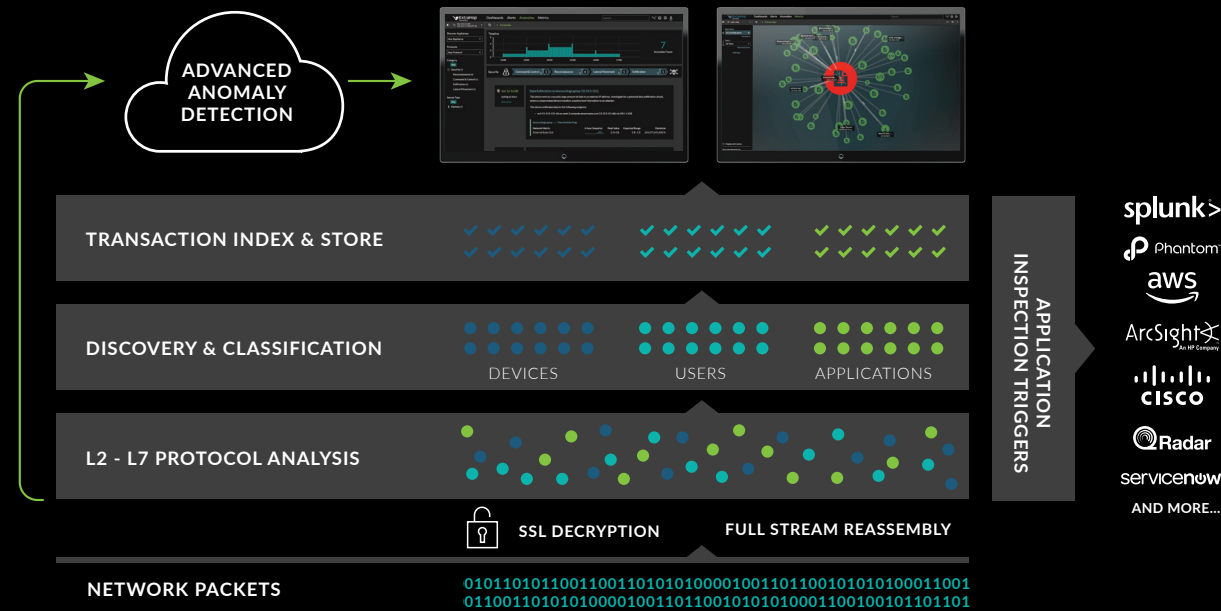


HOW IT WORKS

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.



Reveal(x)

Network Security Analytics Powered By AI

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.



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

DETECT BREACHES. AUTOMATE INVESTIGATIONS. ELIMINATE THREATS.

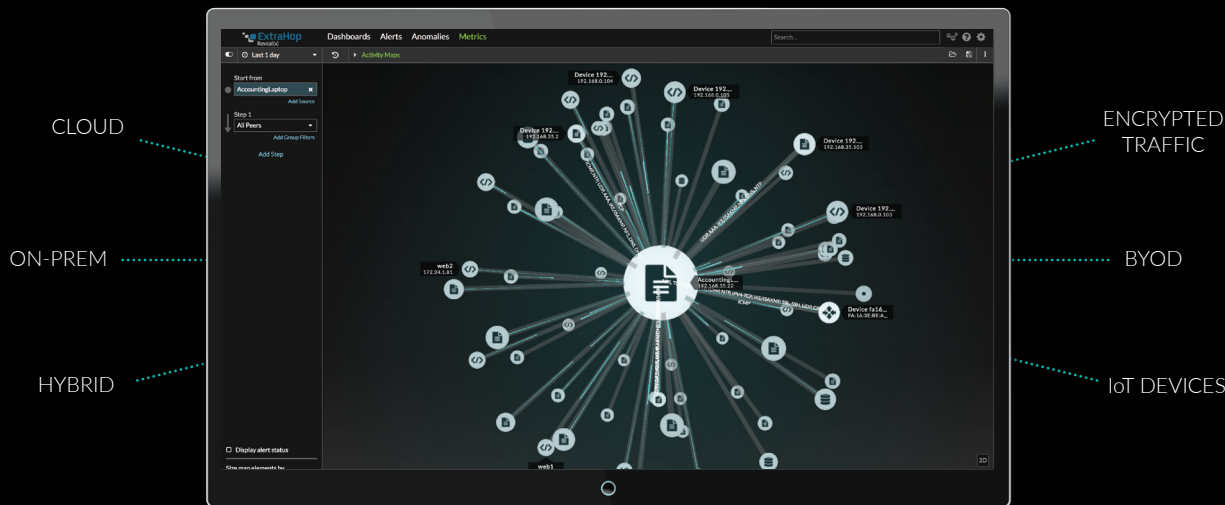
Security teams face the constant challenge of needing to gather and analyze large amounts of data and act quickly based on what they see. They need total visibility throughout their network, but they are held back by siloed data, encrypted traffic, tool sprawl, and the challenges of hybrid network architectures, containerized applications, and the cloud.

