



INFINITY NDR

Network Detection and Response

YOU DESERVE THE BEST SECURITY

North/South vs. East/West

“A sort of crunchy shell around a soft, chewy center”

- *Bill Cheswick, 1990*



Don't know and don't care!

Gartner's Definition of NDR

Uses non-signature-based techniques to detect suspicious traffic on enterprise networks

Models normal network traffic and highlight suspicious traffic that falls outside the normal range

Monitors and analyzes north/south traffic, as well as east/west traffic (as it moves laterally throughout the network).

Provides automatic or manual response capabilities to react to the detection of suspicious network traffic



Definition source: Gartner
(Previous name: Network Traffic Analysis)

KuppingerCole Analysts NDR Leadership Compass

HOW NDR WORKS

Data in -> Intelligence out



OVERALL
LEADER

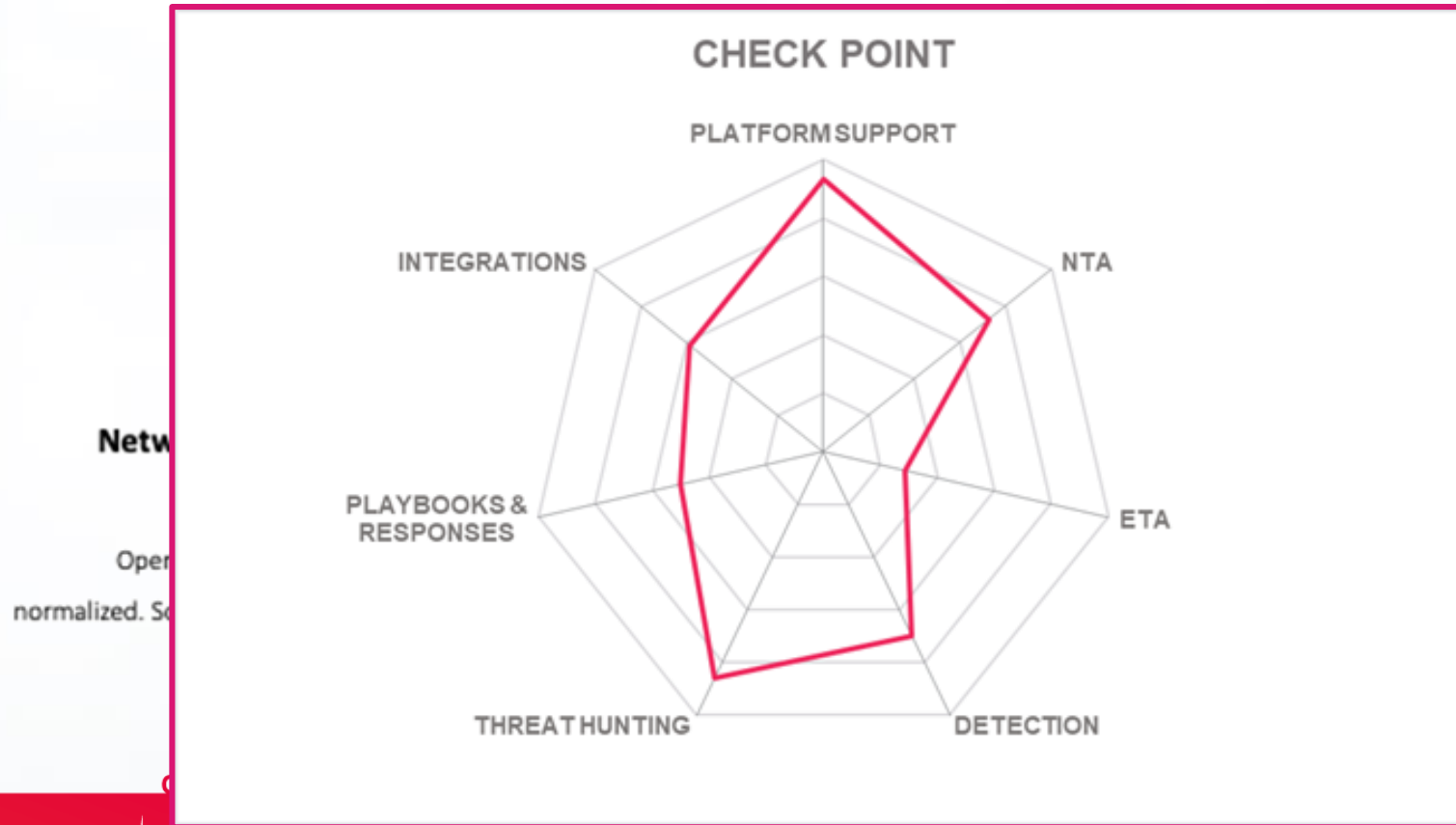


LEADERSHIP
COMPASS
2021

NETWORK
DETECTION &
RESPONSE

KUPPINGERCOLE ANALYSTS AG,
NOV 2021

KuppingerCole Analysts NDR Leadership Compass



Netw
Oper
normalized. Sc

suspicious
responses

NETWORK
DETECTION &
RESPONSE

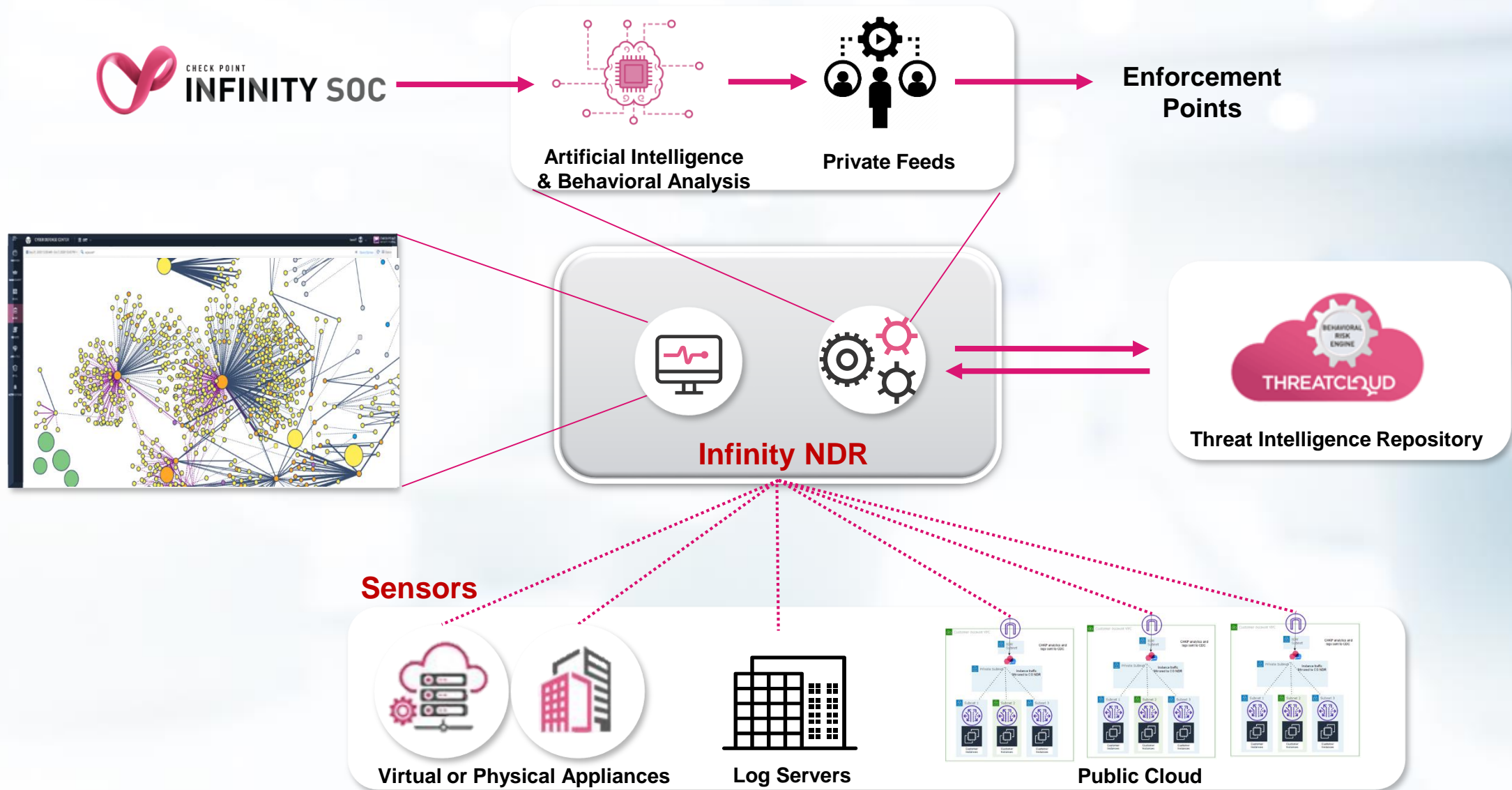
