ExtraHop

ExtraHop Reveal(x)

Cloud-Native Network Detection & Response

Reveal(x) is the only Cloud-Native Network Detection and Response product that provides the scale, speed, and visibility required by enterprise security teams to detect and respond to threats and rise above the noise of increasingly complex hybrid network architectures, containerized applications, and the cloud.

COMPLETE VISIBILITY

Reveal(x) automatically discovers and classifies every device communicating across the network, with real-time, out-of-band decryption so security teams can see hidden attackers and crucial transaction details without compromising compliance or privacy. With full East-West visibility from the data center to the cloud to the edge, you'll understand your enterprise from the inside, out.

REAL-TIME DETECTION

Reveal(x) catches threats in real time by extracting over 5,000+ L2-L7 features from the wire to be used by 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, correlated with risk scores and threat intel so you can prioritize your efforts and respond with confidence.

INTELLIGENT RESPONSE

The Reveal(x) workflow takes you from security event to associated packet in a few clicks, erasing hours spent manually collecting and parsing data. Instant answers enable immediate, confident responses. Robust integrations with security tools including Phantom, Splunk, Palo Alto, and more help you rise above the noise of alerts, automate investigation, and act in time to protect your customers.

STOP THREATS FASTER.

Reveal(x) provides real-time detections, mapped to each step of the attack chain, with expert next steps and security framework references such as MITRE ATT&CK and CIS Top 20 links. With all this context you'll spot valid threats up to 95 percent faster.

Command & Control	Reconnaissance	Exploitation	Lateral Movement	Action on Objective
Outbound Activity	Port Scans	LLMNR Poisoning	Suspicious RDP/SSH	Ransomware
Suspicious IPs/URIs	User Enumeration	IP Fragment Overlap	Peer Group Anomalies	Encrypted Data
Suspect Connections	Login Attempts	RDP Brute Force	Share & File Access	External Data Transfer
Abnormal Geolocation	Reverse DNS Lookups	Suspicious CIFS	Transaction Failures	Database Exfiltration
More Detections	More Detections	More Detections	More Detections	More Detections

PROACTIVE SECURITY USE CASES

DETECT THREATS

Breach Detection & Response
Detect threats and augment or automate response actions

Hybrid Security
Unified cloud-native and on-premises threat detection and response

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

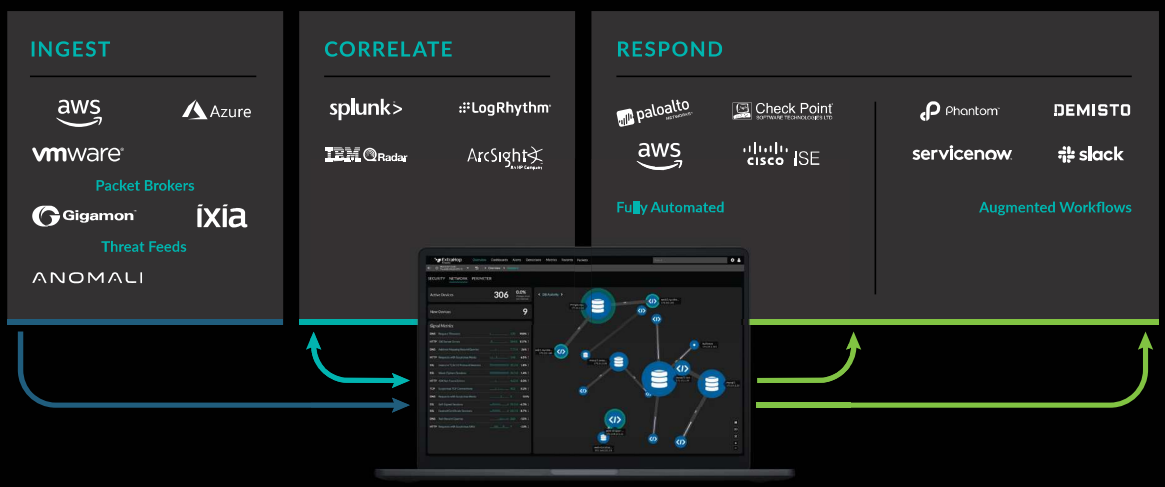
IMPROVE POSTURE

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

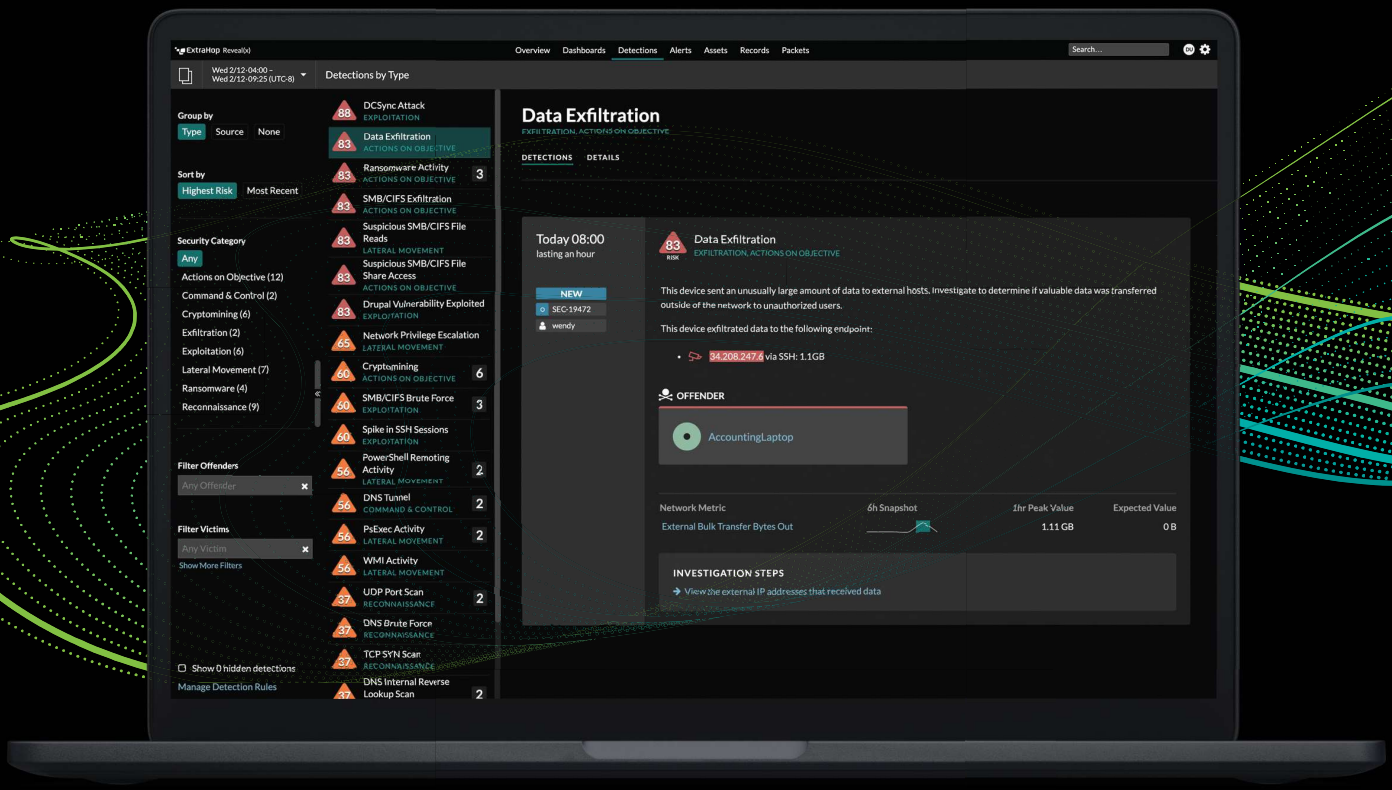
Red Team /Audit Findings
Find or validate concerns and vulnerabilities

Security Hygiene
Inventory devices, audit encryption, and decommission risky assets

AMPLIFY THE POWER OF YOUR ENTERPRISE TOOLS



Enterprise integrations accelerate and automate response so your team can cut time to resolve security threats by 59 percent.
View all our integrations at:
www.extrahop.com/platform/integrations



EXTRAHOP REVEAL(X) FEATURES

Automated Inventory
Reveal(x) keeps an always up-to-date inventory through auto-discovery and classification of everything communicating on the network.

Perfect Forward Secrecy Decryption
Reveal(x) decrypts SSL/TLS 1.3 with PFS passively and in real time so you can detect threats hiding in your own 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 strange behavior with minimal false positives.

