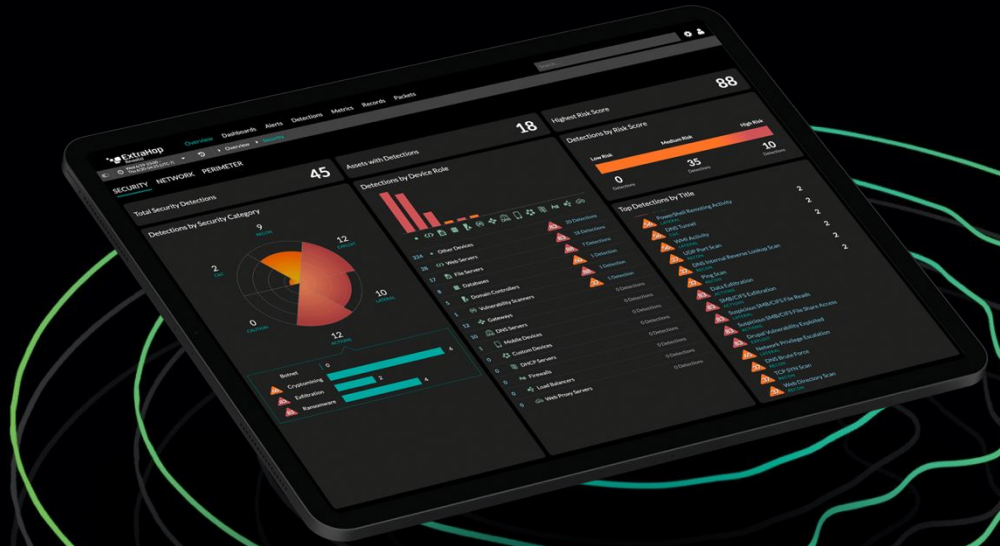
ExtraHop

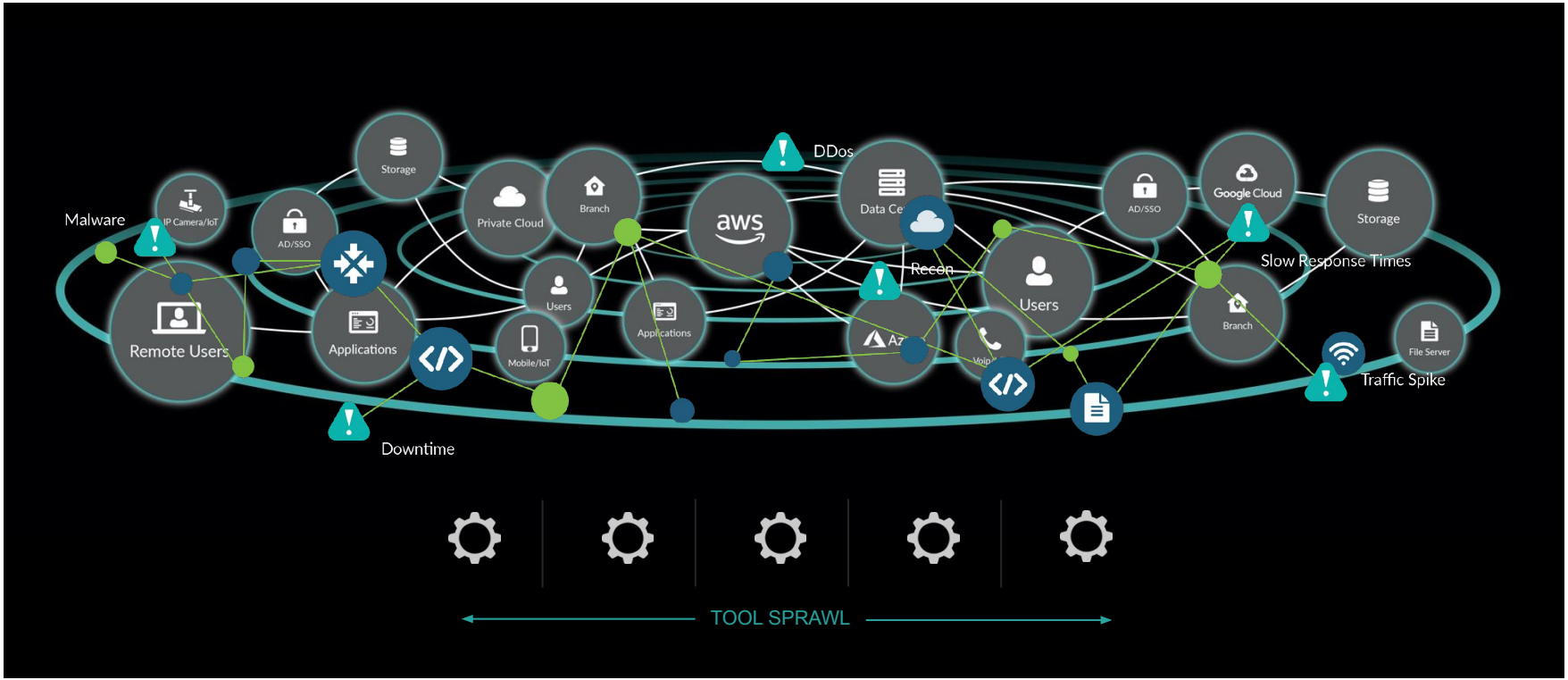
High-Speed Anomalie-Erkennung

mit Network Detection & Response (NDR)



Enterprise Complexity is the New Reality

Noise Doesn't Have To Be



ExtraHop

There is Real Cost to this 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

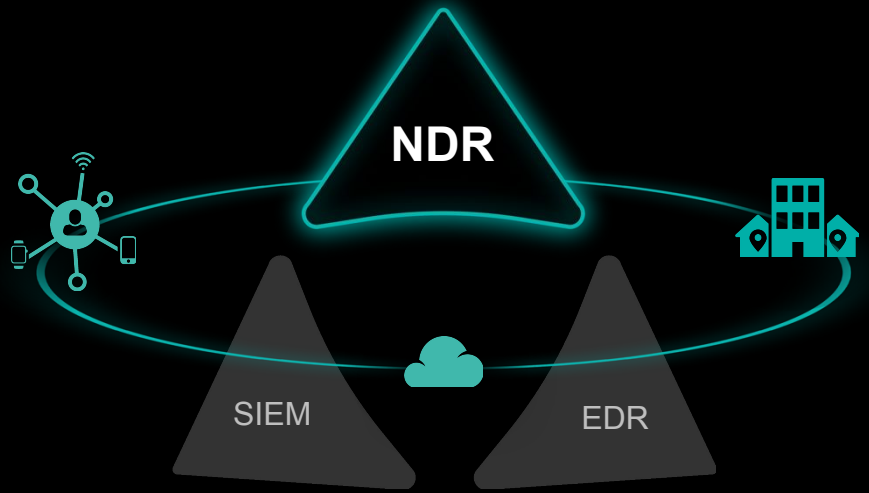
70%

don't share knowledge/resources

ExtraHop

NDR is the Signal in the Noise

Complete Visibility Across East-West and North-South



COMPLETE VISIBILITY

REAL-TIME DETECTION

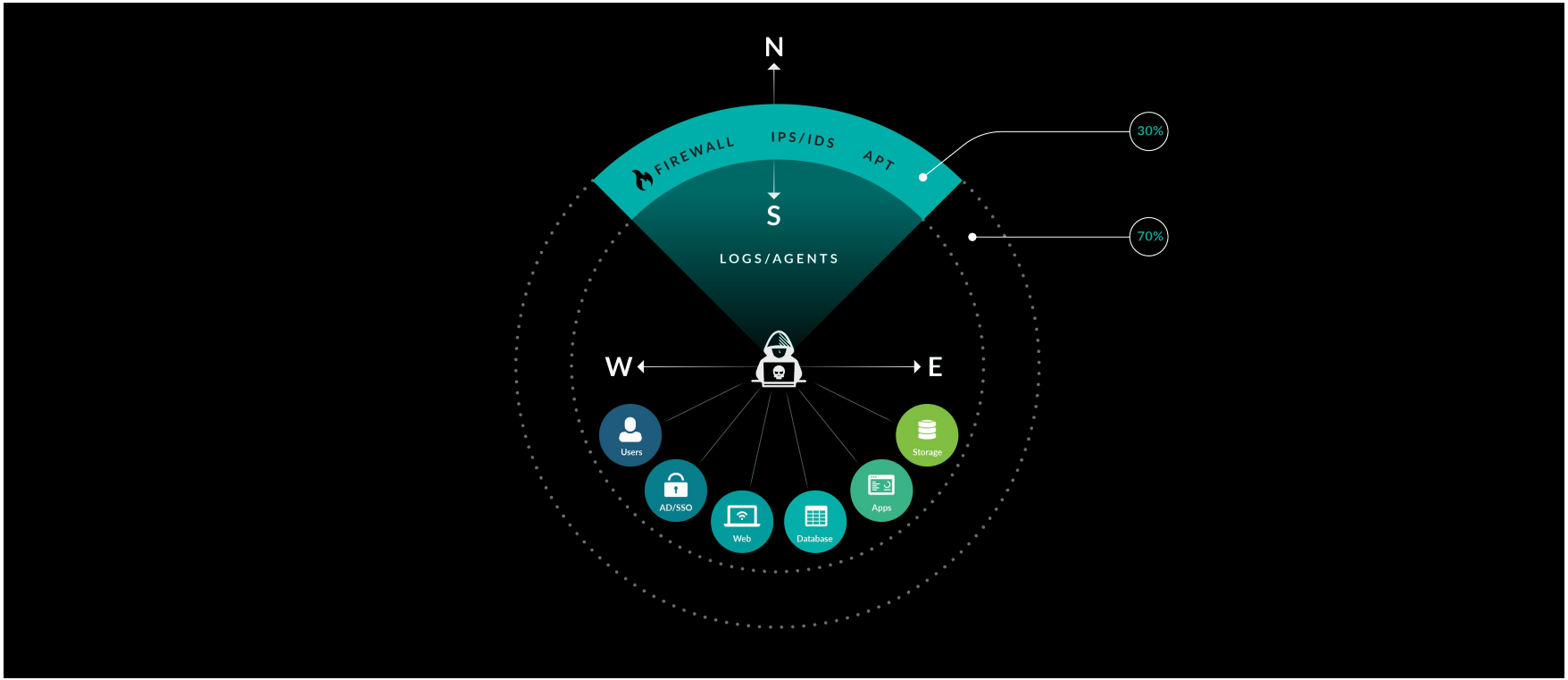
INTELLIGENT RESPONSE

> Network-based detection tools got the highest levels of satisfaction when compared against other detection approaches.
>
> 2019 SANS SOC SURVEY RESULTS

ExtraHop

Security in a Post-Compromise World

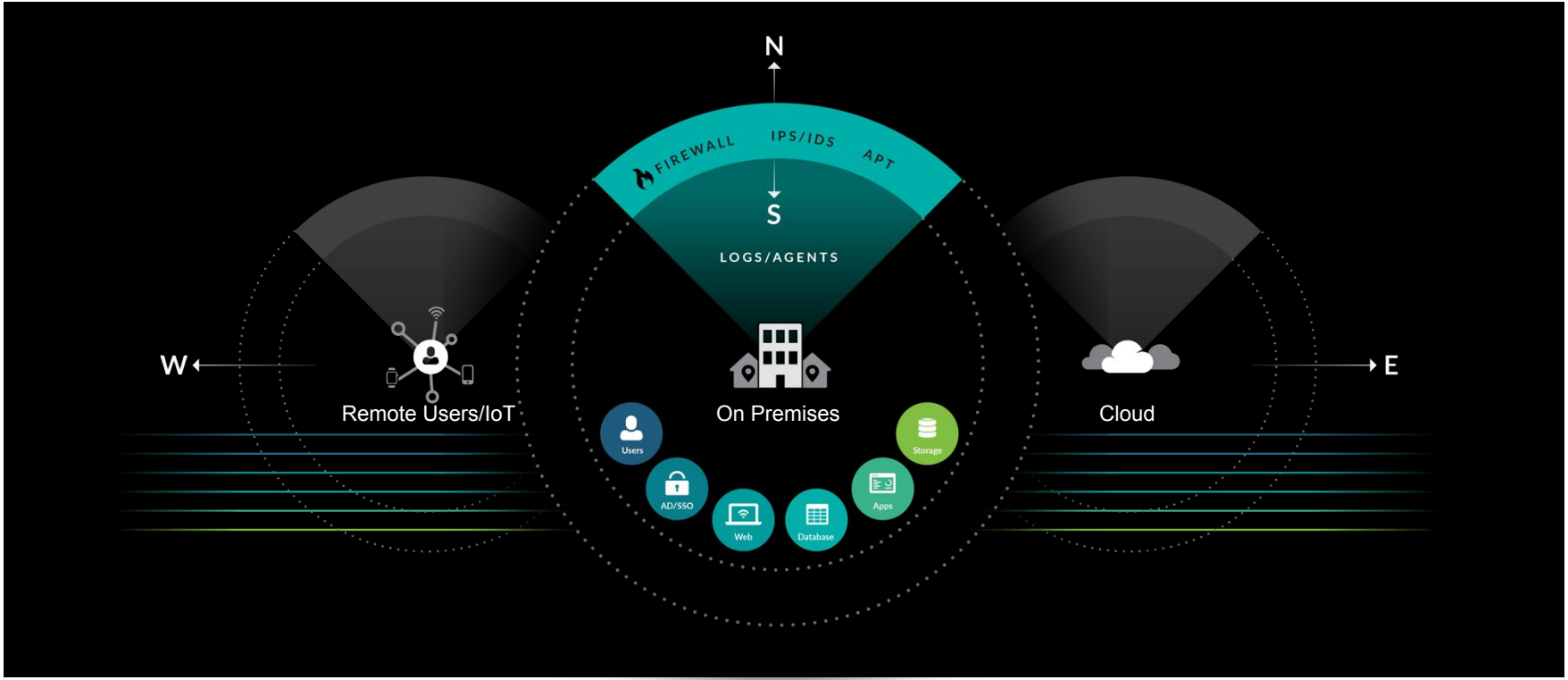
Covering the Four Corners of the Attack Surface: North, South, East, West



ExtraHop

Security in a Post-Compromise World

Covering the Four Corners of the Attack Surface: North, South, East, West



ExtraHop

But Can’t My

“ ”

Do That?

