PROFESSIONAL SERVICES

HARMONY ENDPOINT HEALTH CHECK REPORT

SAMPLE

CHECK POINT™
PROFESSIONAL SERVICES
Consult • Design • Deploy • Operate • Optimize

CHECK POINT™
YOU DESERVE THE BEST SECURITY

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
CONTROL CHANGE 3
ABBREVIATIONS 4
SERVER INFORMATION 5
LICENSE INFORMATION 5
INTRODUCTION 6
RECOMMENDATIONS AND BEST PRACTICES 7
BLADES 10
- FULL DISK ENCRYPTION 10
- MEDIA ENCRYPTION AND PORT PROTECTION 11
- ANTI-MALWARE 11
- SANDBLAST AGENT ANTI-RANSOMWARE, BEHAVIORAL GUARD AND FORENSICS. 13
- SANDBLAST AGENT ANTI-BOT 15
- THREAT EXTRACTION, EMULATION AND ANTI-EXPLOIT 17
- ANTI-EXPLOIT ENGINE 20
- FIREWALL 21
- APPLICATION CONTROL / URL FILTERING 22
- VIRTUAL GROUPS BEST PRACTICES 23

POLICY CONFIGURATION BEST PRACTICES 24
SYSTEM HEALTHCHECK 25
APPENDIX 1 – RELATED SK 27
APPENDIX 2 – DOCUMENTATION 27
CONCLUSION 28

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

EXECUTIVE SUMMARY

The following document summarizes the information collected from up to two (2) Harmony Endpoint Server(s). The project took place between [**date - begin**] and [**date - end**] .

The project examined the deployment of your Harmony solution and identified opportunities to optimize your Endpoint Security Management System.

Each recommendation is rated as follow:

❌	Serious	Needs immediate attention.
❗	Attention	Needs attention.
✅	Good	No need for any action.

CONTROL CHANGE

Version	Date	Description	Author
Initial	19/01/2022	Initial Document	John Smith (Check Point)

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

ABBREVIATIONS

The following table contain the abbreviations would be utilized on this document.

ABBREVIATION	DEFINITION
PS	Professional Services
GUI	Graphical User Interface
SG	Security Gateway
VAP	Virtual Application Processor
VSX	Virtual Network Extender
VS	Virtual System
SMS	Security Management Server
SO	Smart Optimize

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

Check Point
Harmony
Highest Level of Security for Remote Users

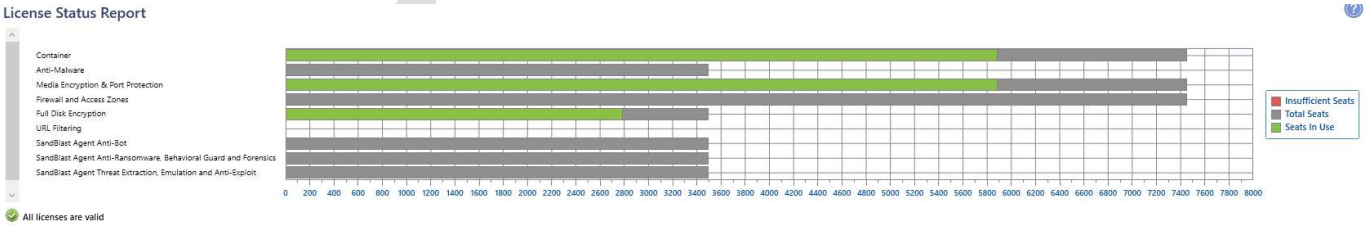
MOBILE EMAIL & OFFICE CONNECT (SASE) BROWSER

SERVER INFORMATION

HOSTNAME	STATUS	VERSION	OS	SW BLADES	REMEDIATION
EPSRV01	⚠	R80.40	Gaia	• Anti-Malware • Media Encryption & Port Protection • Firewall and Access Zones • Full Disk Encryption • SandBlast Agent Anti-Bot • SandBlast Agent Anti-Ransomware, Behavioral Guard and Forensics • SandBlast Agent Threat Extraction, Emulation and Anti-Exploit	Upgrade to R81.10 version

LICENSE INFORMATION

	STATUS	COUNT	PERCENT	REMEDIATION
Total of Endpoint Seats	✓	5884 / 7450	78%	N/A



SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

INTRODUCTION

[COMPANY_NAME] has deployed Check Point Endpoint Security to (#) endpoints throughout their organization.

HARDWARE	NAME	VERSION	FIXES	CPU	RAM
VM	EPSRV01	R80.40	N/A	8 Cores	32 GB

ENVIRONMENT

Note: This is an example of the basic Environment and below the details

- Clients communicate with the Management Server over HTTP/HTTPs.
- The Endpoint Management architecture works in a "star" scheme to support large-scale environments.
- The central "brain" of the system is the "Management Server" and the delegate servers are named "Policy Servers".
- Each Management Server can support a maximum of ~10,000 endpoints. Multiple Policy Servers can be chained to support a management of up to 400,000 devices from a single environment.
- The environment supports unified log reporting through SmartLog.

