

30 May 2023

# *Horizon NDR*

## *Deployment Guide*

---

Dedicated NDR Sensors, Log Server Registration,  
and Security Checkups

---

Classification: [Protected]



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

© 2023 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

**RESTRICTED RIGHTS LEGEND:**

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

**TRADEMARKS:**

Refer to the Copyright page <http://www.checkpoint.com/copyright.html> for a list of our trademarks.

Refer to the Third Party copyright notices [http://www.checkpoint.com/3rd\\_party\\_copyright.html](http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

# Introduction

Check Point Horizon NDR is a comprehensive technology stack for Network Detection and Response. It consists of a back-end service front-ended by a Web application, hosted at <https://now.checkpoint.com>; and network sensors deployed on premises or in the cloud.

The Check Point Horizon NDR operational concept is composed of the following flows:

- **Sensors analyze network traffic, and generate analytical results in the form of logs**
- **Logs are transmitted to the NDR cloud for storage and analysis**
- Behavioral Analytics AI engines process the logs and create analytical conclusions
- Human analysts use event visualization tools for data comprehension
- Data anomalies are incriminated through correlation with ThreatCloud intelligence and application risk scoring
- Analytical conclusions are published in the form of threat indicators and tags
- Input feeds pull threat indicators from third party threat intelligence sources
- **Enforcement points apply the indicators and match them to network traffic, for Detect or Prevent**

This guide focuses on the deployment of sensors for the Horizon NDR application. You can achieve network visibility within minutes, with easy, intuitive deployment and minimal configuration effort, and with no impact on business traffic. No other Check Point products are required for Horizon NDR to work.

## Table of Contents

<b>Horizon NDR</b> .....	<b>1</b>
<b>Horizon NDR Registration</b> .....	<b>5</b>
Registering a Customer Domain .....	5
Access to Horizon NDR Portal .....	5
Forcing Chrome Browser Refresh .....	6
<b>Horizon NDR Sensors</b> .....	<b>6</b>
Overview .....	6
Check Point Quantum NDR Sensors .....	6
Check Point CloudGuard NDR Sensors .....	7
Log Server Registration .....	7
<b>Preparing a Horizon NDR Sensor</b> .....	<b>8</b>
Overview .....	8
Installing Check Point R81.10 or R81.20.....	8
Determining Configuration Settings.....	8
Horizon NDR Sensors for VMware ESX Considerations.....	9
Required Access to the Horizon NDR Application Portal.....	10
Network Interfaces for Traffic Inspection .....	10
Lights Out Management (LOM).....	11
Defining the Sensor on the Horizon NDR Application Portal.....	12
Registering the Appliance .....	13
Accessing the Sensor's Gaia Portal .....	13
Plans.....	14

<b>Moving from Detect to Prevent .....</b>	<b>15</b>
Overview .....	15
Prevention with Inline NDR Sensors .....	15
Determining what would be Blocked in Prevent Mode .....	16
Exceptions .....	16
Threat Prevention using Threat Indicators .....	17
Configuring Check Point Security Gateways to Pull NDR Indicators.....	18
<b>Horizon NDR Log Server Registration .....</b>	<b>19</b>
Overview .....	19
Prerequisites.....	19
Defining the Sensor on the Horizon NDR Application Portal.....	20
Registering the Log Server .....	21
<b>Check Point Horizon NDR for AWS .....</b>	<b>22</b>
Overview .....	22
Terminology.....	22
Scoping and Costs .....	22
Resources Required on the AWS Account.....	23
Launch in AWS .....	24
Horizon NDR CloudFormation Template .....	24
Mirroring Additional VPCs.....	27
Traffic Mirroring Include/Exclude Lists .....	28
Sensor Deactivation on Stack Deletion.....	29
<b>Users and Access Control .....</b>	<b>30</b>
Domains.....	30
Authorizations.....	30
Users .....	30
Roles.....	30
Monitored Domains.....	31
Establishing a Monitoring Relationship between two Domains.....	31
<b>NDR Security Checkup Report.....</b>	<b>33</b>
Overview .....	33
Generating an NDR Report.....	33
Generating a Threat Topology Report .....	34
<b>Appendix A – SPAN Port Configuration .....</b>	<b>35</b>
HP/Aruba Switches .....	35
Cisco Switches.....	35
Juniper Switches.....	35
<b>Appendix B – Binding w. Horizon XDR/XPR .....</b>	<b>36</b>
Creating a Horizon XDR/XPR API Key .....	36
Importing the Horizon XDR/XPR API Key into Horizon NDR.....	37
<b>Appendix C – Known Limitations.....</b>	<b>38</b>

# Horizon NDR Registration

## Registering a Customer Domain

To access the Horizon NDR application, log in to [now.checkpoint.com](https://now.checkpoint.com).



**Note** - This is not part of the Infinity Portal. Horizon NDR maintains its own user and access authorizations repository.

Horizon NDR tenants are identified as 'domains'. Each domain defines a set of objects with:

- User authorizations for accessing the domain
- Sensors that send logs and packet captures to the application
- Reports, views, and insights
- Intel indicators (IOCs)

To create a domain, submit a request via <https://register.now.checkpoint.com/register>. The Company Name you enter will become the new domain name.

We recommend to subscribe to product news, as this allows Check Point to send you notifications for maintenance alerts and security events. Once the request is approved, you will receive a confirmation email with a link to create your new Horizon NDR domain.

## Access to Horizon NDR Portal

If this is your first domain on the portal, you will first be required to register user credentials for your new user account. This process installs a certificate in your browser, and is used to identify and authenticate you to Horizon NDR the next time you log in.

You generate the certificate on the portal, download it to your endpoint, and import it into your browser:

- a. Enter a password at the prompt. This password is used to encrypt your certificate when stored on disk. Enter the same password two times, and remember it for the next step.
- b. Click **Download** to download the certificate to your endpoint.



**Note** - We recommend **not** to double-click the certificate object after you download it. This causes the operating system's certificate import wizard to launch. Some browsers do not recognize the wizard, and you must reboot the endpoint.

- c. In your browser, open **Settings**, go to **Security > Management Certificates**, and click **Import**. Browse for the certificate on your disk and select it.



**Note** - In the browse window you may need to change the file type to "Personal Information Exchange" or to "All files" to see your new downloaded certificate.

- d. Load the certificate into the Personal certificate store (usually the default).
- e. Complete the import procedure.
- f. Go to the Horizon NDR portal <https://now.checkpoint.com> and click **Sign In**.
- g. At the prompt select your certificate to access the portal.

- h. Select the new domain you created from the pull-down menu.

## Forcing Chrome Browser Refresh

If after importing your new certificate into your browser you are not prompted for the certificate when trying to sign in, you might need to restart your browser in order to load the certificate into its Personal certificate store. The following procedure was tested to force Chrome browser on Windows to stop and refresh. Please make sure to save your work, use the history settings to relaunch all tabs.

- a. Close all Chrome open instances
- b. Use the "Windows Key" to search for **PowerShell**. Right click on the PowerShell and select **Run as administrator**.
- c. To force-stop all Chrome-related processes and to active the certificate, run this command:

```
get -process -name Chrome | stop -process
```

# Horizon NDR Sensors

## Overview

Horizon NDR ingests network artifacts in the form of log records. Each record contains log fields that are extracted by a network sensor from the network traffic, including source and destination IP addresses, ports, amount of data transferred, URLs, application categorization, risk categorization, user identity, etc. In order to close the NDR Loop, threat indicators are delivered back to the sensor by the Horizon NDR Intel facility.

Supported sensor types include Check Point Security Gateways (Quantum, CloudGuard, and Quantum Spark), and Check Point Harmony Endpoint. Threat indicators can also be delivered to 3<sup>rd</sup> party devices.

Sensors can be NDR-Managed, in which case they are managed from a Management Server hosted by the Horizon NDR application. This means that you do not need to install a Management Server; nor SmartEvent; nor SmartConsole; nor provision policy. A non NDR-Managed sensor sends its logs to a Management Server or Log Server; Check Point Log Exporter is used to forward the logs to Horizon NDR for processing. In the non NDR-Managed case, the sensor must also be configured separately to subscribe to Horizon NDR Intel feeds.

## Check Point Quantum NDR Sensors

You can easily convert any Check Point Quantum Security Gateway appliance into an NDR-Managed Horizon NDR sensor. The appliance's control layer is then slaved to the Horizon NDR application, and all control layer communications, including policy, logs, ThreatCloud queries, NTP, DNS, etc. are tunneled over a mutually-authenticated SSL VPN tunnel to the Horizon NDR cloud. Traffic inspection is normally achieved via Monitor Mode interfaces attached to switch mirror ports. Inline deployment (Bridge Mode) is also supported – with fail-open network interfaces.



In NDR mode, the appliance applies Check Point's real-time advanced SNBT threat detection engines on the mirrored network traffic, including: IDS/IPS, Application fingerprinting, Anti-Virus and Anti-Bot, and Threat Emulation (evasion-resistant sandboxing). Analytical conclusions are transmitted as log records to the Horizon NDR back end for further analysis.