KUPPINGERCOLE ANALYSTS AG,
NOV 2021



LEADERSHIP
COMPASS
2021

ADER

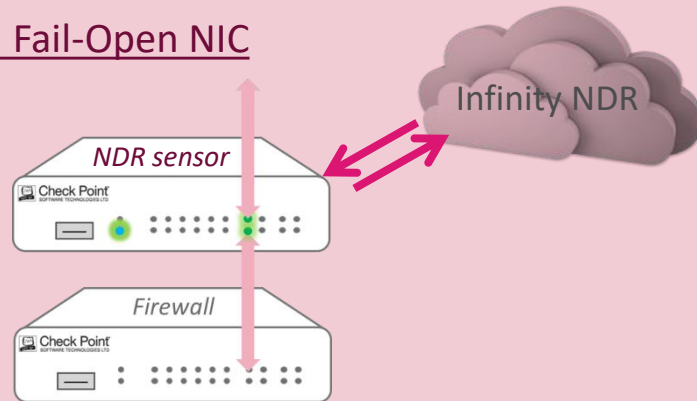
Infinity NDR High Level Architecture



Threat Prevention with Infinity NDR

In line deployment modes

In line Sensor with Fail-Open NIC

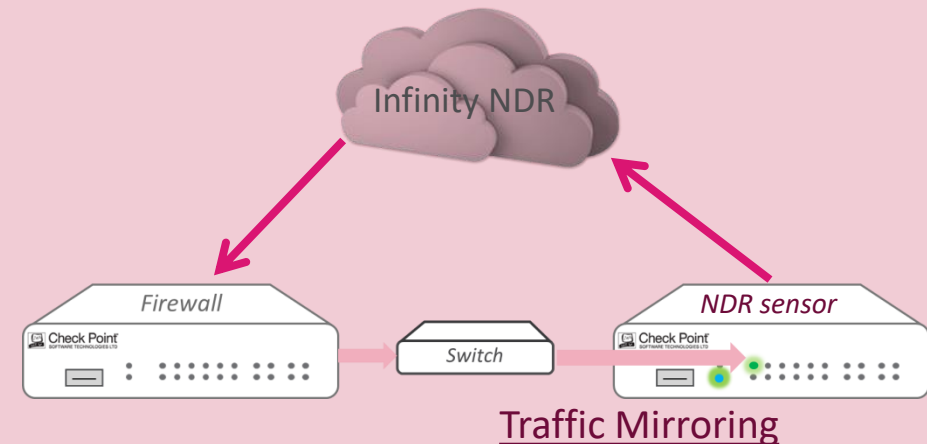


Prevent: Inline NDR sensor blocks attack traffic. Exceptions used to filter out false positives.

Detect: Blocks only identified attack patterns as directed by cyber analysts (exceptions or IOCs).

Bypass: Fail-Open NIC ensures no network disruption during upgrades and maintenance.

Passive inspection deployment modes

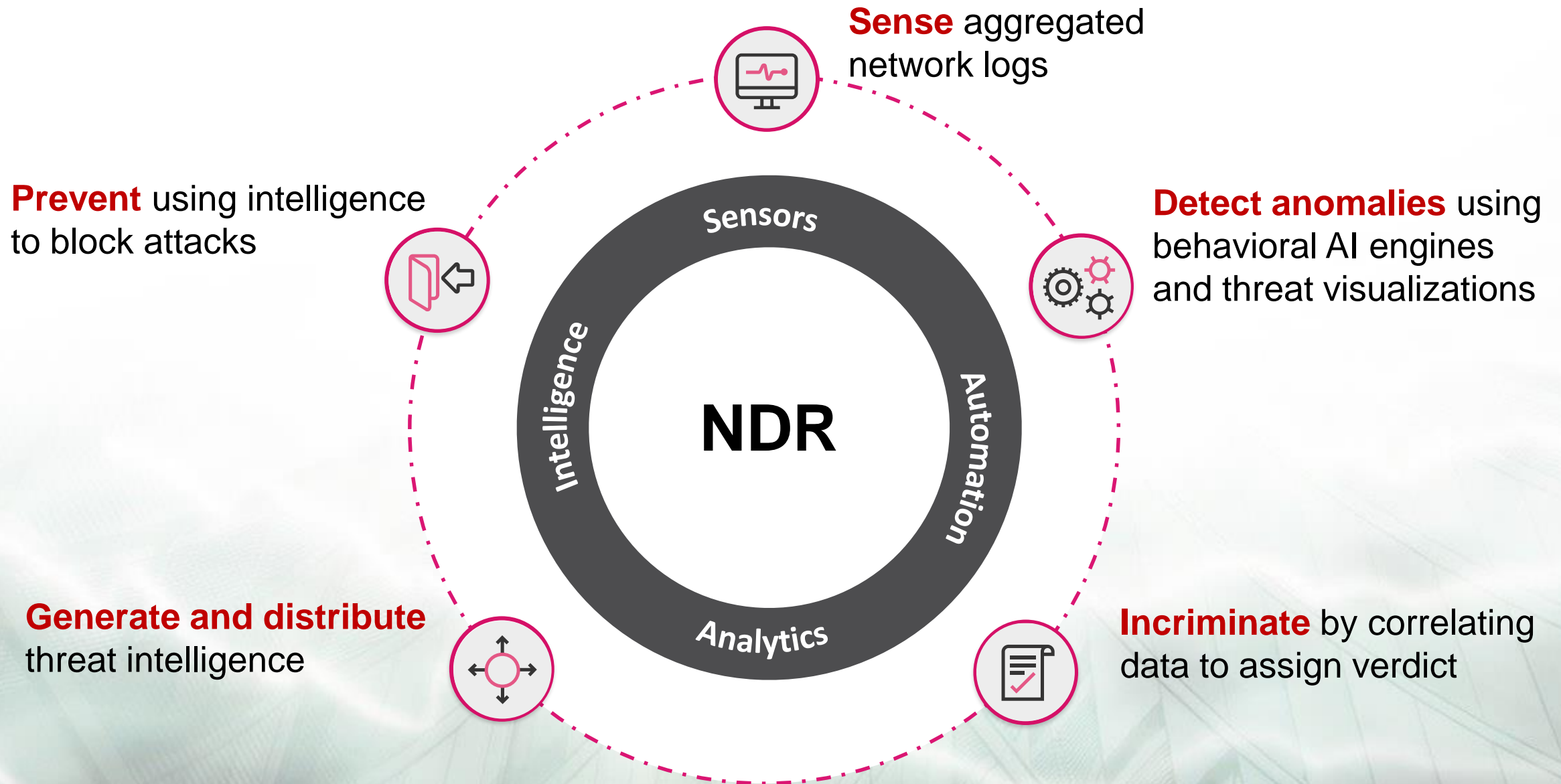


Detect: NDR used for threat hunting and protection development and testing w. zero impact to network.

Prevent: Attack signatures are published via NDR Intel feeds, driving main line prevention.

Bypass: Continued observability when bypass engaged. Now is “ready for action” via ‘bypass off’.

Infinity NDR Continuous Feedback Loop



Behavioral Analysis Engines

01

Recurrent Connections

Use time to find devices repeatedly connecting to a rare external destinations hosted on suspicious infrastructure

02

Geo Anomalies

Use out of ordinary connections to detect potential attacks

03

Protocol Anomalies

Find spikes in regular daily work to detect abnormal behavior, unsolicited network reconnaissance and lateral movement attempts

04

Vulnerability Sonar

(Patent pending)

Analyze the response given to external scanners and deduces which of the scans actually found a vulnerability, and to which servers

05

UEBA

Find anomalies in user behavior to detect escalation of privilege and credential compromise attempts