EDR
Not everywhere
Deep expertise
Management Complexity

SIEM
Expensive
Incomplete data
Lack of Context

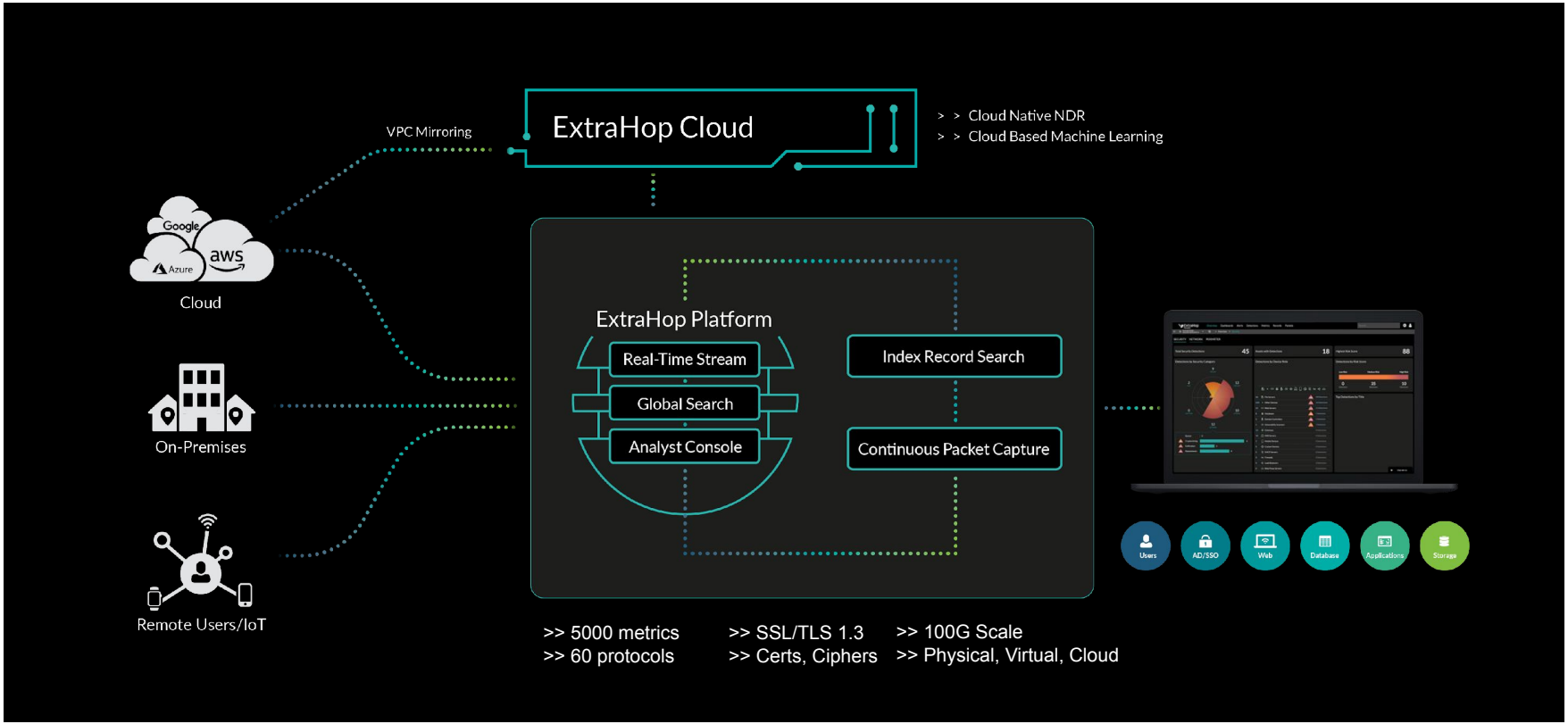
IDPS
Compliant ≠ Secure
False Pos & Neg
Limited Visibility

FORENSICS
Packet-First Approach
Scalability Issues
Limited Detection

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

ExtraHop

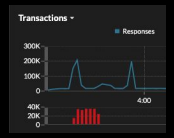
Cloud-Native NDR for the Hybrid Enterprise

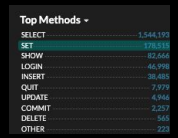


ExtraHop

ExtraHop: Depth of Data

Time-Series Metadata
Retention: Months and Years





1,558 Responses

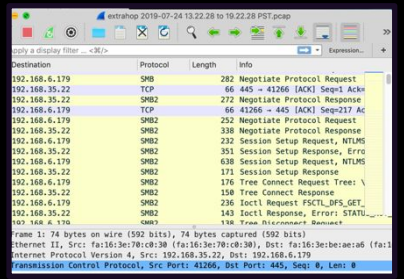
203 Errors

File
\\10.10.10.3\fileshare\accounts\pensions\2014\jan_2014.xls
\\10.10.10.3\fileshare\accounts\pensions\2015\jul_2015.xls
\\10.10.10.3\fileshare\accounts\pensions\2016\jan_2016.xls
\\10.10.10.3\fileshare\accounts\pensions\2016\jul_2016.xls

L7 Protocol	Bytes In	Bytes Out
DNS	108,694	154,526
DHCP	4,264	4,784
udp:161	440	670
RADIUS	96	0

IP	Bytes In ↓	Bytes Out
172.24.1.80	70,420	95,149
172.24.1.81	42,498	64,161
192.168.35.22	2,380	698