Many security products deliver a flood of alerts, mostly false positives, that require manual investigation and take precious analyst attention away from the threats that really matter.

ExtraHop Reveal(x) takes a different approach.

Reveal(x) automatically discovers and classifies everything communicating across the network and uses advanced behavioral analysis to detect anomalous behavior and threats against critical assets. Analysts see a triaged list of true anomalies they can explore with a single click to auto-correlated forensic data, from transactions down to packets. Integrations can automatically kick off further investigation and response, and everything can be customized to work with your business and security systems, processes, and tools.

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



ADVANCED BEHAVIORAL ANALYTICS

Using real-time analytics and machine learning on wire data, the richest source of insight available on the network, Reveal(x) detects anomalous behavior affecting critical assets. Using anonymized metrics, our cloud-based machine learning anomaly detection engine warns you when suspicious behavior occurs, and maps the activity to the steps in the attack chain, including Command & Control, Reconnaissance, Lateral Movement, and Data Exfiltration.

- Focus extra scrutiny on critical assets to get warnings and full context around any anomalous behavior affecting your most valuable data.
- Leverage crowdsourcing to identify emerging threats.
- Accelerate and simplify remediation and proactively address key use cases.



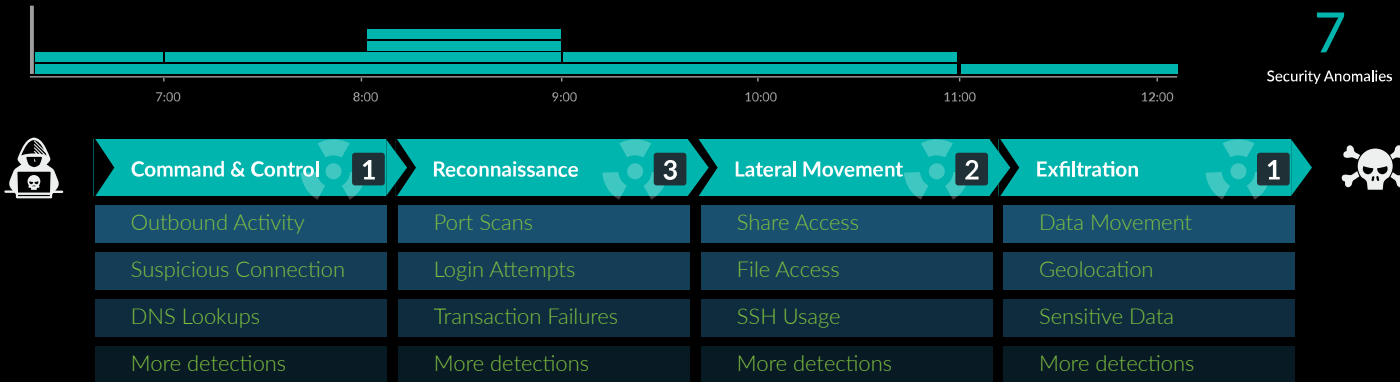
AUTOMATED INVESTIGATION

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 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.



PROACTIVE SECURITY USE CASES

- 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
- 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

INTEGRATE. AUTOMATE. WIN.

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



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

