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.
RISE ABOVE UNCERTAINTY.
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.

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

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

**INGEST**

*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](http://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.**

95% IMPROVEMENT IN TIME TO DETECT  
77% IMPROVEMENT IN TIME TO RESOLVE  
59% REDUCTION IN STAFF TO RESOLVE  
25% MORE SECURITY THREATS SUCCESSFULLY IDENTIFIED
ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach uses cloud-scale machine learning to provide complete visibility, real-time detection, and intelligent response. We help the world’s leading enterprises rise above the noise of alerts, organizational silos, and runaway technology by detecting threats up to 95 percent faster and accelerating response by up to 60 percent. With ExtraHop, you have the perspective you need to protect and scale your business.

© 2020 ExtraHop Networks, Inc. All rights reserved. ExtraHop is a registered trademark of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners.