ExtraHop

Reveal(x)

Network Traffic Analysis for the Enterprise

UNPRECEDENTED VISIBILITY. DEFINITIVE INSIGHTS. IMMEDIATE ANSWERS.

Reveal(x) provides the visibility, insights, and answers that security analysts need to respond quickly and confidently to the highest priority threats against their organization's critical assets. It starts by automatically discovering and classifying every device communicating across the network, and using machine-learning driven behavioral analysis to detect anomalous and malicious activity.

Analysts are provided with a prioritized list of detections, correlated with third-party threat intelligence, that they can explore instantly, from flows to transactions to decrypted packets in just a click. The SOC can use this rich detail to confidently automate investigation and response through direct integrations and orchestration.

Reveal(x) is the only Network Traffic Analysis product that provides the scale, speed, and visibility required by enterprise security teams across hybrid network architectures, containerized applications, and the cloud.

UNPRECEDENTED ENTERPRISE VISIBILITY

Reveal(x) provides richer data and context than any other network security analytics product.

AUTO-DISCOVER AND CLASSIFY EVERY DEVICE that communicates on the network, including BYOD, IOT, and devices that cannot be instrumented or logged.

EASILY FOCUS ON CRITICAL ASSETS such as databases, AAA and DNS servers, executive laptops and R&D systems.

ACCESS AN ENTIRE SET OF L2-7 DATA FOR A TRANSACTION including context and dependencies across tiers, in one event

ANALYZE 50+ PROTOCOLS decrypting SSL and perfect forward secrecy (PFS) traffic

DEFINITIVE INSIGHTS

Reveal(x) uses real-time analytics and machine learning on wire data, the richest source of insight available on the network, to detecting anomalous behavior impacting critical assets. Our cloud-based ML detection system warns you when suspicious behavior occurs, and maps the activity to one or more steps in the attack chain: Command & Control, Reconnaissance, Exploitation, Lateral Movement, or Action on Objective.

- Focus extra scrutiny on critical assets to get warnings and full context around any anomalous behavior affecting your most valuable data.
- Prioritize investigations based on helpful context, including correlated detections, risk scores, and optional annotations from threat intelligence feeds
- Accelerate and simplify remediation and proactively address key use cases.

IMMEDIATE ANSWERS

The Reveal(x) analysis-first workflow takes you from issue to associated packet in a matter of clicks. This simplicity replaces hours spent manually collecting and parsing data. Now you can access real-time insights and rapid root cause determination. Global search and indexing provide immediate access to security insights. And ExtraHop integrates with your existing security infrastructure.

- Prioritize based on automatically correlated live metrics, transaction records, and packets for forensic lookback
- Visualize and explore all communications with live, interactive 3D activity maps
- Automate response using Splunk, Phantom, Palo Alto, ServiceNow, Cisco, Slack, Ansible, Moogsoft, and others

INSTANT PRODUCTIVITY

ExtraHop Reveal(x) organizes likely attack activities according to an attack chain model. Out of the box, Reveal(x) supports the most common security and compliance use cases.

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 misbehavior and malice

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 and decommission assets and services

CUSTOMER VALUE

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

INTEGRATE. AUTOMATE. WIN.

