ExtraHop
Rise Above the Noise.

PARTNER BATTLE CARD

# 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?

### THE COST OF COMPLEXITY

**Lack of Visibility**

**70%**

of the attack surface is opaque and not covered by agents or logging

**Costly Misconfigurations**

**$5T**

estimated cost of cloud misconfigurations in 2018-2019

**Unacceptable Detection**

**78 days**

average threat dwell time in the enterprise

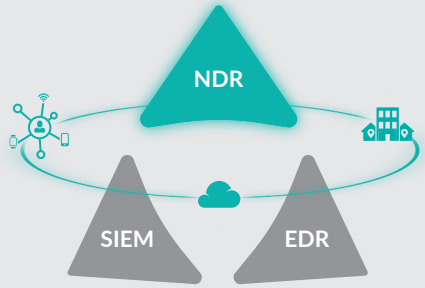
**Lack of Collaboration**

**70%**

don't share knowledge/resources

## WHY NOW?

### CLOSE THE EAST-WEST GAP WITH NDR




Network/wire data is the ground source of truth that can't be tampered with or evaded.

NO AGENTS
ELIMINATE BLIND SPOTS

FASTER DETECTION
INTEGRATE WITH EDR & SIEM

## WHY EXTRAHOP REVEAL(X)?

- 100Gbps Speed and Scale
- Accelerated Investigations
- Real-time Device Discovery including IoT
- Decryption TLS 1.3 @ Line Rate
- Cloud-based ML and Behavioral Analytics
- SOC/NOC Productivity
- Superior Threat Detection
- Automated Response & Quarantining

**COMPLETE VISIBILITY**

**95%** Improvement In Time to Detect

**REAL-TIME DETECTION**

**77%** Improvement In Time to Resolve

**INTELLIGENT RESPONSE**

**59%** Reduction in Staff Time to Resolve

CUSTOMER VALUE: IDC

## ECOSYSTEM: INTEGRATIONS & OPEN API

INGEST: aws, ANOMALI, GARLAND, Google Cloud, Azure, ixia, vmware, Gigamon, ALIEN VAULT

CORRELATE: splunk>, ArcSight, IBM QRadar, LogRhythm

RESPOND: CROWDSTRIKE, aws, Azure, paloalto, Check Point, cisco ISE (Fully Automated); Phantom, DEMISTO, servicenow, slack (Augmented Workflows)

## HOW REVEAL(X) WORKS


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

ExtraHop
Rise Above the Noise.

# PARTNER BATTLE CARD

> "Nine times out of ten, we know about a problem before any of our users can call to tell us about it."
>
> - CURO FINANCIAL

## PERSONA CONCERNS

### Head of Information Security
(CISO, CSO, VP)
Decision Maker/Budget Holder

- Cloud Security
- East-West visibility gaps (cloud & on-prem)
- MTTR
- NOC/SOC collaboration
- Risk from encrypted traffic

### SOC Analyst

- Faster detection and incident resolution
- Focus on high priority alerts
- Improve NetOps communication

### Incident Responder

- Increase speed to intelligence
- Eliminate threat recurrence
- Reduce dwell time

### Security/Cloud Architect

- Ensure hybrid cloud resilience
- Remove organizational silos
- Understand application dependencies

## INITIATIVES

- CLOUD SECURITY
- SOC/NOC OPTIMIZATION
- REMOTE USERS/ ACCESS
- TOOL CONSOLIDATION

## USE CASES

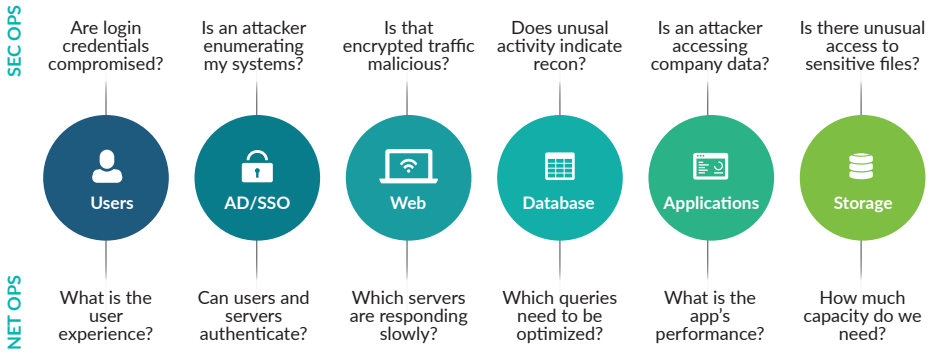
### VISIBILITY & HYGIENE
- Enterprise IoT
- Unauthorized/Unknown Devices
- Expired/Weak Certificates
- Insecure APIs
- VPN & AD Monitoring

### THREAT DETECTION
- Advanced Threats: APTs, Ransomware
- Behavioral Analytics (NBA/UBA)
- Proactive Threat Hunting
- Mapped to Attack Chain

### INCIDENT RESPONSE
- Forensics (Packet Capture)
- Threat Hunting
- Prioritize Threats Based on Risk Score

MITRE | ATT&CK™ NIST CIS Controls™

## QUESTIONS THAT REVEAL(X) ANSWERS




## Can't my "INSERT TOOL HERE" 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
- Reveal(x) 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 @ 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