## Check Point CloudGuard NDR Sensors

The same NDR mode conversion process that is used for Quantum NDR sensors can also be applied on CloudGuard and Open Server Gaia installations. There are some differences in interface naming and licensing but the underlying SNBT functionality is the same on these sensors. However, virtualization impacts data layer attachment. In particular:

- Fail-open interfaces are unavailable – therefore inline deployment is not supported, only Monitor Mode
- CloudGuard for VMware ESX deployments operate similarly to physical appliances, via mirroring
- CloudGuard for AWS is provisioned automatically from the Horizon NDR application, using AWS Lambda serverless computing to manage cloud-native traffic mirroring APIs. The CloudGuard Network Security instance is deployed out of band for its Compute capabilities, with no impact to business traffic
- CloudGuard for GCP operates similarly to AWS, however mirroring is currently manually provisioned
- Alternatively for all environments, a CloudGuard Network Security instance can be deployed and converted into NDR mode; and traffic mirroring provisioned on a separate device (e.g. Check Point CloudGuard Network Security configured with a Mirror and Decrypt policy) over VXLAN

## Log Server Registration

If you have a Check Point Management Server or Log Server that is collecting logs from Check Point Security Gateways and/or Check Point Harmony Endpoint, you can easily enable log export to Horizon NDR for NDR visualizations and analytics. The server is considered non NDR-Managed.

# Preparing a Horizon NDR Sensor

## Overview

This section describes how to convert a Check Point Quantum Security Gateway appliance into an NDR-Managed Horizon NDR sensor. You can use the same process for a CloudGuard or Open Server-based Horizon NDR sensor.

Supported versions:

- R81.10 – Recommended.
- R81.20 – Supported, recommended for customers that require R81.20 capabilities.

Contact the NDR team ([ndr@checkpoint.com](mailto:ndr@checkpoint.com)) if you are installing R81.20 to enable your NDR domain for this version.

- Maestro hyperscale orchestrated deployments require hotfix installation on top of R81.20 – contact the NDR team for more details.

## Installing Check Point R81.10 or R81.20

Clean-install Check Point R81.10 or R81.20 on the appliance as a Quantum (or CloudGuard) Security Gateway, applying the latest Jumbo Hotfix Accumulator for the installed version. See [sk170416](#) or [sk173903](#) for detailed installation instructions for R81.10 or R81.20, respectively.

The Security Gateway is automatically converted to NDR mode when the steps detailed in *Registering the Appliance* complete successfully.



**Note** - You do not need to install a Security Management Server as Horizon NDR handles this function. Installing the gateway as a Standalone (with Management) is not supported.

## Determining Configuration Settings

It is recommended to prepare the appliance ahead of time in a staging network before deployment to the customer's operational environment.

If DHCP is used in both locations, configure DHCP on the Mgmt interface, and networking parameters will be automatically provisioned.

If you do not use DHCP in the target environment, use two different network interfaces for connectivity from the appliance to the Horizon NDR application:

- Target environment: Mgmt interface (eth0 on virtual instances) with static IP address and default gateway.
- Staging network: choose another connectivity interface that will not be used for network monitoring and enable it for DHCP. For example, on an appliance that has onboard interfaces, you can use eth8.

This information is required for the target network environment:



- a. The Mgmt interface IP address; default gateway IP address; and proxy IP and port if required.
- b. Which interface(s) on the appliance will be used as Monitor Mode interfaces.



**Note** – Monitor Mode interfaces are used to connect the appliance to network switch SPAN (mirroring) ports. The default is to enable both eth1 and eth2-01 as the Monitor Mode interfaces. This default can be altered during appliance registration. Customers can also subsequently configure this from the appliance’s Gaia Portal, accessible from the Horizon NDR application.

Eth1 refers to the first onboard 1Gbps copper network interface, available on some appliances. Eth2-01 refers to the first interface on the extension card in bay 2, if available on the appliance.

When you install the gateway:

- Complete the First Time Wizard (FTW), and make sure you can connect to the Internet:
  - Networking configuration on the staging network is complete.
  - You’ve configured a DNS server IP (if not using DHCP) for initial domain name resolution.
- Enter any arbitrary value for SIC activation key – this value will not be used but must be entered.
- License – The appliance starts off after a clean installation with a 14 day evaluation license. When you purchase the license, the Quantum appliance automatically pulls it from the User Center. You can also install an evaluation license, or for a CloudGuard installation, a BYOL license.
- Configure the Mgmt interface IP address and default gateway as required for the target network environment. Leave this interface disconnected while in the staging network.
- If the target environment requires proxy configuration, this must be the last configuration step, as after defining the proxy, the appliance will lose its Internet connectivity while in the staging network.

After you complete the registration sequence, make sure to leave the appliance connected to the portal for about 15 minutes for engine updates to complete downloading.



**Note** - When the registration process successfully completes, you cannot connect to the appliance remotely using SSH or WebUI. This is because the Horizon NDR sensor’s control plane is tunneled over SSL VPN to the Horizon NDR portal and can only be managed from the Horizon NDR application. In addition, the admin password is automatically randomized.

See below, *Accessing the Sensor’s Gaia Portal*, for post-registration maintenance.

## Horizon NDR Sensors for VMware ESX Considerations

Installation on VMware ESX follows the same process as for a physical appliances, with the following caveats:

- At least 100GB disk space should be allocated for the sensor VM

- Allocate at least 2GB RAM per each processing core, with a minimum of 8GB RAM altogether

Refer to [VMware networking documentation](#) for instructions on configuring port mirroring on VMware virtual switches. Capture port groups must have Promiscuous Mode set to Accept when using either VMware VSS or VDS virtual switches.

## Required Access to the Horizon NDR Application Portal

Coordinate with the customer the following access rule authorizations:

- If there is a firewall on the path to the Internet, it must allow TCP port 443 connectivity from the appliance's Mgmt interface to IP addresses 35.156.213.136, as well as to 18.196.115.85 (portal.now.checkpoint.com), and 35.157.19.226 (feeds.now.checkpoint.com).
- The NDR sensor authenticates to the Horizon NDR application portal using mutually-authenticated TLS; therefore if the customer is using HTTPS Inspection on the outbound path, you must request an exemption for the Horizon NDR appliance's management traffic.
- An HTTPS Inspection exemption will also be required for user access to the Horizon NDR application portal at <https://now.checkpoint.com>.

## Network Interfaces for Traffic Inspection

### *Monitor Mode*

In most cases, you will be deploying the Horizon NDR sensor appliance passively, connected to one or more customer network switch's mirroring (SPAN) ports. Identify which interfaces on the appliance will be used for this purpose, ensuring that they match the customer's networking connections (i.e. fiber or copper) and speeds.



**Note** – The effective bandwidth for a monitor-mode port is normally less than the port specification. This is because the switch will mirror bi-directional traffic onto a single appliance interface. For example, a 1Gbps interface on the appliance would only be able to handle a maximum of 0.5 Gbps full-duplex traffic. More than that would overwhelm the link and result in packet loss on the switch.

### *Inline Bridge Mode*

In some cases customers find challenges with provisioning SPAN<sup>1</sup> ports. An alternative connectivity option is inline bridge (bump in the wire). This is an easy-to-provision configuration, however it does not provide the East/West visibility that monitor-mode can. Its primary advantages are the ability to deliver on-box prevention, as well as inline HTTPS Inspection and Threat Extraction. Inline bridge deployment with Horizon NDR sensors is supported only when using a Check Point Quantum Security Gateway fitted with a fail-open network interface.

<sup>1</sup> See Appendix A for command sequences used on common network switches.

When a fail-open NIC is fitted, it should be installed in the appliance's bay 1. A two port fiber fail-open NIC is automatically provisioned with a single two-interface bridge. A four port copper fail-open NIC provides two bridges. The odd-numbered interfaces on the card (eth1-01, and if available, eth1-03) are to be connected to the internal networking device, and the even-numbered interfaces to the external device. The bypass mode can be toggled from the Horizon NDR application portal's Sensors tab, via Actions > BYPASS.



**Notes** – A common mistake is to connect the fail-open interface to a switch mirror (SPAN) port, instead of using it as a bridge. This can result in high CPU consumption and sensor instability.

Another problematic configuration is **management-over-bridge**: the appliance's Mgmt interface is connected to an internal network, and the management traffic to the Horizon NDR portal is passed back through the appliance's bridge. This configuration is supported, but results in the appliance disconnecting from Horizon NDR every time the fail-open NIC bypass mode is toggled. It is therefore recommended to connect Mgmt to a network segment on the external side of the Horizon NDR sensor.

### *Packet Duplication due to Overlapping Traffic*

When processing traffic from multiple interfaces, it is important to prevent a situation whereby the appliance sees the same packet twice from multiple interfaces, as this can result in sensor instability. This scenario can occur if multiple interfaces are seeing network segments that pass packets between them, without intervening NAT.

In contrast, a valid deployment is to mirror a DMZ, and an internal network segment. Or, for the appliance to bridge between the firewall and the ISP router; and to monitor a SPAN port off a core switch. While each packet might indeed be seen twice by the appliance, egress hide-NAT on the firewall means that the two packets' source IP addresses and ports are different.

### *Combined Inline/Monitor Mode*

The best practice configuration combines both inline (for prevention) and monitor-mode (for East-West) attachments. Because of the packet duplication limitation, the inline attachment should normally be external to the NAT. The real internal source IPs are seen on the monitor-mode interfaces, and thus can support Identity Awareness. Alternatively, multiple sensors can be used to address this limitation.