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

RECOMMENDATIONS AND BEST PRACTICES

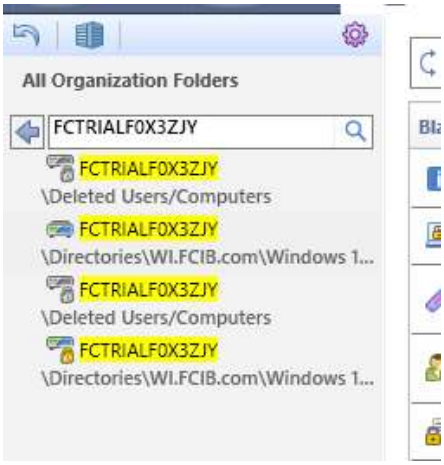
- Check Point recommends that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks. The last version that we have seen working good is **R81** and the recommended Take is the GA, at this moment it is the **Take: 44**.

- It is best practice and recommended to thoroughly test the latest recommended Harmony Endpoint client version before deploying to production machines. The latest recommended version can be found on the Endpoint Security Homepage, sk117536.

- The release notes for the specific client version should be reviewed carefully to ensure the Harmony Endpoint client and blades are deployed to supported client machines. The current recommended Harmony Endpoint client for Windows is **E86.20**, see E86.20 Endpoint Security Client for Windows Release Notes.

- Create Virtual Group for staging and troubleshooting purposes.

  Example: The 2 greyed objects below can be safely deleted to release Endpoint Containers license.



©2022 Check Point Software Technologies Ltd. All rights reserved 2022

- Detected 700 devices with object duplicated, consider delete the duplicated objects.

```
4,FCTRIALF0X3ZJY
4,FCTRIADJ05L20J
4,FCTRIADJ04AWCB
4,FCSKNALF0Y2J04
4,FCJAMADJ04LN78
4,FCIBANTINS001
4,FCBARADJ07CMKE
4,FCBAHALF162ZFY
4,FCBAH7D2VL8X
3,W9140349E9L
3,W90670KEU9
3,W7996WVHEV
3,FCTRIALF1CE0DT
3,FCTRIALF0X3JQ5
3,FCTRIALF0PXSNA
3,FCTRIALC04BHQV
3,FCTRIALC00Z8GR
3,FCTRIADJ07LZ27
3,FCTRIADJ07LZ21
3,FCTRIADJ05L201
3,FCTRIADJ04AWCC
3,FCSTLALF0ZRL6F
3,FCSTLALF0ZRFP7
3,FCSTLADJ07CPX5
3,FCSTL7DJ02BQN0
3,FCSKNADJ07CQ8Y
3,FCSKNADJ07CQ8Q
3,FCSKNADJ07CNKV
3,FCSKNADJ07CNJJ
3,FCSKNADJ05L1SR
3,FCSKN7DJ04LNC3
3,FCSKN7DJ02BQLL
3,FCJAM_LXRHZDL
3,FCJAMALF255QGR
3,FCJAMADJ0BLG76
3,FCJAMADJ07YDVV
3,FCIBCAYINS001
3,FCCUR_L9L2JQL
3,FCCURADJ05L24H
```

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

- Review the following list of Endpoint devices with licenses and no connectivity to Endpoint server for more than 30 days:

- Consider select the option reset data on object to release license.