Raw Original Packets
Retention: Hours and Days



Transactional Metadata
Retention: Days and Weeks

Time ↓	Record Type	Client IPv4 Address	Server IP...	Server	Status Code	Method	URI
2019-09-10 07:24:59.994	HTTP	196.228.169.122	172.23.1.8	web1.londmz.exan	200	GET	demo.example.com:8080/ecomapp/actions/Catalog.action
2019-09-10 07:24:59.667	HTTP	205.79.181.188	172.22.1.9	VMware B84943	200	POST	orbital.example.com:443/AUTHORIZE
2019-09-10 07:24:59.581	HTTP	209.227.237.14	172.22.1.8	web1.nycdmz.exan	200	GET	demo.example.com:8080/ecomapp/actions/Cart.action
2019-09-10 07:24:59.491	HTTP	163.217.145.62	172.24.1.8	web1.syddmz.exan	200	GET	demo.example.com:8080/ecomapp/admin/

Less Granular

Very Granular

ExtraHop

ML and AI is hard

Chiuahua or Muffin?

Puppy or Bagel?

Labradoodle or Fried Chicken?

Parrot or Guacamole?

Sheepdog or Mop?

Sloth of Pain Au Chocolat?

ExtraHop

ExtraHop Full-Spectrum Detection

HYGIENE

Activity that represents risk: ports, protocols, cryptographic compliance, and vulnerable or non-compliant services.

KNOWN ATTACKS

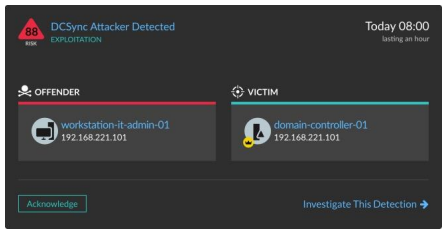
IP addresses, domains, file names, payload strings, or protocol behavior observed in past attacks (including intelligence feeds).

UNKNOWN ATTACKS

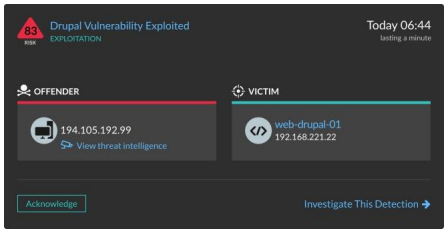
Attacks that do not have a previously known identifier, but exhibit anomalous behavior that can be linked to part of the attack lifecycle.

