ExtraHop

ExtraHop Reveal(x)

Network Traffic Analysis for the Enterprise

Reveal(x) is the only Network Traffic Analysis 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

Our cloud-based machine learning uses over 4,700 features to detect suspicious behavior in real time. Reveal(x) automatically sorts assets into peer groups, focusing the scrutiny on the assets most critical to your business. High-fidelity detections correlated with risk scores and threat intelligence help you easily prioritize your time for greater operational efficiency and confident response.

GUIDED INVESTIGATION

The Reveal(x) workflow takes you from security event to associated packet in a few clicks, erasing hours spent manually collecting and parsing data. Immediate 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.

RISE ABOVE UNCERTAINTY.

Reveal(x) provides real-time detections, mapped to each step of the attack chain, with expert-recommended next steps for investigation built right in. With all this context, you'll spot legitimate dangers up to 95 percent faster.

Command & Control	Reconnaissance	Exploitation	Lateral Movement	Action on Objective
Outbound Activity	Port Scans	LLMNR Poisoning	Suspicious RDP/SSH	Sensitive Data
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 all stages of the attack lifecycle and expedite forensics

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

Ransomware Defense
Contain and minimize active attacks, recover data

IMPROVE POSTURE

SOC Productivity
Prioritized detection, reduced false positives

Red Team/Audit Findings
Find or validate concerns and vulnerabilities

Reduce Attack Surface
Improve hygiene, audit encryption, and decommission risky assets

> “Fast, amazingly thorough... Reveal(x) is a product with which many security operations center (SOC) teams could hit the ground running.”
>
> **DAVE SHACKLEFORD, SANS INSTITUTE INSTRUCTOR**

SANS

RESPOND WITH CONFIDENCE

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

Phantom splunk> paloalto NETWORKS aws servicenow IBM

EXTRAHOP REVEAL(X) FEATURES

Automated Inventory
Reveal(x) ensures an always up-to-date inventory with no manual effort by auto-discovering and classifying everything on the network.

Perfect Forward Secrecy Decryption
Reveal(x) decrypts SSL and TLS 1.3 encryption passively and in real time so you can maintain compliance with full visibility into encrypted threats.

Automated Investigation
Reveal(x) contextualizes detections from an entire transaction with threat intelligence, risk, and asset value for easier triaging and response.

Peer Group Detections
By automatically categorizing devices into highly specific peer groups, Reveal(x) can spot strange behavior with minimal false positives.

Advanced Machine Learning
With machine learning using 4,700+ features, Reveal(x) detects, prioritizes, and surfaces threats according to your critical assets.

Confident Response Orchestration
Reveal(x) handles detection and investigation while powerful integrations with solutions like Phantom and Palo Alto help you automate remediation.

OUR CUSTOMERS RISE ABOVE THE NOISE.

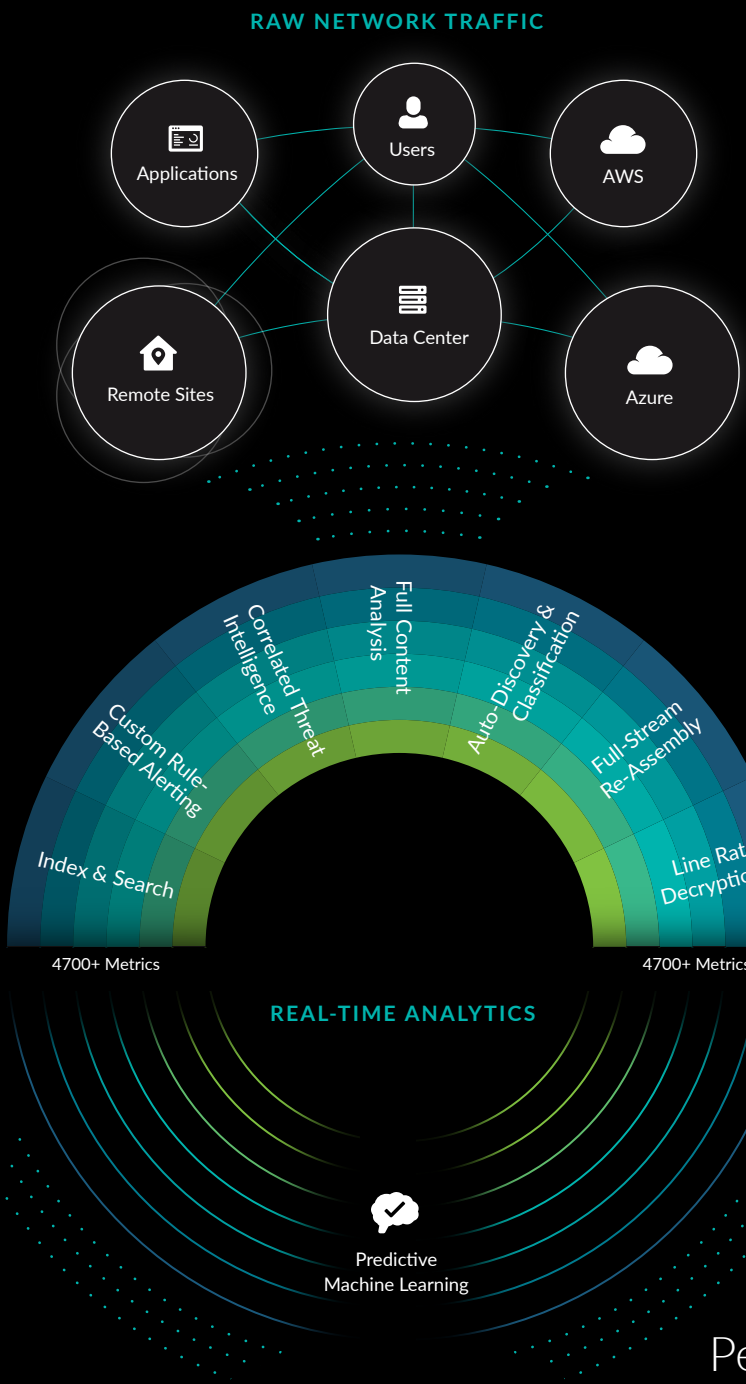
IDC

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

Performance

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

BUSINESS RESULTS

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

ExtraHop

520 Pike Street, Suite 1700
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com