ExtraHop Reveal(x) CLOUD-NATIVE NETWORK DETECTION & RESPONSE
ExtraHop’s cloud-native network detection and response uses cloud-scale machine learning applied to all network traffic – from the cloud to the datacenter to the IoT device – to provide complete visibility, real-time detection, and intelligent response.

WHY CHANGE?

<table>
<thead>
<tr>
<th>THE COST OF COMPLEXITY</th>
<th>WHY EXTRAHOP REVEAL(X)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of Visibility</td>
<td>100Gbps Speed and Scale</td>
</tr>
<tr>
<td>Costly Misconfigurations</td>
<td>Accelerated Investigations</td>
</tr>
<tr>
<td>$5T</td>
<td>Real-time Device Discovery including IoT</td>
</tr>
<tr>
<td>Costly Misconfigurations</td>
<td>Decryption TLS 1.3 @ Line Rate</td>
</tr>
<tr>
<td>Unacceptable Detection</td>
<td>Cloud-based ML and Behavioral Analytics</td>
</tr>
<tr>
<td>Lack of Collaboration</td>
<td>SOC/NOC Productivity</td>
</tr>
<tr>
<td>70%</td>
<td>Superior Threat Detection</td>
</tr>
<tr>
<td>of the attack surface is opaque and not covered by agents or logging</td>
<td>Automated Response &amp; Quarantining</td>
</tr>
<tr>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>estimated cost of cloud misconfigurations in 2018-2019</td>
<td></td>
</tr>
<tr>
<td>78 days</td>
<td></td>
</tr>
<tr>
<td>average threat dwell time in the enterprise</td>
<td></td>
</tr>
<tr>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>don’t share knowledge/resources</td>
<td></td>
</tr>
</tbody>
</table>

WHY NOW?

CLOSE THE EAST-WEST GAP WITH NDR

NO AGENTS ELIMINATE BLIND SPOTS
FASTER DETECTION INTEGRATE WITH EDR & SIEM

ECOSYSTEM: INTEGRATIONS & OPEN API

INGEST
ExtraHop Cloud
Cloud-Based Machine Learning

CORRELATE

How Reveal(X) Works

- 5000 Metrics
- 70+ Protocols
- SSL/TLS 1.3
- Real-time Streaming
- 3.3PB Daily Network Traffic
- Physical, Virtual, Cloud, Saas
- Certs, Ciphers
- Continuous Packet Capture

© 2020 ExtraHop Confidential: For partner use only - not for distribution
Nine times out of ten, we know about a problem before any of our users can tell us about it.

- CURO FINANCIAL

Can’t my tool do that?

- SIEM
  - Expensive at scale
  - Incomplete data, lacks context, often turned off if too noisy

- EDR
  - Not everywhere
  - Complex to manage
  - Requires deep expertise
  - Can be tampered with

- IDS/IPS & FORENSICS
  - Reveals consolidates IDS and forensics in a single workflow
  - Lacks N-S, E-W visibility & scalability
  - No ability to decrypt traffic

- IoT SECURITY/NAC
  - Lack of situational awareness
  - Can’t detect threats in context of the entire hybrid network

- OTHER NDR/NTA SOLUTIONS
  - Can’t cover NOC + SOC use case
  - Not built for scale
  - No decryption at line speed
  - No flexible deployment models
  - ML on box not in cloud

For more information contact: partners@extrahop.com
Partner Portal: https://partner.extrahop.com

© 2020 Extrahop Confidential: For partner use only - not for distribution