TLS 1.3-encrypted traffic enables analysts to see hidden attackers and crucial transaction details without compromising compliance or privacy.

REAL-TIME DETECTION

Reveal(x) catches threats in real time by extracting over 5,000 features from L2 to L7 to power our cloud-scale machine learning and customizable rules-based detections. Reveal(x) automatically identifies critical assets and compares peer groups to deliver high-fidelity detections with smart risk scoring and threat intel correlation, so you can prioritize your efforts and respond.

INTELLIGENT RESPONSE

The Reveal(x) workflow takes you from security event to associated packets in clicks, erasing hours spent manually collecting and parsing data. Instant answers enable immediate, confident response. Robust integrations with Splunk Phantom, Palo Alto, CrowdStrike, and more help you rise above the noise of alerts, automate investigation, and respond in time to protect your IT infrastructure.

FULL-SPECTRUM DETECTION

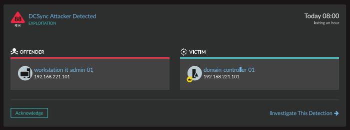
Reveal(x) provides real-time detections across the full spectrum of known and unknown attack tactics, fast, destructive threats and low-and-slow tactics, techniques, and procedures.

Hygiene
Activity that represents risk: ports, protocols, misconfigs, cryptographic compliance, vulnerable or non-compliant services

Known Attacks
IP addresses, domains, file names, payload strings, or protocol behavior were observed in past attacks (including threat intelligence feeds)

Unknown Attacks
Attacks that do not have a previously known identifier, but exhibit anomalous behavior that can be linked to part of the attack lifecycle.

← SPECTRUM OF DETECTION →

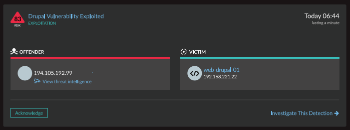


88 RISK DCSync Attacker Detected
EXPLOITATION
Today 08:00
lasting an hour

OFFENDER
workstation-it-admin-01
192.168.221.101

VICTIM
domain-controller-01
192.168.221.101

Rule-Based Detections

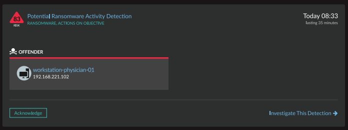


83 RISK Drupal Vulnerability Exploited
EXPLOITATION
Today 06:44
lasting a minute

OFFENDER
194.105.192.99
View threat intelligence

VICTIM
web-drupal-01
192.168.221.22

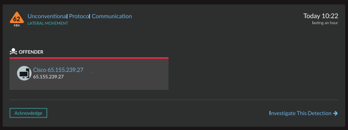
Robust Anomaly Detections



83 RISK Potential Ransomware Activity Detection
RANSOMWARE, ACTIONS ON OBJECTIVE
Today 08:33
lasting 35 minutes

OFFENDER
workstation-physician-01
192.168.221.102

Sophisticated Behavioral Detections



62 RISK Unconventional Protocol Communication
LATERAL MOVEMENT
Today 10:22
lasting an hour

OFFENDER
Cisco 65.155.239.27
65.155.239.27

Peer Group Detections

NIST MITRE | ATT&CK® CIS Controls™

PROACTIVE SECURITY USE CASES

Breach Detection & Response
Detect threats and automate intelligent response actions

Hybrid Security
Unified multi-cloud and on-premises threat detection & response

Insider Threat Detection
Detect, contain, and document risky and malicious behavior.

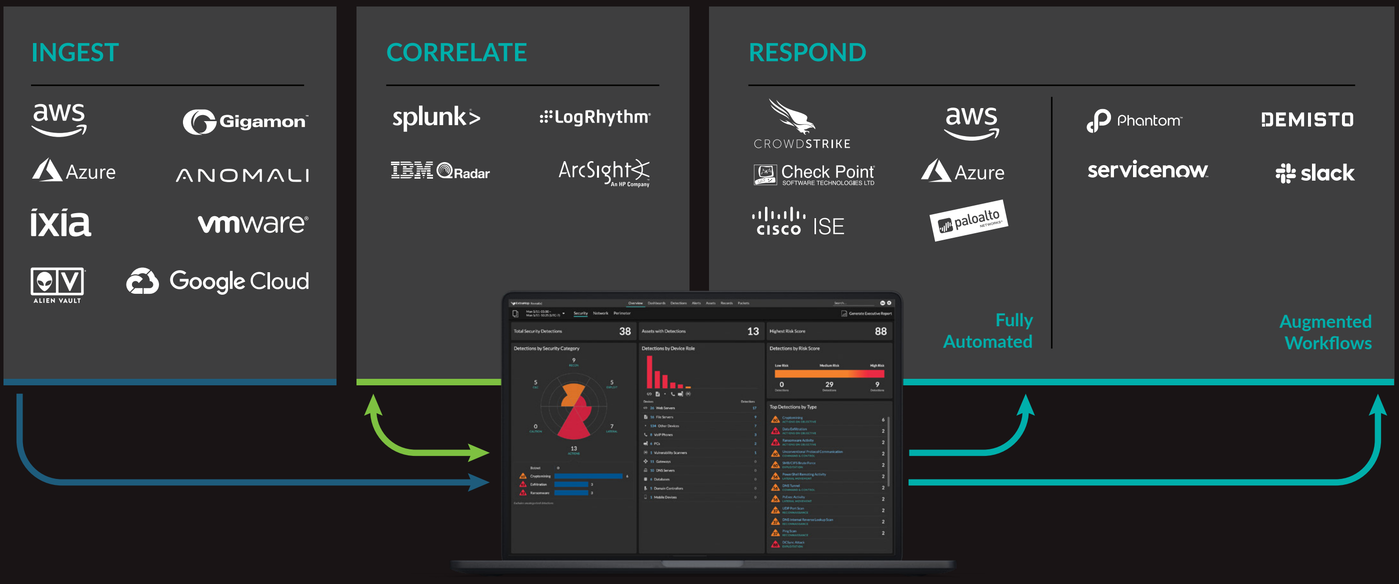
SOC + NOC Productivity
Share data and integrate tools to optimize team performance.