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

Confident Response Orchestration
Reveal(x) handles detection and investigation while powerful integrations with solutions like Phantom and Palo Alto enable augmented and automated response workflows.

OUR CUSTOMERS RISE ABOVE THE NOISE.

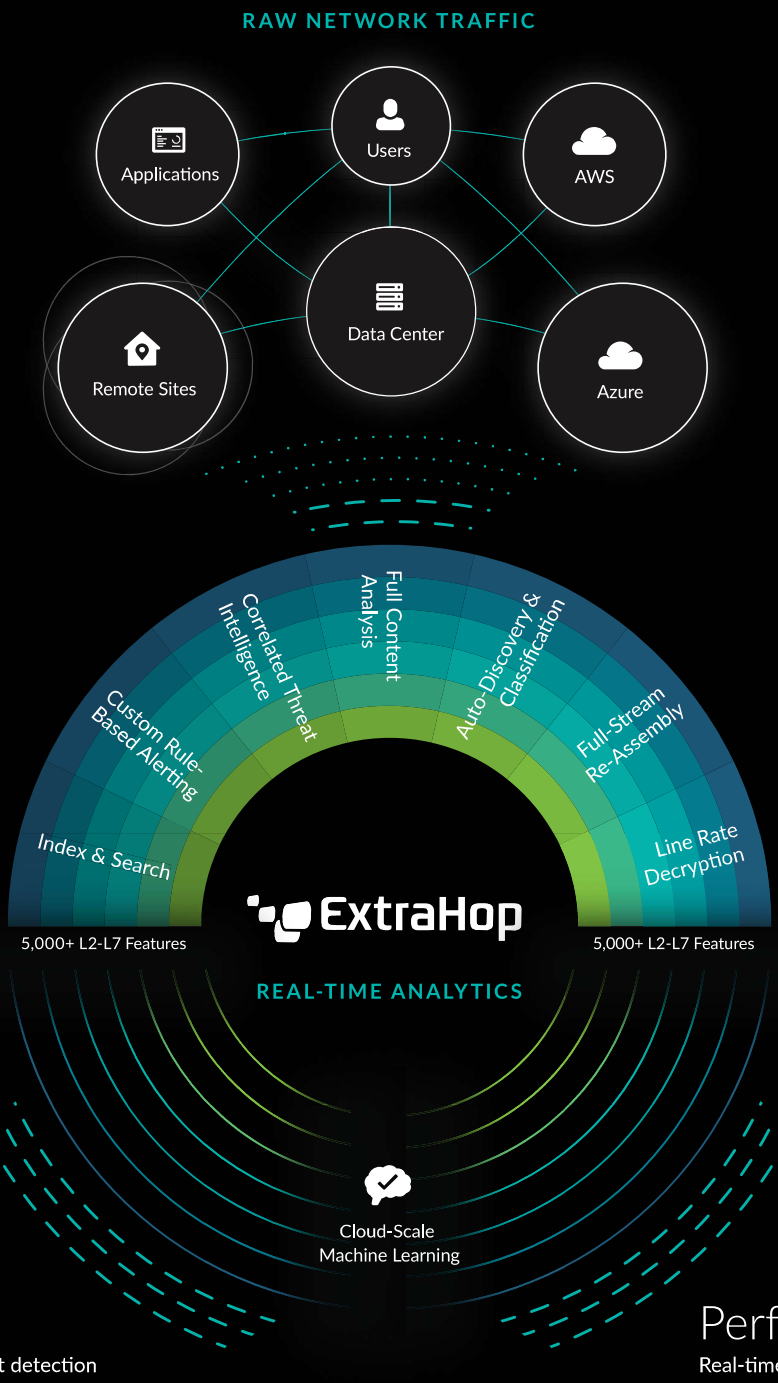
IDC

95%
IMPROVEMENT IN TIME TO DETECT

77%
IMPROVEMENT IN TIME TO RESOLVE

59%
REDUCTION IN STAFF TO RESOLVE

25%
MORE SECURITY THREATS SUCCESSFULLY IDENTIFIED



Security

High-fidelity threat detection
Hygiene and compliance
Critical asset discovery
1-click threat investigation
Automated response via SOAR

BUSINESS RESULTS

Performance

Real-time application analytics
ML-driven anomaly detection
Application dependency mapping
End-to-end visibility and hygiene
Guided investigation

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, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop
520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com