Some network switches support a SPAN with ACL configuration, whereby the switch is provided a set of rules for network traffic that should be mirrored from ingress ports to egress port. This can be used to exempt mirroring of traffic that would be already visible to the NDR appliance from other interfaces. For example, if the NDR appliance is deployed inline inside the NAT for inspecting North/South traffic, configure switch mirroring so it does not include traffic between internal and external addresses.

### *Lights Out Management (LOM)*

In some rare situations, a Horizon NDR sensor might lose its control connection to the cloud, and therefore can no longer be accessed from the Horizon NDR application. In these cases, a LOM module can be used to remotely reboot the appliance, or even provide access to the console interface. LOM configuration is performed from the Gaia CLI, and must therefore be performed before the appliance is registered. See [sk92652](#) for more details.

## Defining the Sensor on the Horizon NDR Application Portal

After all preparations have been completed, you may now proceed to sensor deployment.

1. Login to the Horizon NDR application portal and access the customer domain.
2. You will be directed to the Sensors tab, as there long as there are no sensors on the domain.
3. From the lefthand menu, select **Management** --> **Sensors** --> Click **New** (top middle).
4. For a Quantum Security Gateway appliance, select **Physical** and enter the appliance's MAC in colon-separated six tuple notation (e.g. 00:1C:7F:12:34:56). The MAC is printed on a pullout label on the appliance's front panel. In addition, it is the same as the appliance's Mgmt interface's MAC address.
5. When installing a CloudGuard Network Security Gateway or Open Server, select **Virtual** instead; a virtual MAC will be automatically generated to uniquely identify the sensor.
6. Enter a description/name for the sensor.
7. Enter the sensor's location as a Latitude, Longitude pair. For example, Check Point HQ is located at 32.07, 34.79609. This will used for representation on the Cyber Threat Map.
8. Select the time zone for the sensor.
9. Click **ADD** in the lower right corner of the new sensor form.

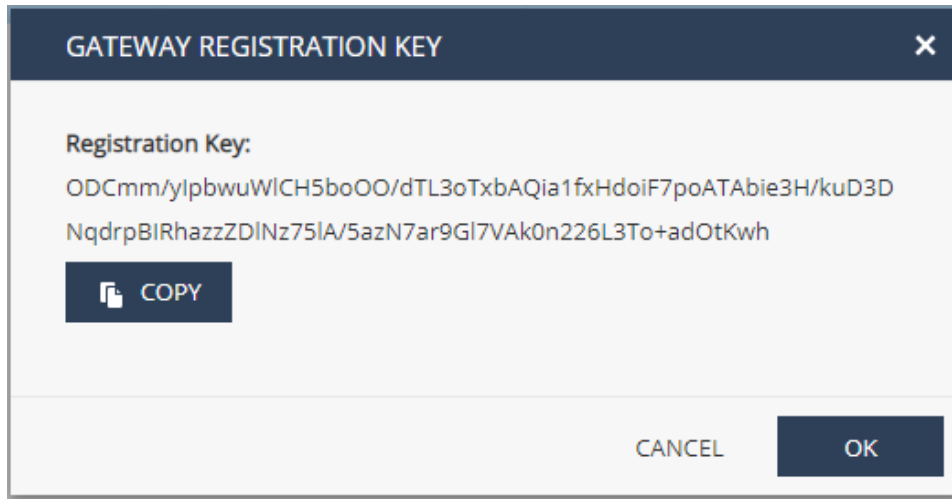
The sensor entry will now be displayed in the Sensors table with the following icons:

- State: "+", signifying that the sensor entry has been "Created".
- Connected indicator (lightbulb) is gray; this will turn green when the sensor establishes the TLS tunnel to the Horizon NDR portal.
- NDR-Managed – the Horizon NDR application will be managing this gateway

State		NDR-Managed
+	💡	✔

10. Select the sensor entry (it will be highlighted in blue) and select "Generate Registration Key" from the Actions... menu.

The registration key will appear in a new pop-up window in the portal, e.g.:



11. Copy the registration key for use on the appliance.

## Registering the Appliance

1. In expert mode on the appliance, run a command as follows using the <registration key> obtained from the Horizon NDR application portal in step 7 above:

```
curl_cli -f -s -S --cacert $CPDIR/conf/ca-bundle.crt
https://portal.now.checkpoint.com/static/install.sh | bash /dev/stdin
--token <registration key> --monitor eth1 --monitor eth2-01
```



**Note** - Configure at least one interface in monitor-mode. In the example above, both eth1 and eth2-01 are set as monitor interfaces.

2. The appliance reboots automatically, and connects to Horizon NDR using the registration key.
3. On the Horizon NDR application portal, the Connected lightbulb will turn green; then the State icon will start turning signifying policy installation. Finally, the State icon will become a check mark (✓) – “Activated”.

## Accessing the Sensor’s Gaia Portal

When an NDR-Managed sensor is activated and connected, it can be monitored and controlled only from the Horizon NDR application portal. Its resource consumption state (CPU, memory, disk) can be viewed by any user on the domain on which it’s registered, via the MANAGEMENT > System Monitor tab.

A user with Domain Administrator role on the domain will receive an additional option in the MANAGEMENT > Sensors tab’s Actions menu: “OPEN GAIA PORTAL”. Selecting the sensor and clicking this option will pop up the appliance’s Web UI in a new browser tab. This is intended to allow administrators to change interface mappings, view appliance status, and apply jumbo hotfix packages.

## Plans

Each NDR sensor is associated with a **plan** that controls its behavior. An Initial-Plan is automatically created for each domain and associated with all new sensors. You can modify this plan, or create additional plans and associate different sensors with the appropriate plan.

In contrast with standard Check Point Security Gateways that implement both access control and threat prevention, NDR focuses only on the latter. In particular, it does not manage an access policy – all traffic is allowed if it is not detected as malicious. This greatly simplifies security management, allowing for plug and play operation. The plan is therefore quite simple, defining the following attributes:

- Threat Prevention – always enabled, this includes the IPS, Anti-Virus, and Anti-Bot blades.
- Extended Visibility – enabled by default, this includes the Application Control and URL Filtering blades.
- Prevent Mode – disabled by default (i.e. default is Detect Mode). Enabling Prevent Mode will cause the sensor to block network traffic forwarded through the sensor’s inline bridges, if it is matched by one or more of the threat prevention blades with Medium or High confidence.



**Note** – An inline sensor will block network traffic matching threat indicators with action **Prevent**, even when associated with a Detect Mode plan.

- Threat Extraction – disabled by default, only active for inline traffic.
- Threat Emulation – enabled by default, files extracted from the network are uploaded to the cloud for static and dynamic analysis (sandboxing).
- Packet Capture – disabled by default, packet captures are created and attached to log records for packets matching a threat prevention detection.
- Identity Awareness and HTTPS Inspection – disabled by default and not editable; these settings reflect the status of the corresponding services, which are provisioned on request by the NDR cloud team.

		* New   Edit   Delete   Refresh							
	Name	Threat Prevention	Extended Visibility	Prevent Mode	Threat Extraction	Threat Emulation	Packet Capture	Identity Awareness	Https Inspection
	Initial-Plan	✓	✓	✗	✗	✓	✗	✗	✗



# Moving from Detect to Prevent

## Overview

The ultimate objective of NDR is to block undesirable network traffic that has bypassed other cyberdefenses (false negatives). This traffic is not obviously bad, or it would already have been prevented. When dealing with such extended detection, false positive detections are a common obstacle, as they can overwhelm the analyst; and when used for automated response, disrupt business traffic.

Therefore, when deploying a new Horizon NDR domain and sensors, the default mode of operation is **Detect**. This section details recommended steps for enabling Horizon NDR-based prevention.



**Note** – Another reason for Detect Mode as a default is that most sensors are deployed passively using Monitor Mode interfaces. Prevent Mode on such sensors would create Prevent logs, but the traffic would not be blocked as the sensor is only inspecting a mirror of the real network traffic.

## Prevention with Inline NDR Sensors

A physical NDR-Managed sensor deployed with inline interfaces supports direct prevention on the traffic flowing through its bridged fail-open NICs.

In order to activate prevention on the inline sensor:

- Define exceptions with action Prevent for protections that should apply even when in Detect Mode
- Edit the sensor's plan and enable Prevent Mode for setting the default threat protection action to Prevent
- Set the action attribute for applicable threat indicators to Prevent



**Note** – Prevention is not applied in the following situations:

- Bypass Mode – when the sensor is in Bypass On, network traffic flowing through the sensor's fail-open NICs is not being processed and cannot be detected nor prevented.
- Monitor Mode interfaces – an inline appliance can also have additional Monitor Mode interfaces; direct prevention is not supported for traffic received on these interfaces.

## Determining what would be Blocked in Prevent Mode

It is recommended to review, based on the network traffic inspected while the sensor was in the default Detect Mode, what traffic would have been blocked in Prevent Mode. Establish exceptions to cover any false positives that might impact business traffic.