Threat Hunting & Audit
Find and validate risk behaviors and vulnerabilities

Hygiene & IoT Inventory
Inventory devices, audit encryption use, and decommission legacy assets.

AMPLIFY THE POWER

Of Your Enterprise Security Tools



ExtraHop Reveal(x)

REVEAL(X) FEATURES

Automated Inventory
Reveal(x) keeps an always up-to-date inventory of assets by auto-discovering and identifying everything communicating on the network.

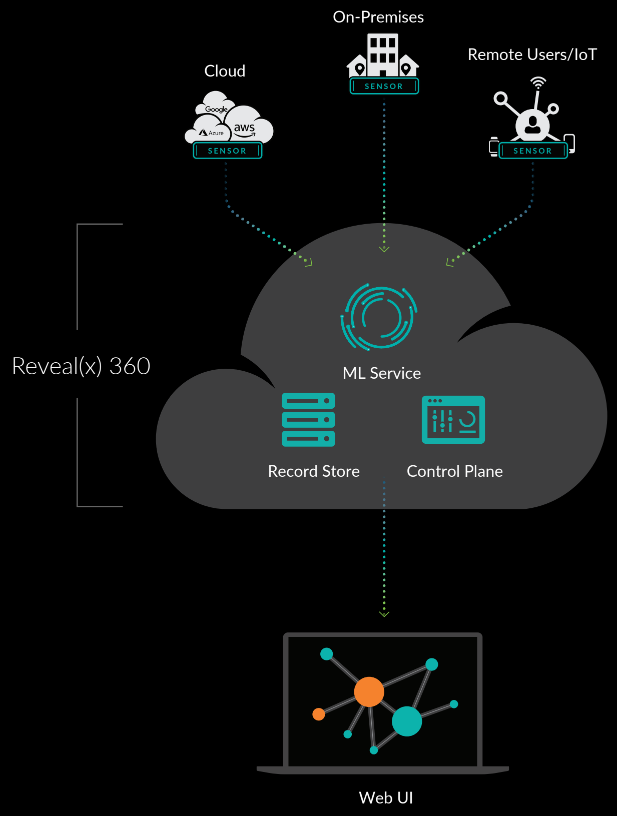
Decrypt TLS 1.3 and PFS
Reveal(x) decrypts SSL/TLS 1.3 with PFS passively and in real time so you can detect threats hiding in your encrypted traffic.

Automated Investigation
Reveal(x) enriches every detection with context, risk scoring, attack background, and expert-guided next steps to enable confident response.

Peer Group Detections
By automatically categorizing devices into precise peer groups, Reveal(x) can spot risks and attack behaviors with minimal false positives.

Cloud-Scale ML
With cloud-scale machine learning and predictive modeling drawing upon 5,000+ L2-L7 features, Reveal(x) detects, prioritizes, and contextualizes threats to your critical assets.

Confident Response Automation
Reveal(x) handles detection and investigation while powerful integrations with CrowdStrike, Phantom, Palo Alto, and more enable augmented and automated response workflows.

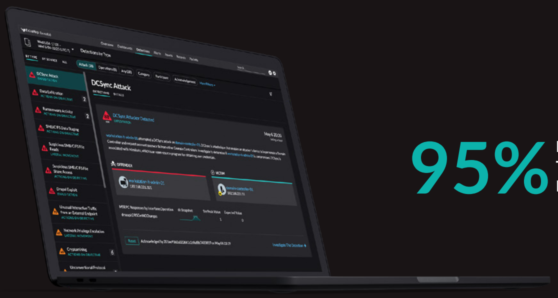


SaaS and Self-Managed Deployment Options For Every Environment

The Reveal(x) platform is available in two deployment models—SaaS-based Reveal(x) 360 and Reveal(x) Enterprise with self-managed sensors. Both deployments offer the full benefits of NDR, including cloud-delivered machine learning and threat detection capabilities.

As illustrated in the diagram, Reveal(x) 360 provides 360-degree visibility across on-premises and cloud environments, a control plane for unified visibility, and a cloud-hosted record store for situational intelligence. Reveal(x) 360 is available with reserved (annual) and on-demand pricing plans.

Reveal(x) Enterprise requires organizations to deploy and manage sensors, record store, and management systems. Reveal(x) Enterprise is available with a reserved (annual) pricing plan.



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