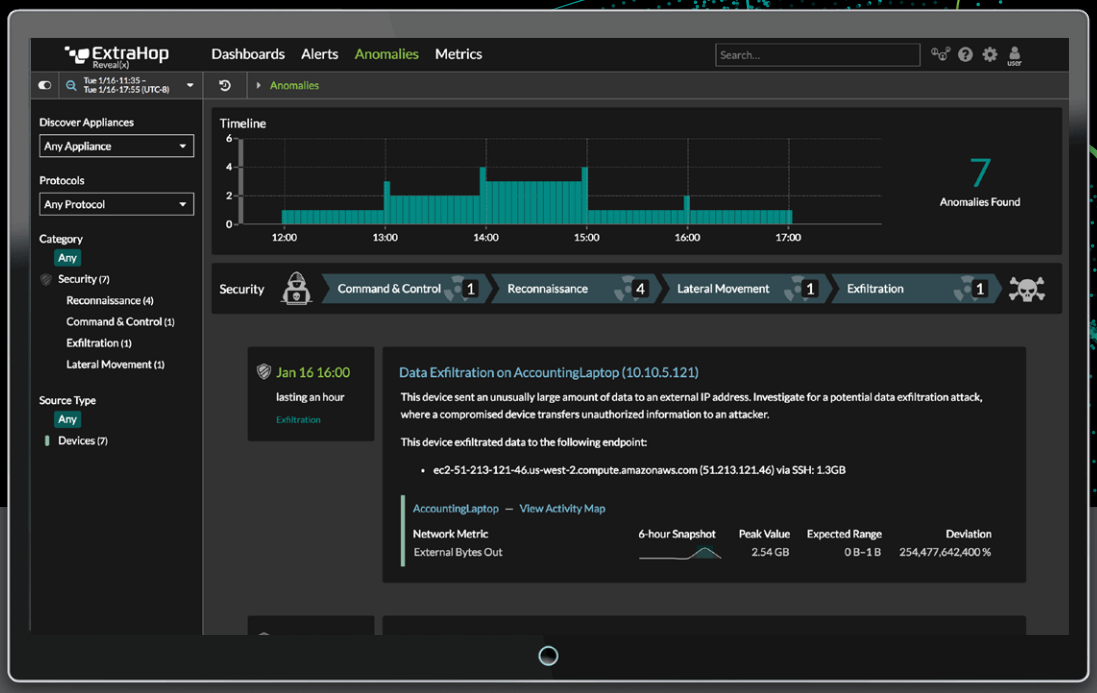
ExtraHop

Reveal(x)

Security Analytics Driven By AI



UNPRECEDENTED VISIBILITY.
ADVANCED BEHAVIORAL ANALYTICS.
AUTOMATED INVESTIGATIONS.

Few (if any) security teams have 100% visibility throughout their network. They are held back by siloed data, encrypted traffic, tool sprawl, and new technologies deployed without a plan for security monitoring, such as cloud services and containers. Despite these blind spots, analysts still face an alert cannon of data, struggling to identify the attack activities and risks hidden there.

ExtraHop believes a better source of insight can empower modern security programs, shortening investigations while providing empirical evidence for rapid, confident results. ExtraHop Reveal(x) harnesses wire data and artificial intelligence to analyze behavior affecting critical assets. Rather than just flagging potential problems, Reveal(x) accelerates security operations with an automated 3-in-1 workflow of discovery, correlation, and investigation.

Analysts see a triaged list of anomalies they can explore immediately through real-time access to forensic-quality data that is directly linked from applications down to packets. After review, integrations can send these insights directly into your preferred response systems. And everything can be customized to work with your business and security systems, processes, and tools.

Unprecedented Enterprise Visibility

You can finally eliminate the opaque network by identifying encrypted traffic, rogue nodes, IoT devices, and BYOD systems the moment they communicate on the network. This situational intelligence turns the network into the most comprehensive and high-fidelity data source available, all in real time.

- Auto-discover and auto-classify all connected devices, including segments that agents and logs don't address
- Easily focus extra attention 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 40+ protocols, decrypting SSL and perfect forward secrecy (PFS) traffic

ADVANCED BEHAVIORAL ANALYTICS

With ExtraHop's real-time analytics and wire data-driven anomaly detection, you can spot abnormal behavioral patterns as they occur. By continuously monitoring all assets, ExtraHop can highlight those displaying unusual behavior, and these and business-critical systems can be given extra attention.

Metrics captured on-premises are anonymized and sent to our machine-learning based anomaly detection engine in the cloud. The anomaly detection engine warns you when suspicious activity occurs on the network, and maps those warnings to one or more steps of the attack chain, including Command & Control, Reconnaissance, Lateral Movement, and Data Exfiltration.

- Gain insight into unusual and risky behavior affecting users, devices, databases, applications, microservices, and containers
- Leverage crowdsourcing to identify emerging threats
- Achieve results easily with ready-to-go solutions for proactive security as well as key attack use cases

AUTOMATED INVESTIGATION

The Reveal(x) analytics-first workflow takes you from issue to associated packet in a matter of clicks. This simplicity replaces hours spent manually collecting and parsing through data, enabling 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 the attack chain using live metrics, transaction records, and packets for forensic lookback
- Visualize live 3D activity maps showing communications between nodes
- 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, and also comes pre-configured to support the most common security and compliance use cases.