For example, you might create a DOMAIN or PERSONAL view that matches such traffic:

The screenshot shows a configuration form for a threat prevention rule. The fields are as follows:

- Name:** WHAT WOULD BE BLOCKED IN PREVENT MODE (N/S)
- Description:** Internal/External communication with high confidence
- Filter:**

```
((src:(10.0.0.0/8 OR 172.16.0.0/12 OR 192.168.0.0/16) AND NOT
dst:(10.0.0.0/8 OR 172.16.0.0/12 OR 192.168.0.0/16)) OR (NOT
src:(10.0.0.0/8 OR 172.16.0.0/12 OR 192.168.0.0/16) AND dst:
(10.0.0.0/8 OR 172.16.0.0/12 OR 192.168.0.0/16)) AND (action:
(Prevent OR Block OR Redirect OR Reject OR Drop) OR
confidence_level:High OR confidence_level:Medium)
```
- Color:** User Defined

Note that the IP ranges in this example are the main default internal ranges. Your network might have different internal IP ranges. These internal ranges should also be defined in the MANAGEMENT > Settings tab. In addition, this example assumes that the NDR sensor's inline bridge forwards traffic between the internal network and the Internet (North/South), and ignores East/West traffic – your network might have a different configuration.

In some cases, e.g. when under active attack, you might prefer to switch to Prevent Mode immediately and create the exceptions only after users complain that their traffic is blocked.

## Exceptions

You can use the MANAGEMENT > Exceptions tab to manage threat prevention exceptions. These are applied on specific sensors, or globally on all sensors of the domain. Exceptions are provisioned on corresponding threat prevention rules, and threat prevention policy is installed on the sensors for every modification.

The exception attributes are equivalent to the ones supported by the Check Point SmartConsole application, including:

- Scope – expressed as Sources or Destinations in CIDR notation. For an individual IP address, use /32.
- Protections or Blades – select blade names from the pull-down menu, or enter a protection name.

- Services – select from the menu or type the service name
- Action – changes the behavior of the selected protections or blades, for the defined scope and services:
  - Prevent – used in Detect Mode, or to enable Prevent on Low confidence protections
  - Detect – used in Prevent Mode to cause the sensor to log, but not block the specified traffic
  - Inactive – turns off the selected protections or blades
- Track – set to 'None' when defining exceptions with action 'Inactive'

## Threat Prevention using Threat Indicators

Threat indicators managed on the INTEL tab have an Action attribute of DETECT or PREVENT. Network traffic matching indicators with Action PREVENT will be blocked by an NDR appliance if forwarded on its inline bridges. Such blocking will apply regardless of whether the plan is set to Detect or Prevent.

In order for the NDR appliance to apply the indicators, they must be associated with a data set that has **Apply on NDR Sensors** enabled (the default). In addition, they should have status **Enabled**, and not be expired.

Threat indicators are the primary Horizon NDR response mechanism, because they can be published to non NDR-Managed Check Point gateways, as well as 3<sup>rd</sup> party firewalls. This allows you to use Horizon NDR in a passive mode of operation, and prevent indirectly via indicators.

You can create threat indicators from the Horizon NDR application manually, load them from file, or configure automated input feeds to pull them from external sources. In addition, Horizon NDR Behavioral Analytics AI engines will automatically publish threat indicators to block detected high-risk traffic.

The default action for new manually-created indicators is DETECT. You can set the action to PREVENT during initial entry, or subsequently by editing the indicators. Editing can be performed individually or in bulk. For editing in bulk – select the indicators that you are looking to switch to PREVENT, select Bulk Edit, and set Action to **Prevent**. Alternatively, select the indicators and click **PREVENT**.

For automatically-created threat indicators, the default action is determined by the corresponding input feed's policy. This policy applies only when the indicator value is first created. You can change the Action on existing indicators and this new Action will persist even if the input feed source refreshes the indicator.

For example, you might consider switching the Behavioral input feed's action to Prevent, for Medium and High confidence indicators. This input feed is created by default for all domains, representing the NDR Behavioral Analytics engines.

For more information on threat indicators, refer to the Horizon NDR Indicator Management User Guide.

## Configuring Check Point Security Gateways to Pull NDR Indicators

You can easily configure your Check Point firewalls to pull feeds of threat indicators from Horizon NDR for blocking. Prevention is achieved automatically, with no policy push required.

Each indicator can be associated with one or more data sets, either manually or via input feed policy. A data set is published on two output feed URLs: Prevent and Detect. Each of these feeds includes the indicators associated with the data set that have the corresponding action (Prevent or Detect). This separation is useful because Check Point Security Gateways associate action with an individual feed configured on the gateway.

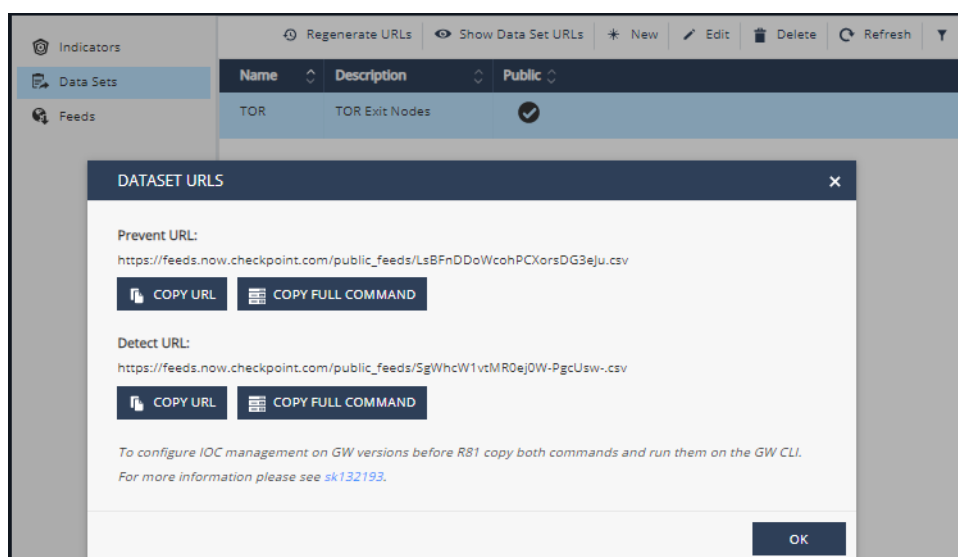
The URL for each output feed is displayed on the portal, and may also be easily copied to the clipboard via the "COPY URL" button. For convenience, a "COPY FULL COMMAND" option is provided, which enters a complete gateway `ioc_feeds` command that can be entered on a gateway for pulling the output feed.

To enable a feed on the Check Point Security Gateway:

- Select the desired data set (e.g. Behavioral, or TOR Exit Nodes).
- Click **Show Data Set URLs**.
- Click COPY FULL COMMAND for the desired set of indicators (DETECT or PREVENT). This places a complete gateway `ioc_feeds` command in the paste buffer.
- On the gateway, in Expert mode, paste and execute the command.

Alternatively, with Check Point Security Management R81.10 and above, you can use the COPY URL option and configure the feeds from your SmartConsole, under **Security Policies > Threat Prevention > Indicators**.

For more information on enabling this functionality on your Security Gateway, refer to SecureKnowledge solution sk132193 - *What is the "Custom Intelligence Feeds" feature?*.



# Horizon NDR Log Server Registration

## Overview

Customers that already have a Check Point log server can send their logs to the Horizon NDR application using Check Point Log Exporter ([sk122323](#)), in addition to or instead of deploying dedicated Horizon NDR sensors. The Log Exporter configuration is packaged by the Horizon NDR application, and then downloaded to the customer's log server and executed with a single command.

## Prerequisites

- The Log Server must be running version R80.30 or higher
- If there is a firewall on the path to the Internet, it must allow TCP port 443 connectivity from the appliance's Mgmt interface to IP addresses 35.156.213.136, 3.120.103.74, and 18.196.115.85 (portal.now.checkpoint.com).
- The Log Server authenticates to the Horizon NDR application portal using mutually-authenticated TLS; therefore if the customer is using HTTPS Inspection on the outbound path, you must request an exemption for the log export traffic from the Log Server
- An HTTPS Inspection exemption will also be required for user access to the Horizon NDR application portal at <https://now.checkpoint.com>
- In order for Horizon NDR to be effective, you should enable Extended Logging for the Application Control and URL Filtering blades on your Check Point gateways. Additional recommended blades include: IPS, Anti-Bot, Anti-Virus, and Threat Emulation.





## Registering the Log Server

1. Login to the Check Point log server in Expert Mode.
2. Paste the personalized script and hit "Enter".
3. If everything is working correctly, the script will execute cleanly and wish you a good day. If there is any error message, please contact the Check Point Horizon NDR team with the error details.
4. Once logs start flowing to NDR, the lightbulb icon next to the sensor will turn green:

State	NDR-Managed
✓	💡 ... ✗

# Check Point Horizon NDR for AWS

## Overview

Horizon NDR automatically deploys a Check Point CloudGuard Network Security instance in Monitor Mode into the customer's AWS VPC, via an AWS CloudFormation stack. The stack registers Lambdas (serverless compute instances) that use cloud-native APIs to provision cloud vendor traffic mirroring, in order to selectively mirror network traffic for analysis and threat detection. Deployment is quick and intuitive, and takes minutes. There is no need for network security expertise because the sensors do not require any configuration and do not influence traffic flow; there is no need to create complicated policy rules.

## Terminology

Before you use this solution, you should make yourself familiar with these AWS terms and services:

- VPC
- Region and Availability Zone (AZ)
- EC2
- Traffic Mirroring
- Elastic Network Interfaces (ENI)
- Elastic Load Balancing (ELB/NLB)
- Lambda
- CloudFormation
- CloudWatch
- Identity and Access Management (IAM)

If you are new to AWS, see [Getting Started with AWS](#).