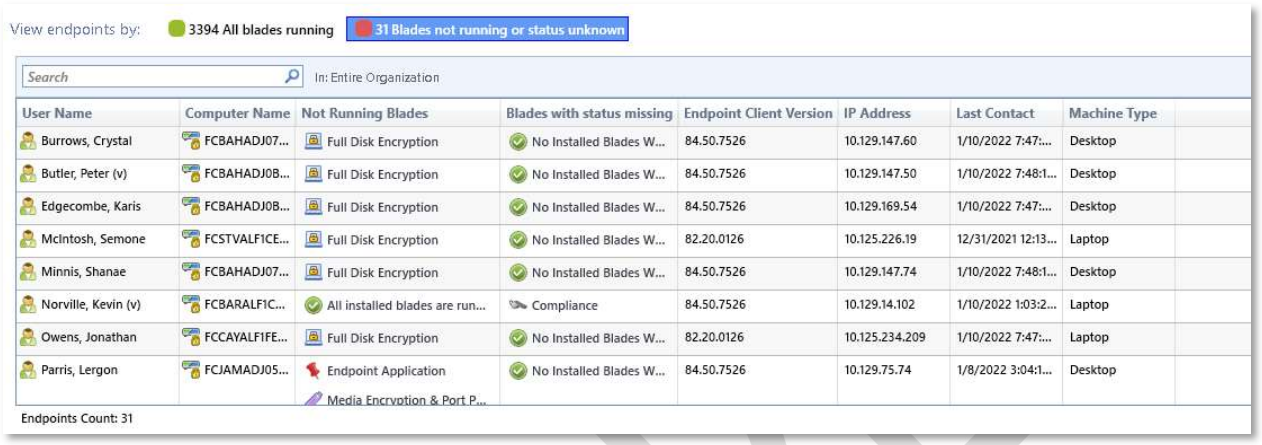
```
                nid                 |                                  distinguished_name
------------------------------------+-------------------------------------------------------------------------------------
e5f5e588-93e2-3c42-af1a-4253dc18e42e | CN=FCBARADJ05L1R5,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
e4f84447-36fb-46f5-8f6d-cbd666a1d597 | CN=FCIBANTINS001,CN=Computers,DC=WI,DC=FCIB,DC=com
f62d5bc0-f479-4b5b-b59f-d1cdc015eaa0 | CN=FCCAYADJ07N0NS,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
f5a16ef4-5595-9c40-ae2d-9c5df0810836 | CN=FCANTADJ05L1YY,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
06d82713-4788-4a45-ba92-d82f3820bfbb | CN=FCGRE_L0Z8GYL,FN=deleted
b26a23f6-c48f-47f3-8859-a402557275a6 | CN=W92700KENL,FN=deleted
a5b5187b-f9e5-4aeb-b5a6-835b3c0a3e40 | CN=FCJAMADJ04LNEM,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
946ba15b-d2ef-40fa-80ee-5b8b6296a28f | CN=FCBAR7LC0AKNZ3,FN=deleted
992f6572-811f-4277-adae-68731367ba92 | CN=FCBAR7DJ04LND0,FN=deleted
a7ca6649-d3e5-d941-aa95-7e9839290aec | CN=FCBAH_LXEBBDL,FN=deleted
70ebee1c-18cc-b342-bb2e-ef550c499566 | CN=FCBAHALFVY5N7,CN=Computers,DC=WI,DC=FCIB,DC=com
ae824222-4648-6645-b29a-114df4eec796 | CN=FCCAYADJ078AM3,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
f6a1fd7d-889a-d440-9bfd-3204a34cdd62 | CN=FCBARADJ072956,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
e3b54d49-3823-406e-bd25-dd839a1ec346 |
220491dc-87ab-42af-9b11-8be43bf954c0 | CN=FCBARADJ72FMF,CN=Computers,DC=WI,DC=FCIB,DC=com
9eea94b6-89a9-4b6a-9cd5-40b9d88cd200 | CN=FCBAHALF1VYDCP,OU=Laptops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
a429a5d2-922d-4643-81d0-c61a3c98b205 |
ff22e0fd-46e2-4bbe-ab88-8865f9a51deb | CN=FCBAH7D2VL8X,FN=deleted
683c163f-fb05-f349-a33d-98f268ffc797 | CN=FCJAMADJ0BLG4P,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
52fe92f1-2d0e-f34a-8dc8-94d0d7e6de42 | CN=FCJAMADJ0BLG2F,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
a4447ff0-fa98-4c25-a92a-870598598a02 |
5551a459-e297-4403-8b65-1f987b3c990a | CN=FCSTV_L0YVHTL,FN=deleted
181020ec-f2ad-4032-a87b-e148a482abeb | CN=FCBARALF0PXQFR,OU=Proof Machines,OU=XPMachines,DC=WI,DC=FCIB,DC=com
97db2f59-1d7e-1047-b9b7-9fd44a73fa7b | CN=FCBAHADJ07YDAC,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
0dc3c6e1-6a81-4e37-b388-b0e3d7a8ba99 | CN=FCCAYADJ07MZUH,OU=Desktops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
45328588-cfce-4a58-9200-21c3dbd91e1a |
f8352c0b-e4c2-4d46-a7ac-0c5212ae14a7 |
4c10f311-af49-4062-acad-c09cce76da07 |
b89c8b62-4592-6340-bb98-0c16d549cdc8 | CN=FCJAMALF1WK3X5,OU=Laptops,OU=Windows 10 Machines,DC=WI,DC=FCIB,DC=com
(599 rows)

 (599 rows)
```

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

BLADES

There are 31 Endpoint clients no reporting status of software blades or state unknown.



This cloud be a general error, in order to fix the status of the clients to make sure they are protected, validate if process are running in the background, and connectivity to Endpoint Management Server, if the problem persist, consider re-install Endpoint software. The status of Endpoint client can be remoted validated using windows registry values, see sk105818.

FULL DISK ENCRYPTION

For Check Point Full Disk Encryption Preboot is recommended to associate a global account for machine access and decryption besides the current Preboot user, this could be used for troubleshooting and device decommission.

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

MEDIA ENCRYPTION AND PORT PROTECTION

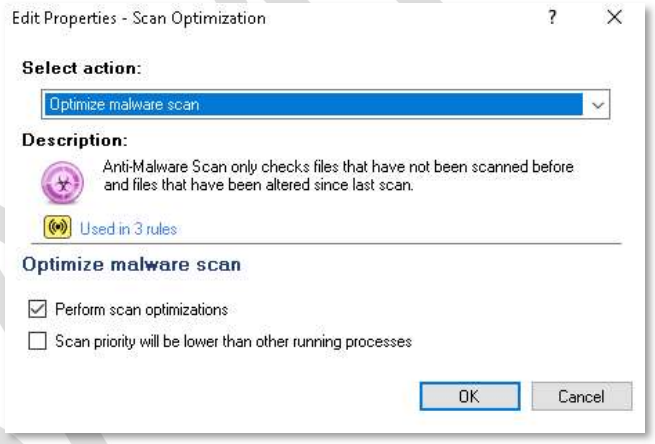
1. Comment rule #1 and #5 (offline), and rule #1, #3, #4, #5, #7 (online) for audit and compliance purposes.

2. For client upgrade is highly recommended test the following before (crashes of MEPP driver MeDlpFlt reported on E86.01, solved on E86.10):

    a. Encrypt device USB or HDD with E84.50.
    b. Test upgrade to E86.20.
    c. Validate the USB encrypted, the user should access to data.

ANTI-MALWARE

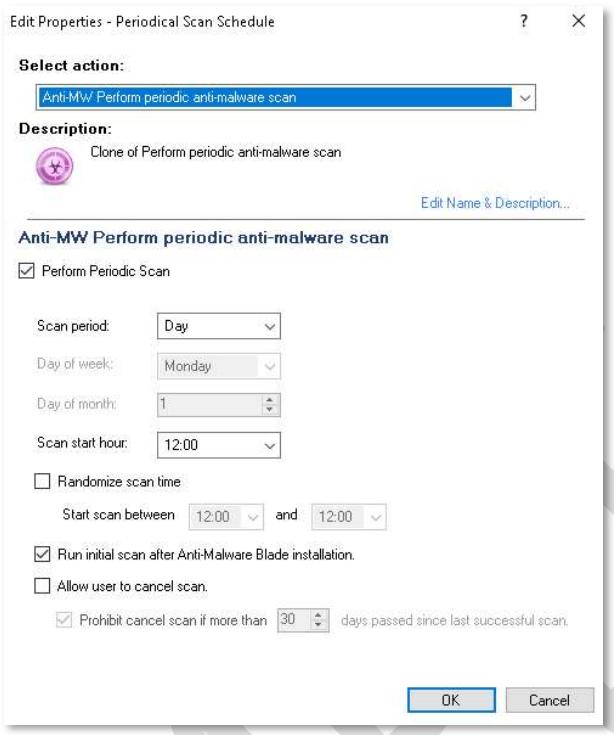
Under the Anti-Malware blade Scan Optimization action "*Scan priority will be lower than other running process*" should be checked if there are performance issues with the Anti-Malware blade.



Any 3rd party Anti-Malware solution should be disabled on all machines before deploying the Endpoint Security Client. Select Randomize scan time to make sure that not all computers do a scan for malware at the same time. This makes sure that network performance is not affected by many simultaneous scans. In Start scan between, specify the time range during which the scan can start.

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022



Exclusion area: Exclusion locations could be where the application is installed as well as any cache folders used by the application. This is assuming that the application doesn't dump or export any files into these folders that could have the chance of being malicious.

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

SANDBLAST AGENT ANTI-RANSOMWARE, BEHAVIORAL GUARD AND FORENSICS.

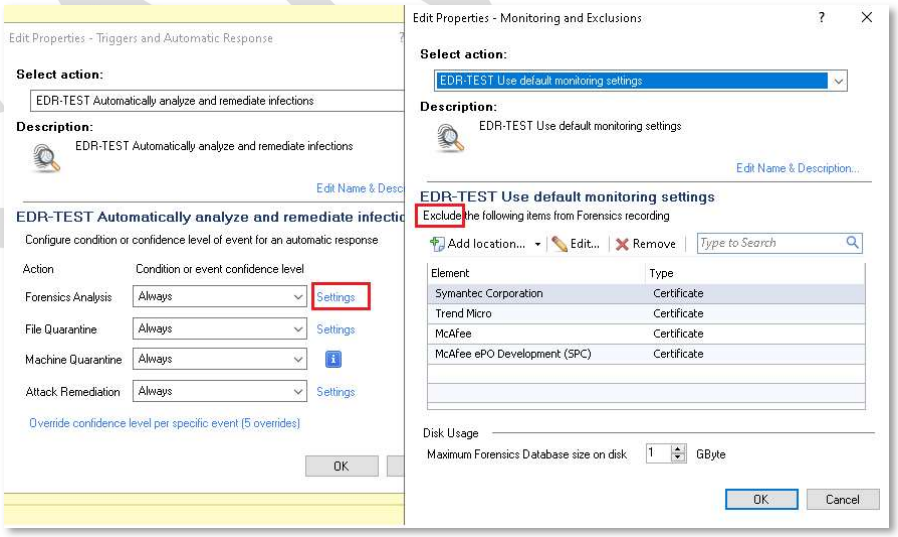
Anti-Ransomware, Behavior Guard and Forensics Blade Overview:

Anti-Ransomware is an automated process that can take point in time backups of user file data as an executable is trying to read and write to the file system. The process creates honeypot folders and creates a vaulted folder where the backup files are stored and are only readable by the Check Point system account.

Behavior Guard uses real-time dynamic analysis to determine what an executable is trying to do and if it resembles a malware family. BG looks for zero-day behaviors and with the help of other blades stops threats in real-time.

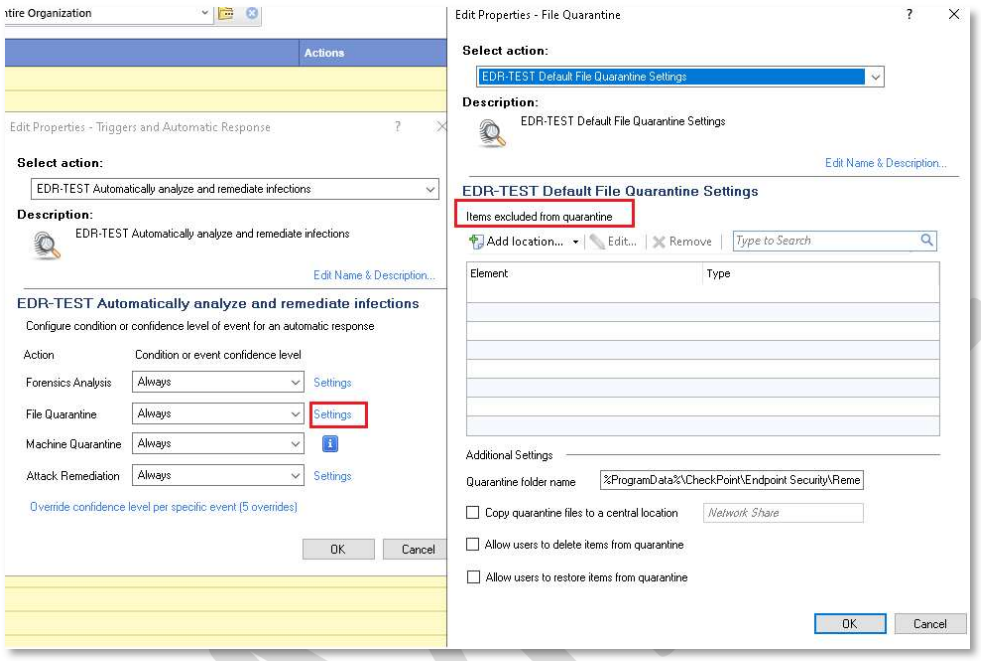
Forensics helps from an EDR perspective by having a process running to monitor and log what executables do so that in the case of an event, the end-user or admin can see a forensics report and save precious time to try to figure out what happened.

The Forensics Analysis engine takes up the bulk of resources used by the Sandblast Agent client. This engine runs in the background collecting data in real-time. This process may slow down individual applications. Therefore, as a best practice, we are looking specifically for applications that have a lot of I/O and thrashing of disks. Once you have tested and determined the applications that are affected and deemed safe, it is recommended to add the application, the folder installation and any cache folders to the exclusion area:



©2022 Check Point Software Technologies Ltd. All rights reserved 2022

The above image displays where you would input the exclusions for Forensics Analysis. Be 100% certain that whatever you exclude is deemed clean and secure. It is a best practice to provide the full path to folders and executables. The primary reason to exclude an application here is due to the performance degradation of the application.



SAMPLE

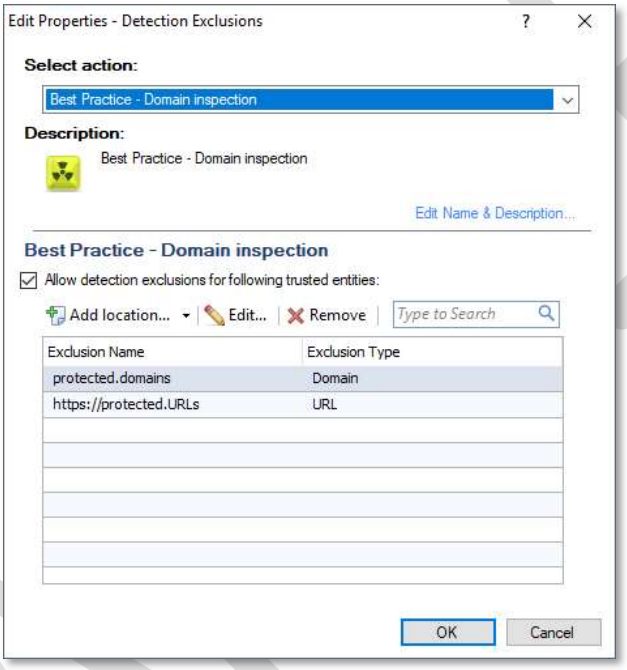
©2022 Check Point Software Technologies Ltd. All rights reserved 2022

SANDBLAST AGENT ANTI-BOT

The purpose of this blade is to monitor network traffic to see if it is reaching out to Command and Control centers for instructions on how to pull down malicious code and other instructions.

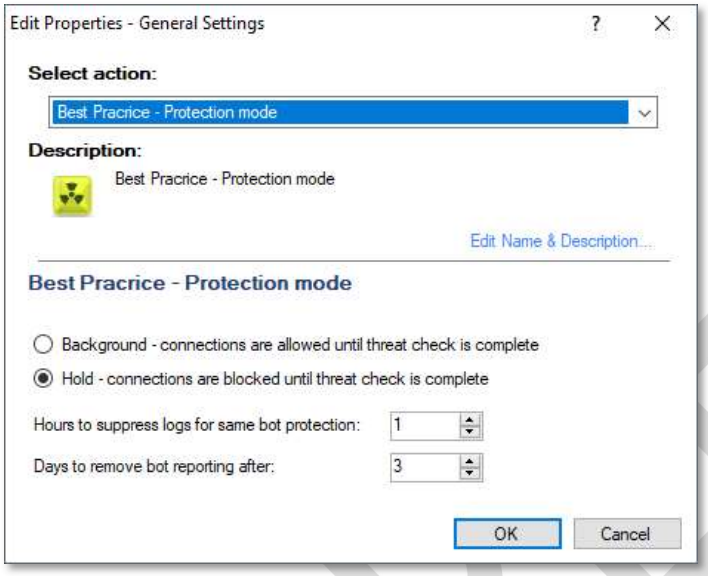
Best Practice configuration

Exclude trust domains:



©2022 Check Point Software Technologies Ltd. All rights reserved 2022

The anti-bot engine should set to hold after testing applications and operation functionality:



SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

THREAT EXTRACTION, EMULATION AND ANTI-EXPLOIT

Threat Extraction, Emulation and Anti-Exploit Overview:

This multi-purpose blade is responsible for 0-day protection around file downloads from the web as well as when files are written to disk. It also monitors and does further inspection around the most vulnerable applications with Anti-exploit.

Threat Extraction is the ability to strip out any live content that could be exploited and very quickly deliver a sanitized copy to the end user right away. This feature only works with the Browser plugin.

Threat Emulation can run with the browser plugin as pre-download protection, and it also can run in the background when a supported file is written to the hard disk.

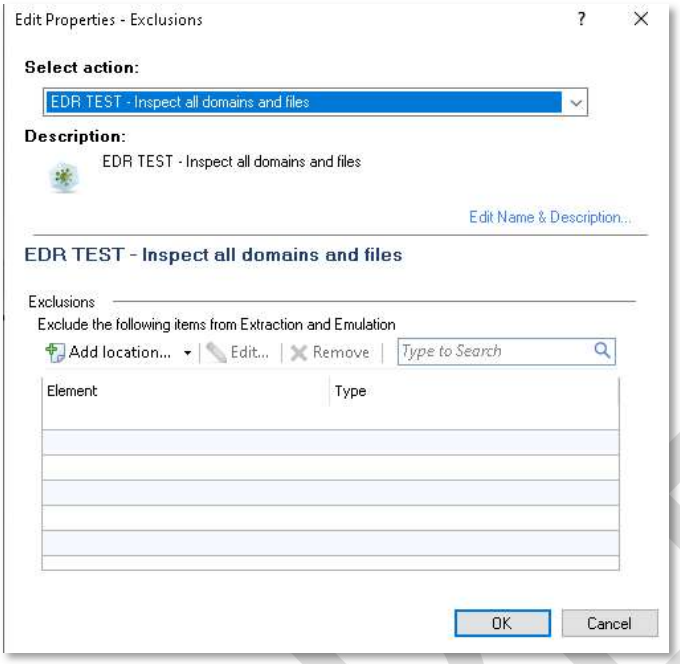
Anti-Exploit performs additional inspection around the most vulnerable applications like Microsoft Office, Internet Explorer, Edge, Flash, RDP, Java, etc.

Best Practice configuration

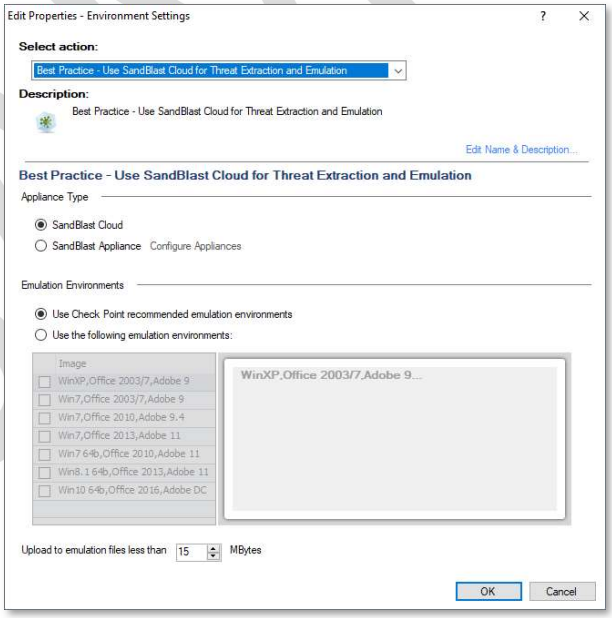
There is the option under exclusions to add locations and folders of applications you deem to be safe. Only put exclusions of applications you know to be safe. We are only emulating file types that are supported by Threat Emulation. An example would be an application that generates dozens of PDF files on a hard disk. These files being generated on the server, should not introduce a security risk and may not need to be emulated:

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022



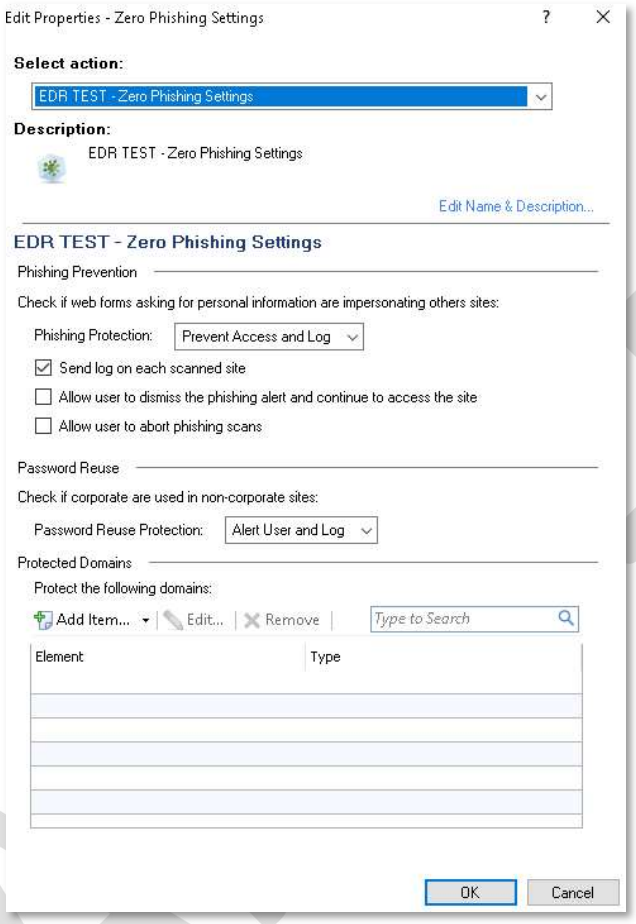
The Threat emulation engine should use the threat cloud engine unless the local TE appliance exists on Check Point architecture:



SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

Zero Phishing and Password Reuse are included in the Browser plugin. It is assumed that admins are not accessing the internet or inputting passwords on a web browser on a server, to make this feature works properly, configure your company domain into the *Protected Domains* section:

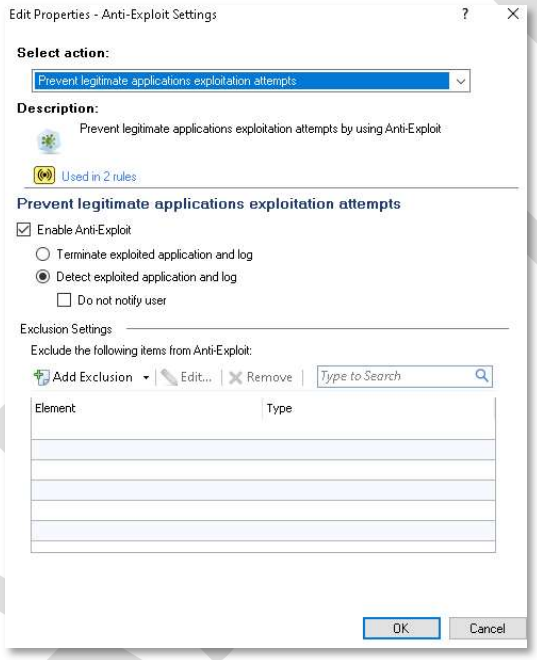


©2022 Check Point Software Technologies Ltd. All rights reserved 2022

ANTI-EXPLOIT ENGINE

The Anti-exploit engine further evaluates the most vulnerable applications that are highly exploitable. This includes internet explorer, java, flash, and office as well as new protections around the remote desktop protocol; this is recommended especially for Windows Servers.

Test applications functionality, and you can add exceptions for false positive if exists:



SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

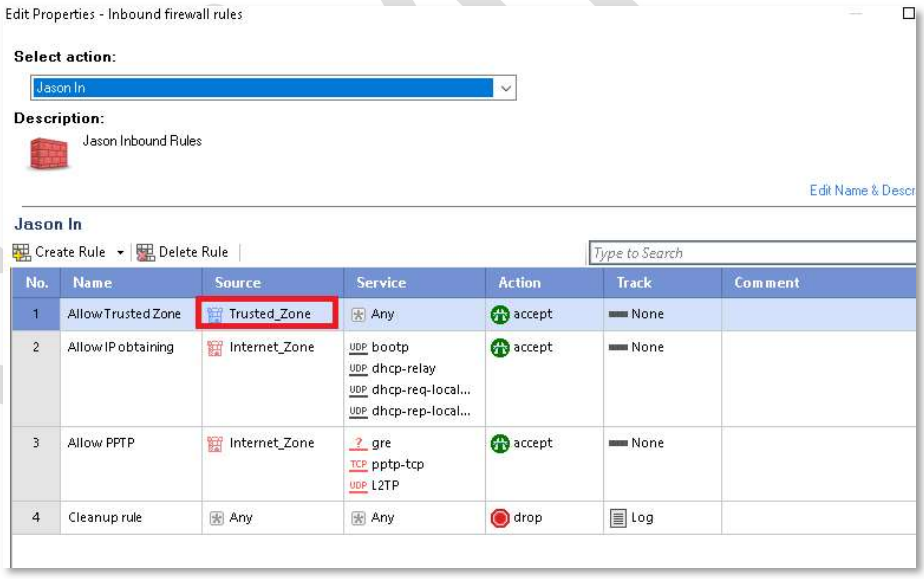
FIREWALL

Endpoint Security client installation disabled Windows Defender Firewall, using Microsoft's "wscsvc" service.

For the latest windows updates according to Microsoft there is the absence of "wscsvc" service, or AD GPO can disable the option to turn off Windows Defender Firewall, for these cases, Windows Defender Firewall should be disabled on all machines before deploying the Endpoint Security Client.