SPECTRUM OF DETECTION

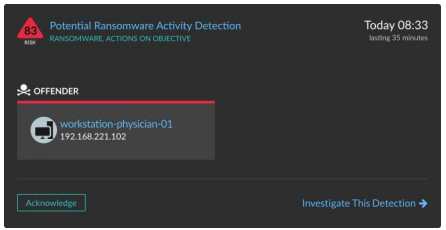
Rule-Based Detection



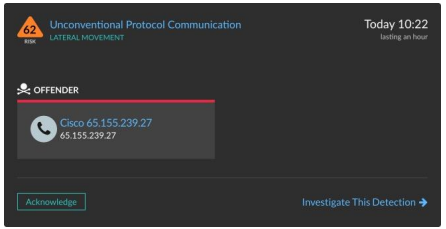
Robust Anomaly Detection



Sophisticated Behavioral Detection

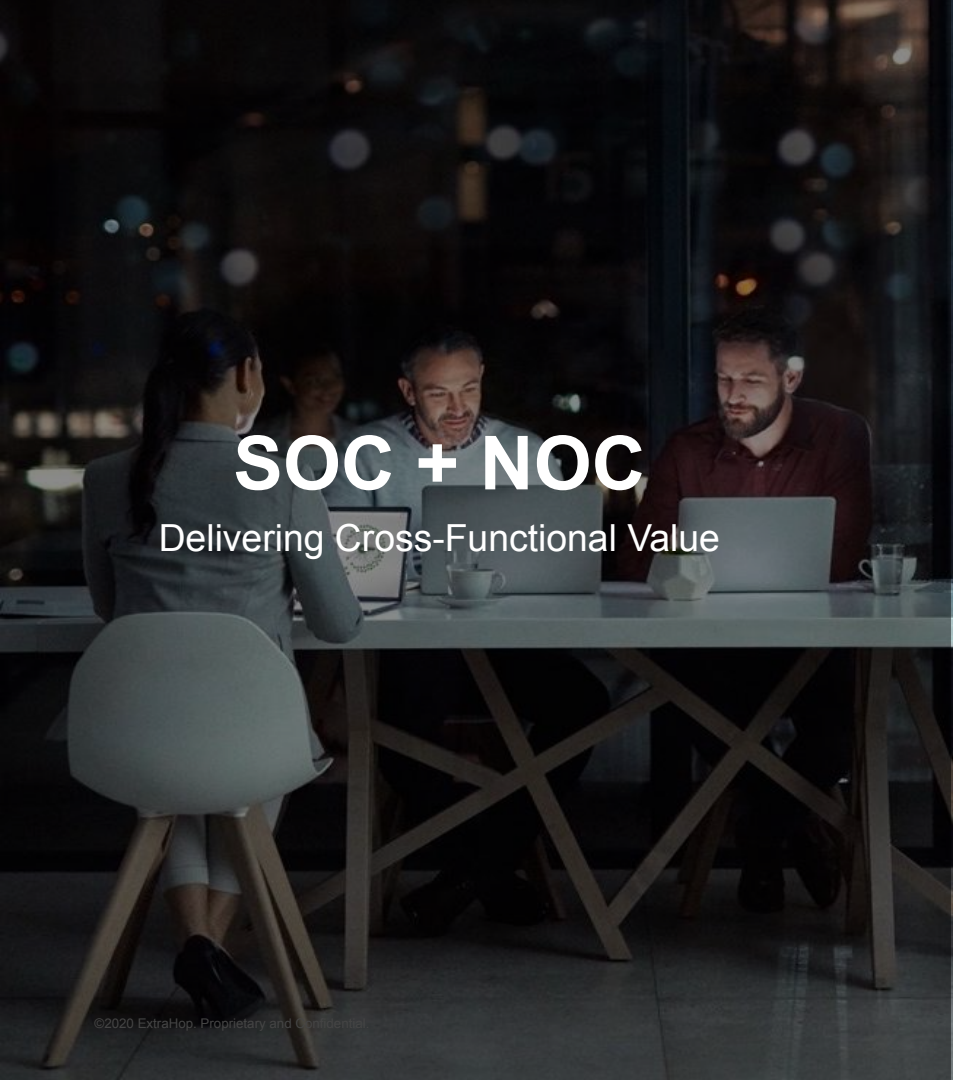


Peer Group Detections



MITRE ATT&CK™ NIST CIS Controls™

ExtraHop



SOC + NOC

Delivering Cross-Functional Value

Better Data, Better Security & IT Operations

Operational Value	Business Value
Visibility	Tool Consolidation
Detections Investigation	Talent
Hygiene	Data Storage
Mitigation	Productivity