## Scoping and Costs

The customer's AWS estate is allocated to accounts, regions, and VPCs. The Check Point Horizon NDR solution monitors network traffic between, into, and out of EC2 compute instances. Each EC2 instance is defined in a single VPC and AZ, and communicates using one or more ENIs.

NDR uses cloud-native AWS Traffic Mirroring in order to receive network traffic for inspection. A CloudGuard Network Security (CG NS) instance is provisioned as an NDR sensor via CloudFormation stack. An AWS Network Load Balancer (NLB) is also provisioned in front of the CG NS. Traffic mirroring is configured for a specific VPC and AZ, by creating mirroring sessions from all ENIs that match a mirroring policy, to the NLB. The NLB routes the mirrored traffic to the NDR sensor.

Traffic Mirroring is priced by AWS on a per-mirrored ENI basis at approximately \$11/month per ENI. (This pricing varies across different AWS regions.) Horizon NDR instance costs are dependent on the sustained rate of mirrored traffic sent to the sensor (larger amount of mirrored traffic requires larger Horizon NDR instance size). These two factors are the major contributors to the cost of the Horizon NDR solution. The other components (lambda compute, NLB, etc.) are typically comparatively negligible, assuming that the mirrored ENIs and the mirroring target (the NDR instance) are in the same AZ.

## Resources Required on the AWS Account


### Step 1: Preparing the customer's AWS account

1. Make sure you know which VPCs and AZs you will be mirroring, and have sufficient IAM permissions to provision the NDR components. Missing permissions will cause the deployment to fail, with indicative error messages being output to the AWS Console.
2. Use the region selector in the navigation bar to select the AWS region, where you want to deploy the NDR instance on AWS.
3. You will need an [SSH key pair](#) in your preferred region.
4. If necessary, request a service limit increase for the AWS resources that you plan to use. By default this guide uses:
  - c5.xlarge for the Horizon NDR instances
5. The Horizon NDR instance is intended to be deployed into an existing VPC with existing workloads. Accordingly, customers must deploy into an existing VPC and create 2 subnets for use by Horizon NDR. These subnets must be in the same Availability Zone within the region:
  - 1 internal subnet to be used for the Horizon NDR instance's interface to receive traffic mirroring
  - 1 external subnet with Internet access for the instance to send logs to the Horizon NDR portal
6. The external subnet should present a route out to the Internet. If it is placed behind a network gateway, the Horizon NDR instance can be allocated a local AWS IP address. Otherwise, an Elastic IP (EIP) should be configured for the Horizon NDR instance for direct outbound access.

### Step 2: Subscribing to CloudGuard Network Security in AWS Marketplace

In order to deploy a Check Point CloudGuard NDR Sensor, you must first subscribe your AWS account to Check Point CloudGuard Network Security with these steps:

1. Log in to AWS Marketplace.  
(You must have aws-marketplace:Subscribe IAM permission.)
2. Select the BYOL licensing option for the Check Point CloudGuard Network Security: [CloudGuard Network Security with Threat Prevention & SandBlast BYOL](#)
3. If the account is already subscribed, you will see at the top of this AWS Marketplace page that the AWS account is already entitled, as follows:



**You have access to this product**  
You or someone in your organization has already purchased entitlements for this product. You can view your subscription or share access to it via [AWS License Manager](#)

View Subscription

✕

4. Otherwise, select **Continue** to subscribe.
5. Select **Accept Terms** to confirm that you accept the AWS Marketplace license agreement.

## Launch in AWS

After all preparations have been completed, you may now proceed to sensor deployment.

12. Login to the Horizon NDR portal and access the customer domain.
13. You will be directed to the Sensors tab, as there are no sensors on the domain.
14. From the lefthand menu, select **Management** --> **Sensors** --> Click **New** (top middle), then select **Virtual** and enter a description/name for the sensor. Select the correct time zone. Then click ADD in the lower right corner.
15. Select the new sensor entry, and click on **Actions** --> **LAUNCH IN AWS**.
16. This action generates a registration key for the new virtual sensor, and launches an AWS CloudFormation template in a new browser tab. It will first redirect you to login to your AWS account.



**Note** – Customers' AWS credentials are NOT provided to the Horizon NDR application portal nor in any way received or stored by Check Point Software Technologies.

## Horizon NDR CloudFormation Template

### 1. AWS General Configuration

The following parameters must all be filled in before creating the stack:

- a. **Stack Name:** will be automatically generated based on the sensor name. You may change this name if desired, e.g. to identify the AZ in which the sensor is instantiated.

If relaunching the stack due to some error, e.g. missing IAM permissions, it is recommended to change this name to avoid resource collision in case the previous stack has not completed automated cleanup operations.)

- b. **VPC** where you want to deploy the Horizon NDR instance.
- c. **Availability zone:** a Horizon NDR instance should be deployed in each monitored AZ in order to avoid AWS inter-AZ network traffic mirroring costs.
- d. **AZ External subnet:** This subnet should have access out to the Internet (either directly or routed via other networks).

In particular, the network should support TCP port 443 traffic to the following IP addresses: 3.64.14.68 and 35.156.213.136. If there is an outbound proxy, it must exempt HTTPS traffic inspection to these addresses.

- e. **AZ Internal subnet:** The mirrored traffic will be delivered to a Horizon NDR instance's VXLAN endpoint on this subnet. It may be the same as the AZ External subnet.



**Note** - Make sure the selected subnets are compatible with the selected availability zone.

## 2. Horizon NDR Sensor Configuration

The following parameters must all be filled in before creating the stack:

- a. **EC2 Instance type:** AWS instance size used for the NDR sensor instance.

The default is **c5.xlarge**. An oversized sensor will be more expensive in terms of AWS costs. On the other hand, an undersized sensor will provide reduced visibility due to uninspected connections, and in extreme cases will become unstable and disconnect from the Horizon NDR back end.

The primary sizing consideration is the volume of traffic mirrored to the sensor for inspection. See Appendix A for guidelines on estimating traffic volumes in AWS, using AWS CloudWatch, where customers do not have this data handy.

For a rough guide on choosing the instance type:

AWS instance type	c5.large	c5.xlarge	c5.2xlarge	c5.4xlarge	c5.9xlarge
# vCores	2	4	8	16	32
Max total traffic/sec	~0.5 Gbps	~1 Gbps	~2 Gbps	~4 Gbps	~8 Gbps

- b. **EC2 key name:** AWS security key pair for SSH access to the Horizon NDR instance. Normally this key is not used, but some key pair must be entered to allow instance deployment. There is no default.
- c. **Allocate EIP?** By default this attribute is set to "No", as in most customer VPCs, the Horizon NDR EC2 instance that is created on the AZ External subnet will receive an internal AWS IP address and a default gateway for outbound connectivity. Set this to "Yes" if you require an AWS Elastic IP to be allocated on the instance for direct Internet access.

### Procedure for Resizing a Horizon NDR Sensor on AWS

For an activated sensor (in "✓" state), in case it is undersized or oversized and you need to change instance Type, follow these steps to relaunch it with the new size:

1. On AWS, delete the stack. This will clean up all resources consumed by the Horizon NDR solution.
2. On the Horizon NDRapplication portal - on the MANAGEMENT > Sensors tab
  - a. Select the sensor entry (it will be showing as "Disconnected" (grey lightbulb icon)
  - b. Click on **Actions** --> **X DEACTIVATE**
  - c. Click on **Actions** --> **LAUNCH IN AWS**
3. Fill in the CloudFormation Template with the new parameters.



**Note** – It is recommended to verify that the old stack has completed deletion before launching the new one; or to manually modify the stack name to avoid named collisions on deployed AWS resources.

### 3. CG NDR Configuration – Advanced

The following parameters all have valid default values and do not require modification. They provide for advanced Horizon NDR sensor configuration.

- a. **Expiration period:** Time after which the stack is automatically deleted, releasing all AWS resources allocated for this stack. Defaults to “No expiration”.
- b. **Include EC2 Instances with the following tags (default all):** May be used to constrain the set of mirrored EC2 instances, using a comma-separated list of Key=Value AWS tags.
- c. **Exclude EC2 Instances with the following tags (default none):** May be used to further constrain the set of mirrored EC2 instances.
- d. **Monitor all ENIs?** For multi-homed EC2 instances, setting this parameter to “No” will only monitor the main ENI.
- e. **VXLAN ID:** VTEP number for mirroring sessions. Normally set to default value of “1”.
- f. **VPC scan interval:** Defaults to 10 minutes.
- g. **Version:** Do not change.
- h. **Registration key:** Do not change.

### 4. Confirmation and Stack Creation

Check the acknowledgement and click “Create stack”. The CloudFormation Template (CFT) spins up the Horizon NDR instance in your selected VPC and AZ, and runs two lambda functions that provision AWS traffic mirroring. It will typically take up to 20 minutes before you start seeing logs on the Horizon NDR application portal. The sensor’s display on the portal will change to a green lightbulb icon with a “✓” state. CFT progress can be tracked in the AWS Console, including any relevant error messages.