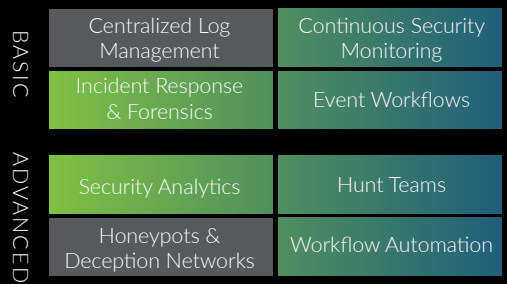
EXTRAHOP REVEAL(X) ATTACK CHAIN DETECTIONS

Command & Control 1	Reconnaissance 3	Lateral Movement 2	Exfiltration 1
Outbound activity	Port Scans	Share access	Data movement
Suspicious Connection	Login attempts	File access	Geolocation
DNS Lookups	Transaction failures	SSH usage	

PROACTIVE SECURITY USE CASES

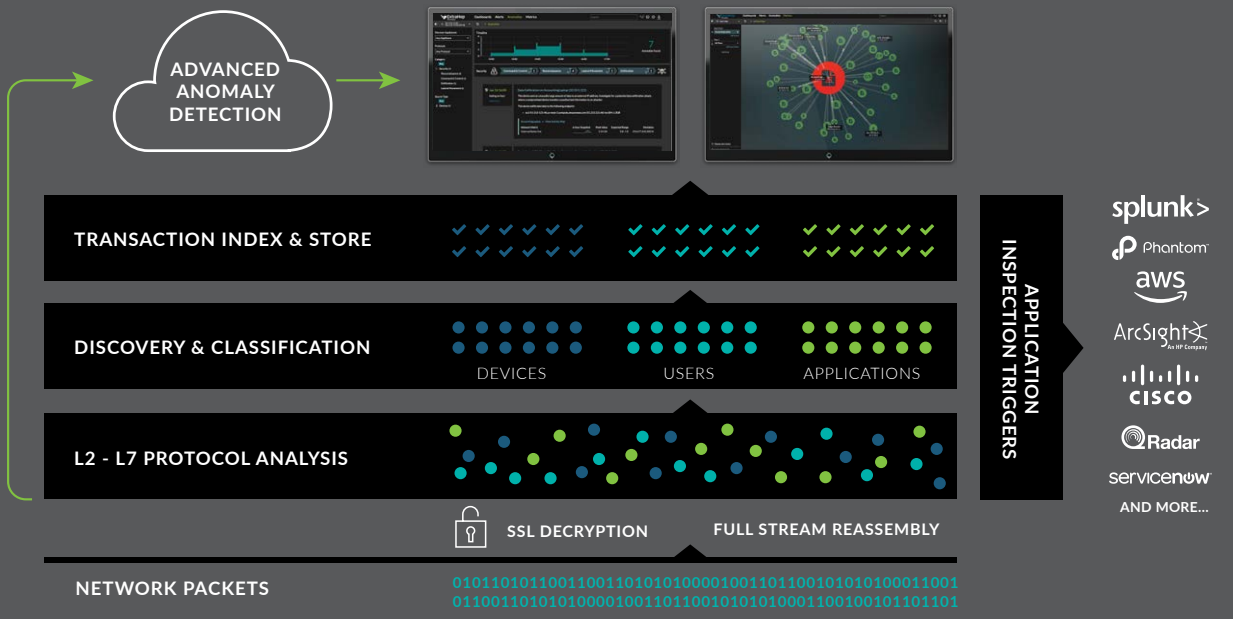
- East-West Traffic Analysis
- Ransomware Detection
- Automated Threat Hunting
- Anonymous sessions and weak ciphers
- Vulnerable certificates (expiring and wildcard)
- Insecure protocol usage (FTP, telnet, POP3, IMAP, and SNMP v1 and V2)
- Outdated transport layer security protocols (such as SSLv3m and TLSv1.0)
- Custom analytics for rapid deployment of new, real-time metrics and triggers
- Hybrid Security Monitoring
- Public and Private cloud usage
- PII and clear text transmission
- Encryption and Cipher Strength
- Enabling GDPR Compliance
- Continuous Packet Capture

WIRE DATA PROVIDES HIGH-FIDELITY TRANSACTIONAL EVIDENCE TO ENABLE THE EVOLVING SECURITY OPERATIONS CENTER (SOC).



HOW IT WORKS

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



SIMPLE SUBSCRIPTIONS SUITED TO ANY SECURITY PROGRAM

STANDARD

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

FEATURES

- Security Anomaly Detection
- Global Index & Search
- 40 plus Enterprise Protocols

PREMIUM

For mature programs needing encrypted traffic analysis and integrations

FEATURES

- Security Anomaly Detection
- Global Index & Search
- 40 plus Enterprise Protocols
- \+ Decryption (SSL & PFS)
- \+ Integration & Automation

ULTRA (coming soon)

For sophisticated, proactive programs with forensic and retention requirements

FEATURES

- Security Anomaly Detection
- Global Index and Search
- 40 plus Enterprise Protocols
- Decryption (SSL and PFS)
- Integration & Automation
- \+ Continuous packet capture
- \+ Extended storage

ABOUT EXTRAHOP NETWORKS

ExtraHop is the first place IT turns for insights that transform and secure the digital enterprise. By applying real-time analytics and machine learning to all digital interactions on the network, ExtraHop delivers instant and accurate insights that help IT improve security, performance, and the digital experience. Just ask the hundreds of global ExtraHop customers, including Sony, Lockheed Martin, Microsoft, Adobe, and Google. To experience the power of ExtraHop, explore our interactive online demo. Connect with us on Twitter, LinkedIn, and Facebook.

ExtraHop

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