INFINITY NDR

CYBER DEFENSE PLATFORM
DEPLOY – HUNT – PREVENT

Product Benefits

- Web-based application for cyber situational awareness, threat hunting, and security operations automation
- SaaS/on-prem platform for MSSPs, IR teams, enterprise SOCs, and network auditors
- Incorporates industry-leading threat prevention powered by ML, DL, behavioral AI
- Powered by Check Point ThreatCloud big data threat intelligence and research platform, for immediate and accurate threat detection
- Identifies anomalous traffic, vulnerable and infected assets, lateral movement, suspicious user and application behavior
- Fully automated sensor deployment - on traditional networks and cloud fabrics, no impact on network traffic and business applications
- Complete SOC analyst workflow automation: from detection and investigation
- Real-time prevention via threat indicator ingestion, generation, and distribution
- Highest performance NDR with throughput options ranging up to 1.5Tbps

HOW DO YOU PROTECT AGAINST TOMORROW'S ATTACKS?

Threat actors keep finding new tactics to attack organizations and cover their tracks. Organizations need additional lines of defense inside their internal networks. In order to prevent attacks and to accelerate detection and remediation, Network Detection and Response (NDR) plays a central role in their security strategy.

Check Point Infinity NDR is a plug-and-play solution enabling you to discover, investigate and respond to attacks in a timely and intelligent manner. Utilizing real-time network visibility into your public, private cloud, and on-premises, advanced AI detection technologies, and the industry's most powerful threat intelligence, it addresses even the stealthiest attacks.

Infinity NDR extends the Check Point Infinity architecture to empower a new cyber defense paradigm. Infinity NDR tenets are DEPLOY – HUNT – PREVENT. Deploy NDR sensors – literally within minutes. Hunt combines AI analytics with advanced visualization techniques to allow cyber analysts to identify and investigate attacks that bypassed other defenses. Prevent automates the conversion of this insight into action, delivering threat indicators to Check Point and 3rd party enforcement points.

DEPLOY

Infinity NDR processes network logs other artifacts from firewalls, endpoints, mobile devices, and cloud fabrics in order to identify and incriminate anomalies.

In many cases, existing solutions are not suitable for this task: complete internal segmentation might not have been achieved; not all networked devices can run endpoint agents; or are simply lacking security capabilities or configuration. This is the SIEM data overload dilemma: excess of noise, insufficient information.

Therefore in addition to the ability to consume logs from existing devices, Infinity NDR automates deployment of NDR-managed Check Point Security Gateways in passive mode as network sensors. Sensors process both North/South and East/West network traffic, with no impact on business traffic.

Sensor deployment is quick and intuitive. There is no need for network security expertise because the sensors do not require any configuration or policy rules, nor a modification to network routing or topology. Physical appliances are attached either in Monitor Mode to process mirrored traffic, and/or inline Bridge Mode with fail-open NICs. Public cloud is supported via cloud-native mirroring APIs.

No reliance is placed on any existing investment in the Check Point Infinity Suite. This makes Infinity NDR effective alongside either Check Point or 3rd party security solutions. Enterprises and MSSPs can greatly reduce SOC TCO by leveraging Infinity NDR to deliver a complete, dedicated, unified, integrated, agile, fit for purpose NDR sensor architecture.

March, 2022

CHECK POINT
YOU DESERVE THE BEST SECURITY

DEPLOY

- Automated log collection from Check Point Log Servers
- Check Point Gateways can be repurposed as NDR sensors in passive/inline modes
- Cloud-native traffic mirroring on AWS, GCP
- Harmony Endpoint/Mobile

HUNT

- NDR Behavioral Analytics: AI engines identify, incriminate malicious network behavior, automatically generating IOCs
- Built-in SmartEvent for log visualization and searching, scheduled reporting
- Notifications: flexible filter language, email-based alerting
- Threat Topology, Activity Mapping: visualization of network traffic, data flow and anomalous behavior
- Vulnerability Sonar: passive detection of exposed assets
- Infinity SOC Insights: ML-based threat prioritization
- InfinitySOC Investigate: IOC research on ThreatCloud and open source intelligence
- SIEM/SOAR/MDR integration
- Selective Packet Capture

PREVENT

- Built-in threat intelligence IOC management platform
- Automated input feeds, APIs
- Manage IPs, domains, URLs, hashes, mail fields, Snort, etc.
- Automated delivery to Check Point and 3rd party devices

HUNT

The Infinity NDR Web application provides cyber defenders and SOC analysts with situation awareness and intervention capabilities. It incorporates, consolidates, and correlates event logs from physical and virtual sensors, combining on-premises, perimeter, and cloud network visibility into a single picture.

Application and threat visualization appears on Infinity NDR within minutes of sensor deployment. Infinity NDR harnesses the power of Check Point ThreatCloud threat intelligence and the industry's largest application fingerprinting and risk scoring library, in order to incriminate any identified anomalies. This combination of AI and intelligence delivers immediate insights into the traffic patterns, as well as reduces the false-positive noise level characteristic of pure-behavioral solutions.

Triage of anomalous network traffic involves a combination of automated analysis and human analysts, working together to ensure timely, accurate and relevant information is delivered for effective response to cyber-attacks. While automated controls excel at sifting through huge amounts of big data and detecting anomalous behavior, human intelligence is still superior when it comes to identifying patterns of unauthorized behavior, weeding out false positives, categorizing events by motive and intent and identifying effective and safe Courses of Action (COAs). This methodology allows identification of initial attack vectors, as well as subsequently subverted hosts and compromised data.

In particular, Infinity NDR is tightly integrated with Infinity SOC, which delivers ML-powered threat prioritization for in-context investigation on the Infinity NDR portal. Infinity SOC also provides IOC research capabilities, allowing SOC analysts to pivot on detected anomalies and determine reputation and previously-seen behavior.

Beyond threat-based defense, analysts can utilize powerful application and URL fingerprinting to provide a deep understanding of business flows and anomalous behavior across Web browsing, business apps, end even SCADA and IOT. Identity Awareness can be layered in for complete User and Endpoint Behavioral Analysis.

PREVENT

The ultimate objective of NDR is incident detection, response and recovery. This requires prevention throughout the threat kill chain, both pre- and post-infection. A threat indicator or IOC (Indicator of Compromise) is a statement that signs network traffic that should be blocked.

Infinity NDR's Intel facility enables the automation of large-scale managed repositories of threat indicators. Supported indicator types include IP and URL reputation; file and application hashes (MD5 and SHA); mail fields, Snort and Yara signatures, and more.

Indicators can be fed into Infinity NDR using a variety of industry-standard formats and protocols including STIX/TAXII, CSV, and REST APIs. They are also autonomously generated by Infinity NDR's Behavioral Analytics AI engines.

Finally, in order to close the loop from detection to prevention, indicators are automatically distributed to Check Point and 3rd party gateways and endpoint agents.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2117 | Fax: 650-654-4233 | www.checkpoint.com