## 5. AWS Resources Provisioned by the CFT

- a. A security group is created for each ENI:
  - Internal ENI: allow incoming vxlan (udp 4789), reject outbound
  - External ENI - allow incoming ssh/https (tcp 22/443), allow outbound
- b. AWS Traffic Mirroring sources and sessions for each mirrored ENI.
- c. AWS Network Load Balancer (NLB), defined as the mirroring target, routes mirrored traffic to the NDR sensor instance over the defined VXLAN on the AZ Internal subnet.
- d. Two lambda functions that automatically configure AWS traffic mirroring. An EC2 instance creation event on the VPC will trigger its evaluation against the mirroring policy (include and exclude lists). In addition, the VPC will be scanned on the defined scan interval, and any deleted EC2 instances will result in cleanup of the corresponding mirroring sources and sessions. These invocations are controlled by EventBridge rules.
- e. Elastic IP if enabled in the CFT.



**Note** - If you delete the stack from the AWS Console - this will clear up all related resources in your VPC, including the Horizon NDR CloudGuard Network Security instance, the lambda functions, and the traffic mirroring sessions.

## Mirroring Additional VPCs

The “LAUNCH IN AWS” CFT provisions traffic mirroring for a specified VPC and AZ, and mirrors the traffic to a load balancer and Horizon NDR sensor. An alternative “PROVISION AWS MIRRORING” CFT is provided which does not create the latter two instances. Rather, it accepts the mirroring target as a parameter. This is intended to allow reuse of a single deployed Horizon NDR sensor for mirroring traffic from multiple VPCs. As long as the sensor and the mirrored traffic are defined in the same Availability Zone, there are no additional AWS costs due to inter-VPC or even inter-account traffic mirroring.



**Note** – It is not recommended to mirror across AZ boundaries (even though there is no technical limitation). AWS costs will grow significantly if traffic is mirrored between different AZs.

In order to provision mirroring on a different VPC:

1. From the lefthand menu, select **Management** --> **Sensors** --> Click **New** (top middle), then deselect **Managed** and enter a description/name for the sensor. Select the correct time zone. Then click ADD in the lower right corner.
2. Select the new sensor entry, and click on **Actions** --> **PROVISION AWS MIRRORING**.
3. This action launches an AWS CloudFormation template in a new browser tab. It will first redirect you to login to the customer's AWS account. Ask the customer to enter his AWS account number and access credentials in order to access his AWS Console.
4. The CFT parameters are equivalent to those of LAUNCH IN AWS, with the following exceptions:
  - As no sensor is deployed, the CFT omits the following parameters: AZ External Subnet, AZ Internal Subnet, the entire CG NDR Configuration section, Version, Registration key
  - A Traffic Mirror Target parameter is added. Enter a Horizon NDR load balancer's mirror target ID (e.g. 'tmt-xxxxxx').
5. Check the acknowledgement and click "Create stack".

## Traffic Mirroring Include/Exclude Lists

Traffic mirroring include and exclude lists are handled by the Horizon NDR Cloud Formation template which is deployed per sensor from the Horizon NDR portal. You can include comma-separated key value pairs in the CFT to indicate whether you'd like to include or exclude that instance from traffic mirroring. For example:

- MYTAG=DOMIRROR,MYOTHERTAG=INSTANCE
- CKP\_TYPE = Sensor

Be sure to apply these tags to each instance according to whether you'd like to include or exclude them from traffic mirroring.

If you'd like to update your traffic mirroring include/exclude tags after initial CFT deployment, simply issue a CFT Stack update to revise the tags or to apply a different tag scan interval.

1. Find the CloudFormation Stack used to deploy your sensor, and select the "**Change Sets**" tab, then click on "**Create Change Set**".
2. Choose to Use the current template and click "**Next**".
3. Change the Include or Exclude tags as applicable and/or change the VPC Scan interval. When satisfied, click "**Next**".
4. Leave all stack options as-is (do not make any changes) and click "Next".
5. At the review screen, verify all parameters, then acknowledge the stack capabilities and click "**Create Change Set**".
6. Give the change set a name and click "**Create Change Set**" to make the changes to the applicable Horizon NDR sensors.

## Sensor Deactivation on Stack Deletion

If you choose to delete the Cloudformation Stack which deployed your NDR Sensor, and relaunch in AWS from the Horizon NDR application portal, you will also need to first deactivate the sensor on the portal. This is because the Horizon NDR back end is not aware that the sensor was deactivated, only that it is disconnected.

On the MANAGEMENT > Sensors tab, select the relevant sensor, and X DEACTIVATE from the Actions menu.

# Users and Access Control

## Domains

The “domain” is the fundamental object collection on Horizon NDR. All objects are associated with a domain. This includes sensors, logs, packet captures, indicators, views, insights, reports, etc.

## Authorizations

Each domain defines a set of user authorizations, viewed and edited via MANAGEMENT > Users. A user’s authorization on the domain defines a Role for the user’s access to the domain.

## Users

The user object itself is created the first time an authorization is created on any domain, naming the user’s email address. The user is independent of any domain. The user’s email address is used both as the user’s unique identity, and for the purpose of communicating with the user, e.g. for reports and notifications.

The user receives an email with a link. Clicking on the link provisions the user object and generates a certificate with the user’s email address as the CN. This certificate is downloaded to the user’s endpoint and installed with a user-defined security level.

When the user logs in using his certificate, the Horizon NDR application verifies his or her certificate, retrieves the user’s domain authorizations, and matches them to the requested domain and service. Unauthorized requests will be rejected. Both authorized and unauthorized requests are audited and can be viewed on the MANAGEMENT > System Events tab.



**Note** – Deleting a user record from MANAGEMENT > Users will not revoke the user’s certificate – only the user’s authorizations to the domain. If a user is left with no authorizations to any domain, the user account will be eventually deleted by automated cleanup services, and the user certificate revoked.



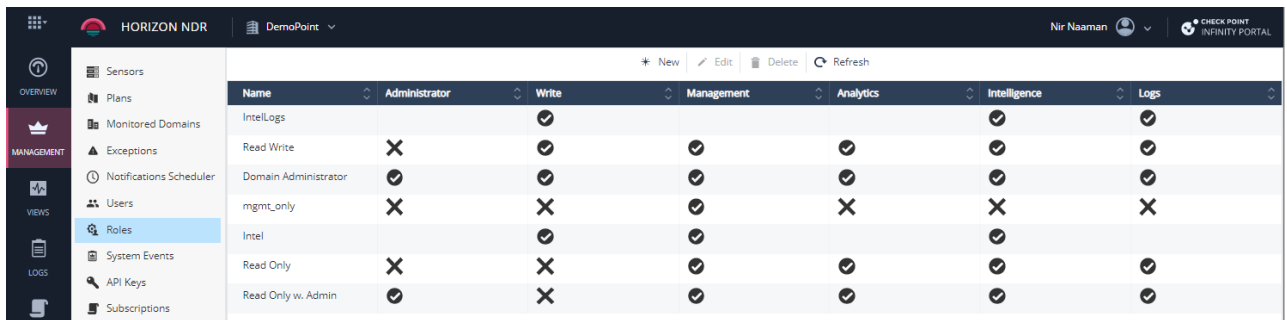
**Note** – MANAGEMENT > Users > Actions > REISSUE CREDENTIALS can be invoked on a user entry by any user with Write authorizations. This triggers an email with a reissue link to be sent to the target user’s email address; if the user receives the email and click the link, a new certificate will be generated and provided for download.

## Roles

A Role defines a set of permissions that enable Horizon NDR services. Currently-supported permissions can be seen on the MANAGEMENT > Roles tab. These include:

- **Administrator** – required for sensitive services such as user authorizations, monitored domains, and input feed management
- **Write** – allows modifications to objects on the domain
- **Management** – controls access to the MANAGEMENT tab and its services

- **Analytics** – controls access to the VIEWS and INSIGHTS tabs and their services
- **Intelligence** – controls access to the INTEL tab and its services
- **Logs** – authorizes the user to view logs on the domain



Name	Administrator	Write	Management	Analytics	Intelligence	Logs
IntelLogs		✓			✓	✓
Read Write	✗	✓	✓	✓	✓	✓
Domain Administrator	✓	✓	✓	✓	✓	✓
mgmt_only	✗	✗	✓	✗	✗	✗
Intel		✓	✓		✓	
Read Only	✗	✗	✓	✓	✓	✓
Read Only w. Admin	✓	✗	✓	✓	✓	✓

Permissions are grouped under named roles. By default, each domain includes the “Read Only”, “Read Write”, and “Domain Administrator” roles. Additional roles can be defined as required.

For example, the Read Only role provides access to all tabs, but does not allow the user to manage user authorizations or modify any objects. The Intel role depicted above will allow the user to view and modify indicators, but not logs. The Horizon NDR application will display a tailored menu for a user in the Intel role, omitting OVERVIEW, VIEWS, LOGS, REPORTS, and INSIGHTS. Thus such a user would only see MANAGEMENT and INTEL.

## Monitored Domains

An authorized Domain Administrator can create a new domain from the MANAGEMENT > Monitored Domains tab. This creates a monitored subdomain, that can be accessed by all users authorized to the monitoring domain. The monitored domain will be added to the domain drop-down menu for these users.

The role construct is also used when provisioning monitoring relationships between domains. The monitored domain defines the permissions that the users authorized to the monitoring domain will receive on the monitored domain’s objects. Effective permissions will be the intersection (i.e. minimum) of the user’s permissions on both domains.