06

Infinity SOC Insights

Machine Learning-based alert prioritization for precise attack detection

PRECISION

FROM MILLIONS OF LOGS TO ONLY REAL ALERTS

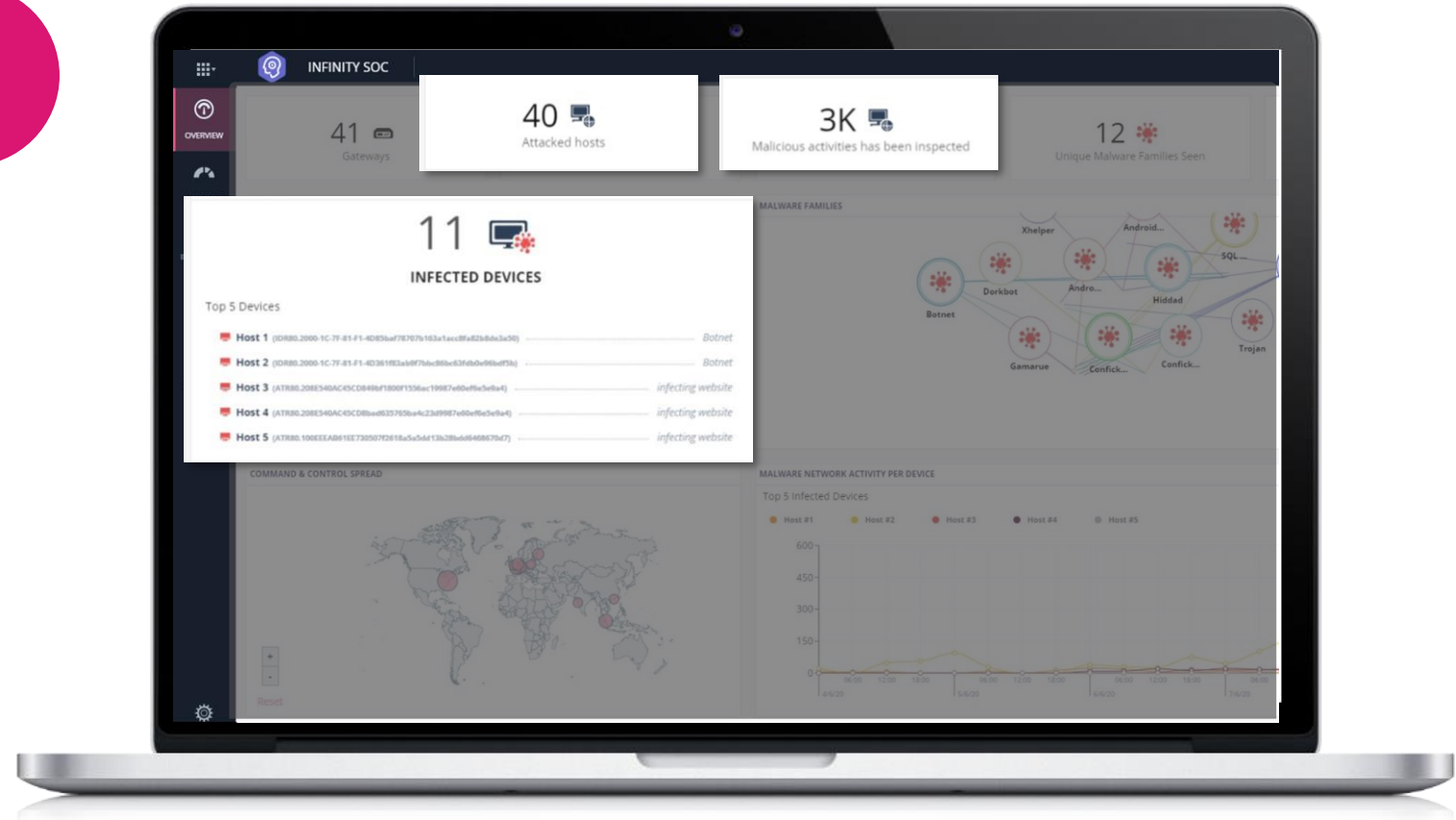
IN AN AVERAGE WEEK:

59,000,000
logs across endpoint, network,
cloud, mobile and IoT

3,000
Malicious activities

40
Targeted assets

11
Infected assets





PRIORITIZATION



RESPOND INTELLIGENTLY BASED ON SEVERITY AND PROBABILITY

AUTOMATED TRIAGE



99%
TRICKBOT MALWARE

99%  **Host #1** 6:58, 6/20/2020 
Host 1 might be infected with Trickbot (High probability)



99%
ADWARE

99%  **Host #2** 6:58, 6/20/2020 
Host 2 might be infected with Adware (High probability)

30%
EXTERNAL THREAT

30%  **Lookalike URL** 13:42, 6/8/2020 
Lookalike URL impersonating your website (Low probability)

10%
MOBILE THREAT

10%  **Mobile Device** 6:57, 6/8/2020 
Mobile Device might be infected with Trojan Horse (Low probability)



THANK YOU

Nir Naaman, CISSP | nir@checkpoint.com

Infinity NDR: <https://now.checkpoint.com>
<https://www.checkpoint.com/infinity-vision/infinity-ndr/>

YOU DESERVE THE BEST SECURITY