ExtraHop

Arming Security and IT Ops Teams to Answer the Tough Questions

In Real time and in Context

SEC OPS

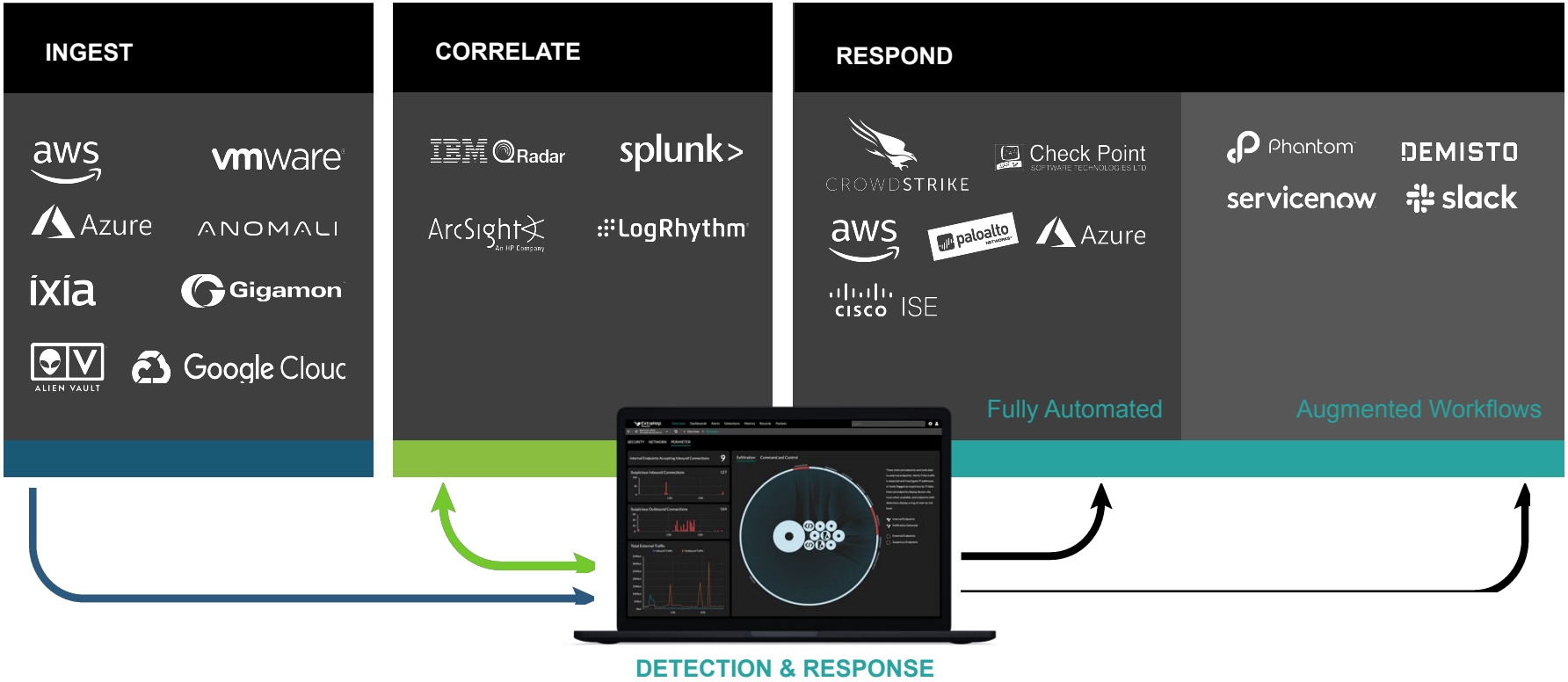
- Are login credentials compromised?
- Is an attacker enumerating my systems?
- Is that encrypted traffic malicious?
- Does unusual activity indicate recon?
- Is an attacker accessing company data?
- Is there unusual access to sensitive files?

IT OPS

- What is the user experience?
- Can users and servers authenticate?
- Which servers are responding slowly?
- Which queries need to be optimized?
- What is the app's performance?
- How much capacity do we need?

ExtraHop

Amplify the Power of Your Enterprise Tools



ExtraHop

Use Case: Visibility & Hygiene

Why Reveal(x)?

Cloud-native NDR provides faster time to value, eliminates blind spots, supports on-prem, hybrid and multi-cloud deployment scenarios

- Automated, continuous device discovery and identification
- Unmatched 100 Gbps of full payload analysis
- Line-rate decryption of SSL/TLS 1.3 encrypted traffic
- Complete, observed visibility of all E-W and N-S traffic
- Built in visibility for CIS controls 1 & 2, MITRE, NIST CSF
- Full spectrum detection and response for security and performance

Case Study

1 Tb

of unauthorized data exfiltration
(“Phoned Home” Security Advisory)

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

MITCH ROBERSON – CURO FINANCIAL

ExtraHop

Use Case: Incident Response

Why Reveal(x)?

Cloud-native NDR delivers best-in-class incident response with behavioral analysis, data correlation, and detection-record-packet workflows

- Faster forensic investigation with continuous packet capture capabilities
- High-level visualizations, intuitive drill-downs, global search (threat hunting)
- Multi-cloud innovations (AWS, GCP) to support forensics use cases
- Automatic investigation workflows, deep visibility into critical asset activity
- Native remediation capabilities, robust API and integrations with orchestration platforms

IDC

59%

Reduction in staff time to resolve

77%

Improvement in time to resolve

ExtraHop


ExtraHop