For example, suppose domain X is monitoring domain Y, with Read Only role. A user is authorized as a Domain Administrator on X. His effective permissions on access to Y’s objects and services will be Read Only Domain Administrator. If the user is authorized to both X and Y, access to Y’s objects and services will be controlled using the more specific role assignment, i.e. the authorization on the Y domain.

When the monitoring relationship is created in the context of creation of a subdomain, the Domain Administrator role is used for the relationship.

## Establishing a Monitoring Relationship between two Domains

The monitoring relationship between monitoring and monitored domains can also be created between any two arbitrary domains, even if the two domains were originally created independently. This is achieved as follows:

- A Domain Administrator on the monitored domain clicks “\* New” on the MANAGEMENT > Monitored Domains tab, and specifies a Monitoring Domain Name. A contact name and email should be provided, as well as a role selected for the monitoring relationship.
- The request will show up on the monitoring domain. A Domain Administrator for that domain must Approve the request before it takes effect.

For example, in order to allow the Check Point Managed Detection and Response (MDR) service to monitor your domain, enter “Check\_Point\_MDR” as the Monitoring Domain Name. Once the monitoring request is approved by the MDR team, the MDR service will automatically start using Horizon NDR APIs to pull insights and logs from Horizon NDR to MDR, and to deliver threat indicators to enforcement points for prevention.

A Domain Administrator on either monitoring or monitored domain can break the relationship by deleting it.



# NDR Security Checkup Report

## Overview

The Horizon NDR Web application allows the user to easily generate a Security Checkup report as well as other more specialized reports for delivery to the customer. Where desired, additional users can be authorized to review this information on the application.

After the Horizon NDR sensor completes activation, it will start sending logs generated by the different Check Point “software blades”. By default, these include both threat prevention (Anti-Bot, Anti-Virus, IPS, Threat Emulation) and access blades (Firewall, Application Control, URL Filtering). These logs persist on the customer’s domain even after the sensor has been deactivated.

## Generating an NDR Report

1. Browse to the Reports tab.
2. Click “+ REQUEST” to submit a new report request.
3. Enter a **Description** for the report.
4. The **Date** range defaults to the last 7 days – this is typically sufficient for a Security Checkup.
5. Leave the **Language** setting as “English” – currently the only supported language.
6. Select report **Type**: “**NDR Security Checkup**” or “**Security Checkup - Advanced**” (see below).
7. Enter your email address to which the report will be delivered.
8. Optionally enter a **Filter**. This is typically used to exclude uninteresting data, or to focus on a specific part of the network.
9. Click **SEND** to submit the report request.
10. After a few minutes, the report should be received in your mailbox and displayed in the Reports tab on the portal.

The screenshot shows a web interface for generating a report. At the top, there are navigation options: '+ REQUEST', 'SCHEDULER', 'Delete', 'Refresh', and a search bar. Below this is a modal window titled 'NEW REPORT' with a close button. The main form is titled 'Request Report' and includes the following fields:

- Description:** A text input field containing 'NDR Security Checkup' with a green checkmark icon on the right.
- Date:** Two date pickers. The first is set to 'October 17th 2021' and the second to 'October 24th 2021'.
- Choose a Language:** A dropdown menu set to 'English' with a green checkmark icon.
- Type:** A dropdown menu set to 'NDR Security Checkup' with a green checkmark icon.
- Emails (separated by a comma):** A text input field containing 'nir@checkpoint.com' with a green checkmark icon.
- Filter:** A text input field with the placeholder text 'Type Here...'.

At the bottom right of the form, there are two buttons: 'CANCEL' and 'SEND'.

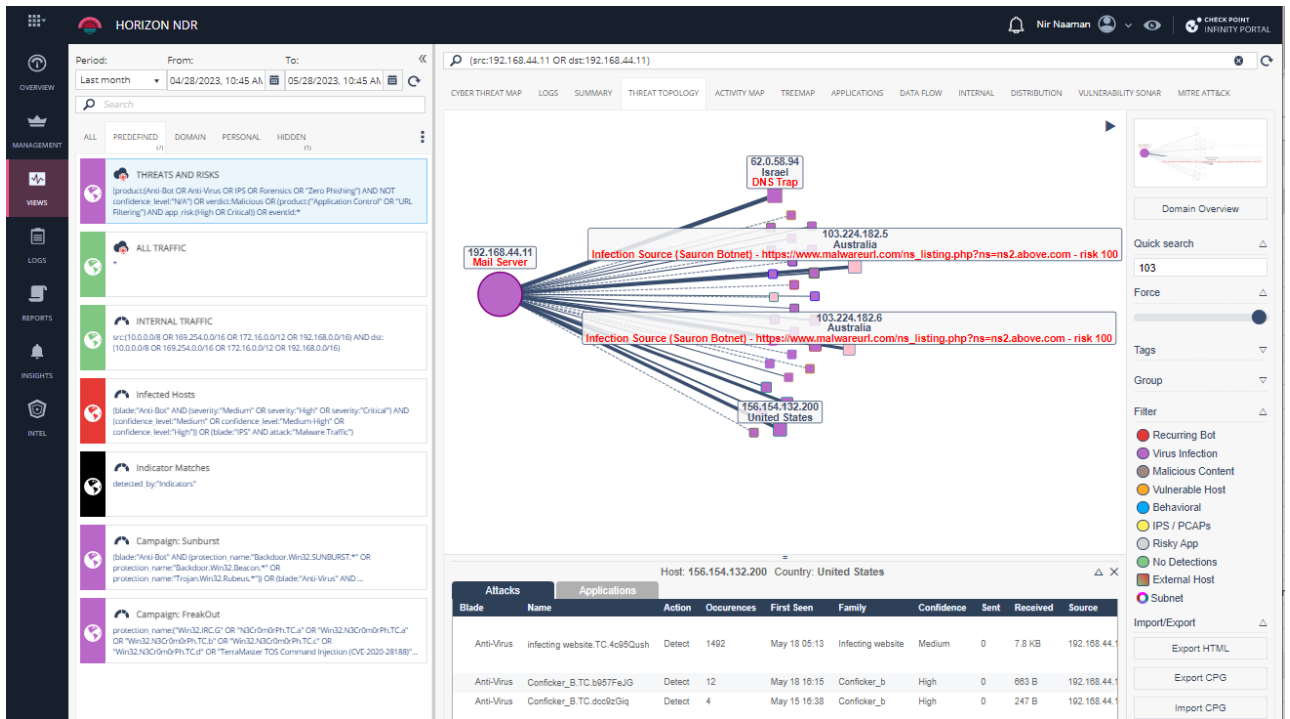


### Horizon NDR Report Types for Security Checkup

- **Security Checkup - Advanced** – Includes the findings of a variety of security threats: malware infections, usage of high risk web applications, intrusion attempts, loss of sensitive data, etc.
- **NDR Security Checkup** – Customized and scoped report for NDR, including the findings of a security assessment conducted in your network leveraging AI insights and threat analytics.

# Generating a Threat Topology Report

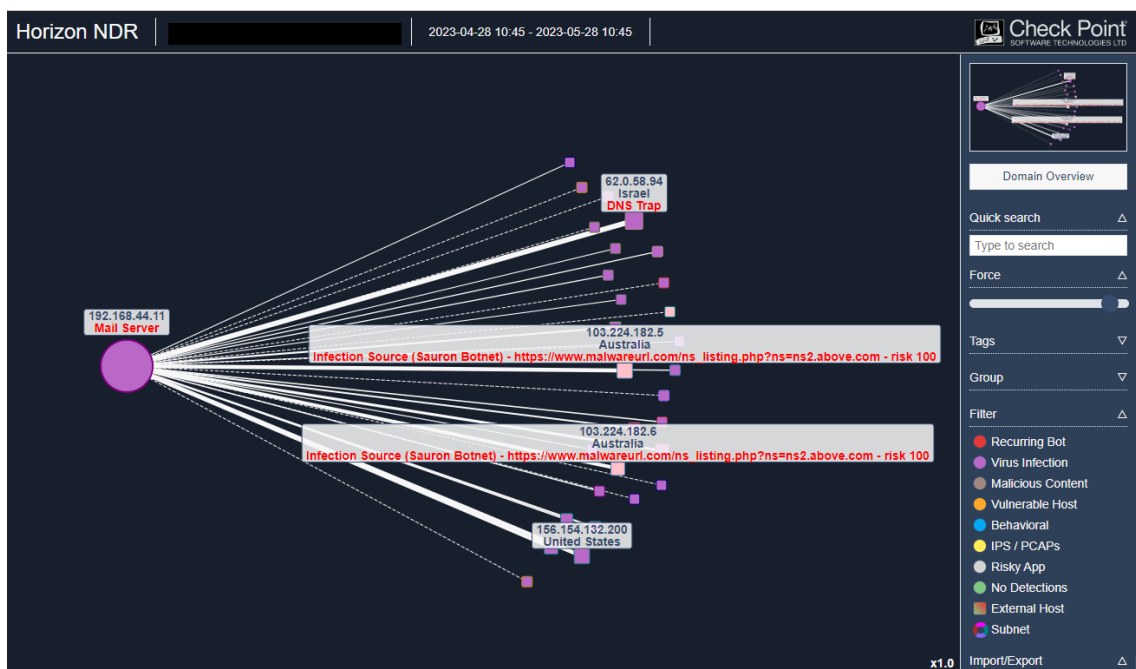
One of the advanced analytical tools on the Horizon NDR portal is the Threat Topology visualization. Threat Topology allows the customer to map network interactions and prioritize different event types.