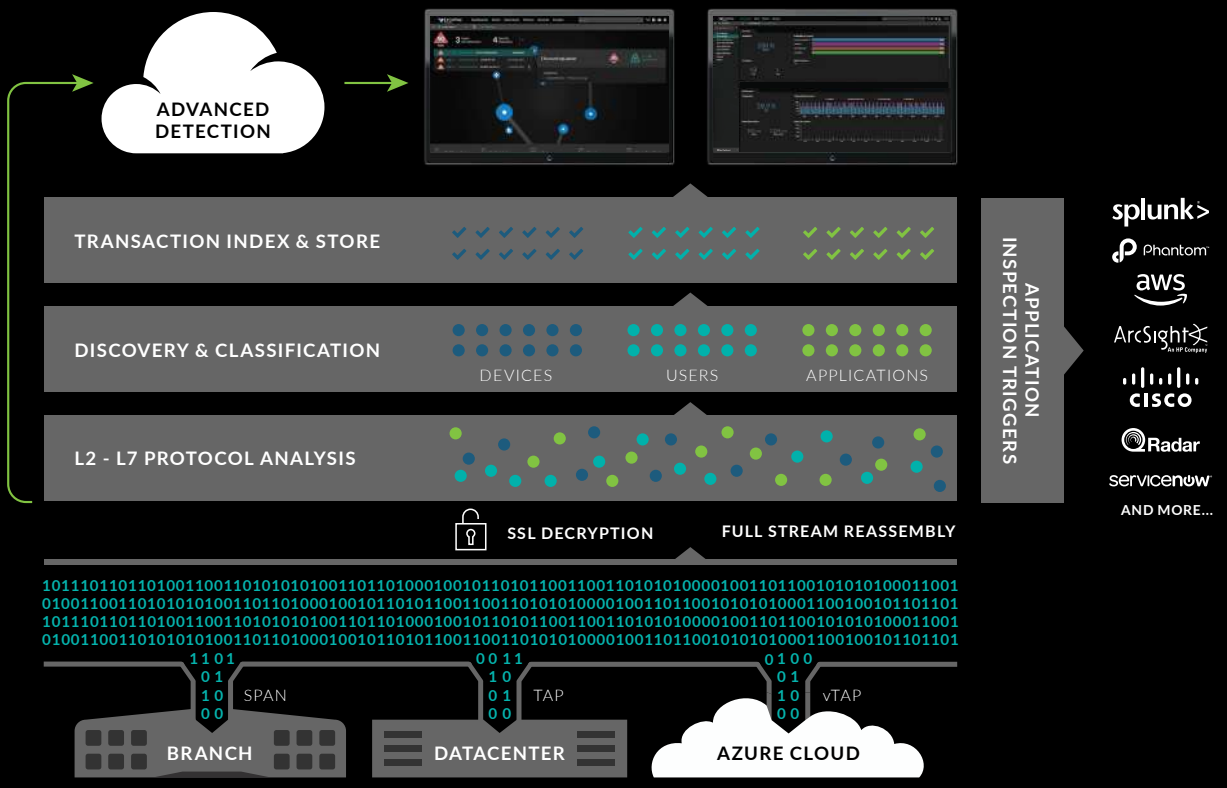
Reveal(x) integrates with every component of your security workflow so you can optimize your resources and act with confidence.

Phantom, aws, splunk>, paloalto NETWORKS, ArcSight An HP Company, servicenow, amazon web services, cisco, ALIEN VAULT, CYLANCE, LogRhythm, Radar, vmware, HipChat, slack, ANOMALI

View all our integrations at www.extrahop.com/platform/integrations

HOW IT WORKS

Powered by wire data, the richest data source available, ExtraHop Reveal(x) focuses behavioral detection on critical assets providing fast, high-fidelity insights into what matters in your environment.



SIMPLE SUBSCRIPTIONS SUITED TO ANY SECURITY PROGRAM

STANDARD

Ideal for SecOps teams with a modest security program and monitoring requirements

FEATURES

Security Detection
Global Index & Search for Rapid Investigation
50 plus Enterprise Protocols
Threat Intelligence Integration

PREMIUM

For mature programs needing encrypted traffic analysis and integrations

FEATURES

ALL STANDARD FEATURES +
+ Decryption (SSL & PFS)
+ Integration & Automation

ULTRA

For sophisticated, proactive programs with forensic and retention requirements

FEATURES

ALL PREMIUM FEATURES +
+ Continuous Packet Capture with Extended Lookback

ABOUT EXTRAHOP NETWORKS

ExtraHop is the leader in analytics and investigation for the hybrid enterprise. We apply real-time analytics and advanced machine learning to every business transaction to deliver unprecedented visibility, definitive insights, and immediate answers that enable security and IT teams to act with confidence. The world's leading organizations trust ExtraHop to support core digital business initiatives like security, IT modernization, and application service delivery. Hundreds of global ExtraHop customers, including Sony, Microsoft, Adobe, and DIRECTV, already use ExtraHop to accelerate their digital businesses. To experience the power of ExtraHop, explore our interactive online demo. Connect with us on Twitter and LinkedIn.

ExtraHop

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

www.extrahop.com