In order to export a Threat Topology visualization for presentation outside of the portal:

1. On ANALYTICS > Threat Topology, click Export HTML (bottom right)

This will generate a report in HTML archive format, that you can send to the customer. Opening the report object will provide an offline interactive experience that is similar to the one on the Horizon NDR application.



# Appendix A – SPAN Port Configuration

## HP/Aruba Switches

See: <https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=25100>

1. Create the session and assign the local mirroring port (where your IDS is connected):
  - a. **mirror session-# port exit-port-# [name name-str]**
  - b. e.g.: *mirror 1 port 11*

\*session-# = value from 1 to 4

2. Assign the monitored ports, vlans or mac addresses to any of the created local port mirroring sessions:
  - a. **interface {port | trunk | mesh} monitor all {in | out | both} mirror {session-# | name-str} [{session-# | name-str}] [{session-# | name-str}] | [{session-# | name-str}] [no-tag-added]**
    - i. e.g.: *interface 28 monitor all both mirror 1*
  - OR
  - b. **vlan vid-# monitor all {in | out | both} mirror {session-# | name-str} [{session-# | name-str}] [{session-# | name-str}] [{session-# | name-str}]**
    - i. e.g.: *vlan 32 monitor all both mirror 1*

## Cisco Switches

See: [https://www.cisco.com/c/en/us/td/docs/switches/metro/me3600x\\_3800x/software/release/15-3\\_2\\_S/configuration/guide/3800x3600xscg/swSPAN.pdf](https://www.cisco.com/c/en/us/td/docs/switches/metro/me3600x_3800x/software/release/15-3_2_S/configuration/guide/3800x3600xscg/swSPAN.pdf)

1. Enter the switch configuration mode
  - a. **configure terminal**
2. Create the monitoring session
  - a. **monitor session {session\_number} type local**
  - b. e.g.: *monitor session 1 type local*
3. Designate the source port with 'both' for ingress and egress
  - a. **source interface interface\_type {list(,) or give range(-) of interfaces} both**
  - b. e.g.: *source interface gigabitethernet 2/1 both*
  - c.
4. Designate the destination port
  - a. **destination interface interface\_type {list(,) or give range(-) of interfaces} both**
  - b. e.g.: *destination interface gigabitethernet 2/4*
5. Enable the SPAN session
  - a. **no shutdown**

Example all together:

```
Switch# configure terminal
Switch(config)# monitor session 1 type local
Switch(config-mon-local)# source interface gigabitethernet 2/1
Switch(config-mon-local)# destination interface gigabitethernet 2/4
Switch(config-mon-local)# no shutdown
```

## Juniper Switches

See: <https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/port-mirroring-and-analyzers-configuring.html>

# Appendix B – Binding w. Horizon XDR/XPR



**Note** – Horizon XDR/XPR is served from a separate portal from Horizon NDR – it is published on the Infinity Portal: [portal.checkpoint.com](https://portal.checkpoint.com).

## Creating a Horizon XDR/XPR API Key

1. Login to the Horizon Portal and select HORIZON XDR/XPR as the application.
2. On GLOBAL SETTINGS > API Keys, click “\* New”, select “Horizon XDR XPR” as the Service, and optionally enter a Description (e.g. “Binding with Horizon NDR”). Click CREATE.
3. Horizon XDR/XPR outputs two values: a Client ID, and an Access Key. Copy these values, as you cannot retrieve the Access Key after you close the window.

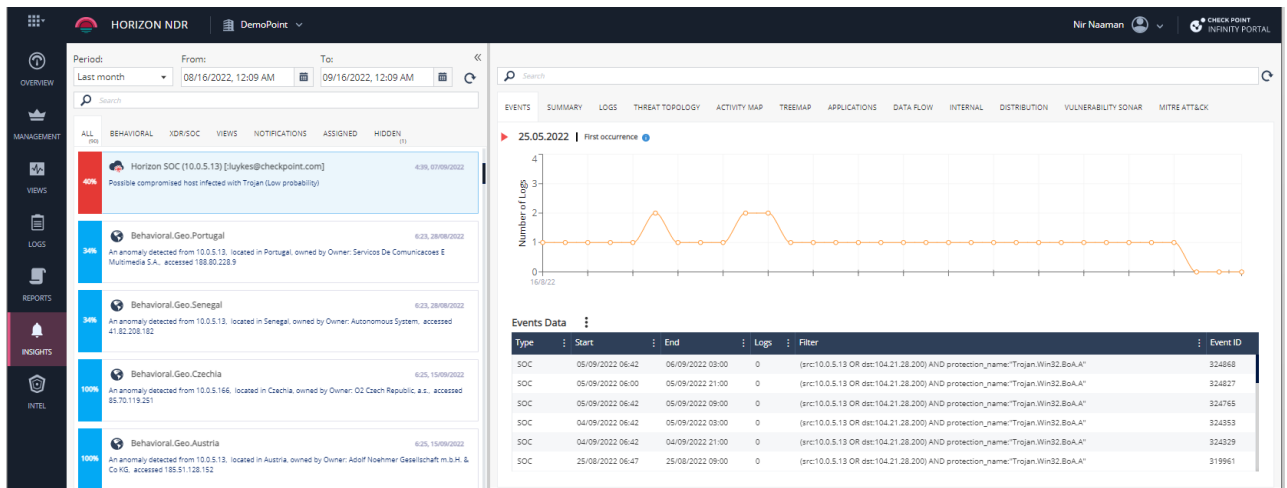
The screenshot displays the 'API Keys' management page in the Horizon XDR/XPR portal. The page title is 'HORIZON XDR/XPR' and the user is 'Nir Naaman'. The left sidebar shows the navigation menu with 'API Keys' selected. The main content area shows a table of API keys with the following data:

	Status	Service	Roles	Client ID	Description
<input type="checkbox"/>	✓	Horizon SOC	Admin	8444e...	Binding with Horizon SOC
<input type="checkbox"/>	✓	Horizon XDR XPR	Admin	dfa3d...	Binding with NDR

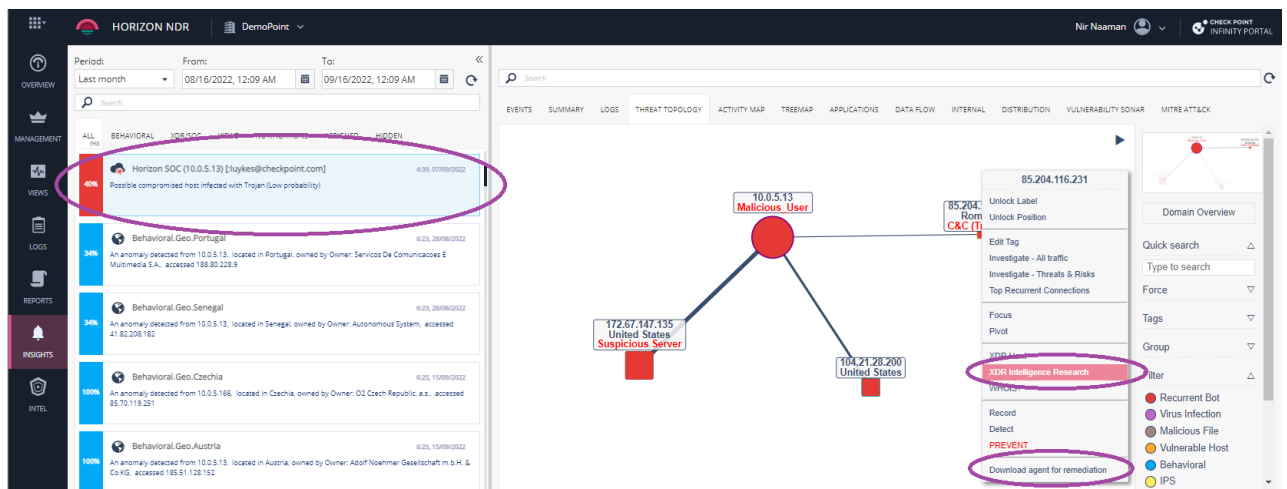
At the bottom of the table, there is a note: "It is best practice to give a separate API Key for each third-party application."

# Importing the Horizon XDR/XPR API Key into Horizon NDR

1. Login to the Horizon NDR application portal and access the customer domain.
2. On the MANAGEMENT > API Keys tab, click “\* New”, select “Horizon XDR/XPR” as Type, and enter the previously-copied Client ID and Access Key from Horizon XDR/XPR.
3. Horizon NDR pulls the Horizon XDR/XPR Incidents and adds to Horizon NDR’s native Behavioral Analytics AI engines. This allows the incidents to be contextually visualized using all of Horizon NDR’s advanced threat visualization capabilities.



4. In addition, Horizon NDR allows you to pivot back to Horizon XDR/XPR for ThreatCloud and Open Source investigation.



# Appendix C – Known Limitations

- Horizon NDR dedicated sensors must support Check Point Gaia R81.10 or R81.20. This currently excludes:
  - Quantum Spark SMB appliances (Embedded Gaia)
- Threat Extraction and Zero Phishing results are not included in the Security Checkup reports.
- Cluster is not supported for dedicated NDR sensors.
- Note: <https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-limits.html>. In particular, some non-Nitro EC2 instance types are not supported by AWS traffic mirroring.