Only one custom Firewall rule exists:

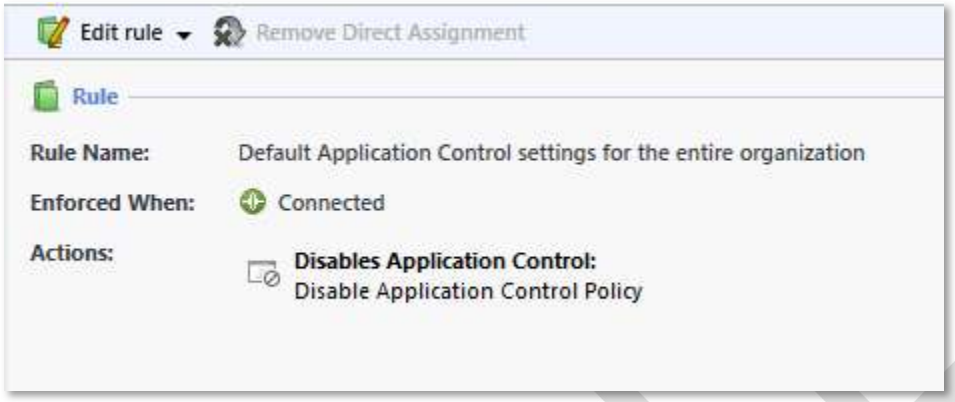
Consider configure Trusted Zones with CIBC's trusted network to allow network inbound traffic for support or user machine monitoring:



©2022 Check Point Software Technologies Ltd. All rights reserved 2022

APPLICATION CONTROL / URL FILTERING

This is disabled currently:



SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

Check Point
Harmony
Highest Level of Security for Remote Users
MOBILE EMAIL & OFFICE CONNECT (SASE) BROWSER

VIRTUAL GROUPS BEST PRACTICES

In order to test new Operating Systems version and/or new Laptops/Desktops hardware, its recommended to create a separate Virtual Group, associate only the new endpoint devices and this allows to configure new policies parameters in a transparent way without impacting all the devices.

1. Create a Virtual Group named **Staging**
    a. This can be useful to test the New Harmony Endpoint client as well.

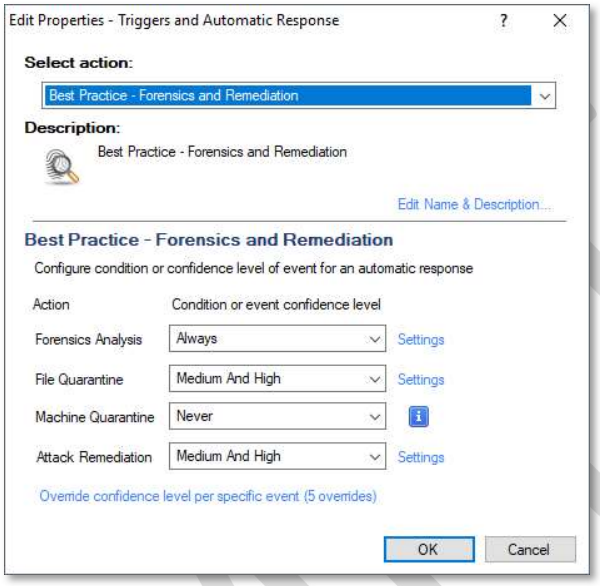
2. Create a Virtual Group **Troubleshooting**:
    a. Create a Troubleshooting rule in order to move (temporary) machines to disable features or modify the security policies, without affecting all devices associated with a rule.

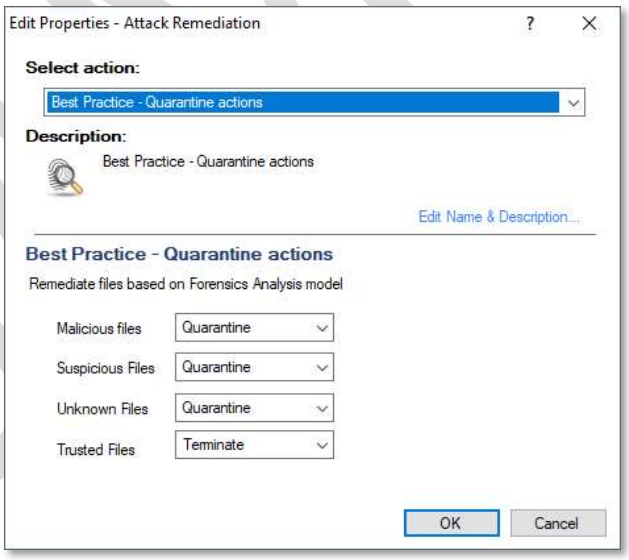
SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

POLICY CONFIGURATION BEST PRACTICES

The following configuration is part of the best practice configuration for Forensics and Remediation:





SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

SYSTEM HEALTHCHECK

System information:

Platform:	VMware Virtual Platform
Model:	Intel(R) Xeon(R) CPU E5-2650 v3
CPUs Total:	8
RAM Total (KB):	32726564

Known Issue found on /var/log/messages:

- Core dump file created for FWM process:

```
EPSRV01 kernel: fwm[9054]: segfault at 1c ip 00000000f381b1c0 sp 00000000ffd87a80 error 6 in libDataStruct.so[f37f2000+6d000]
```

Recommendation:

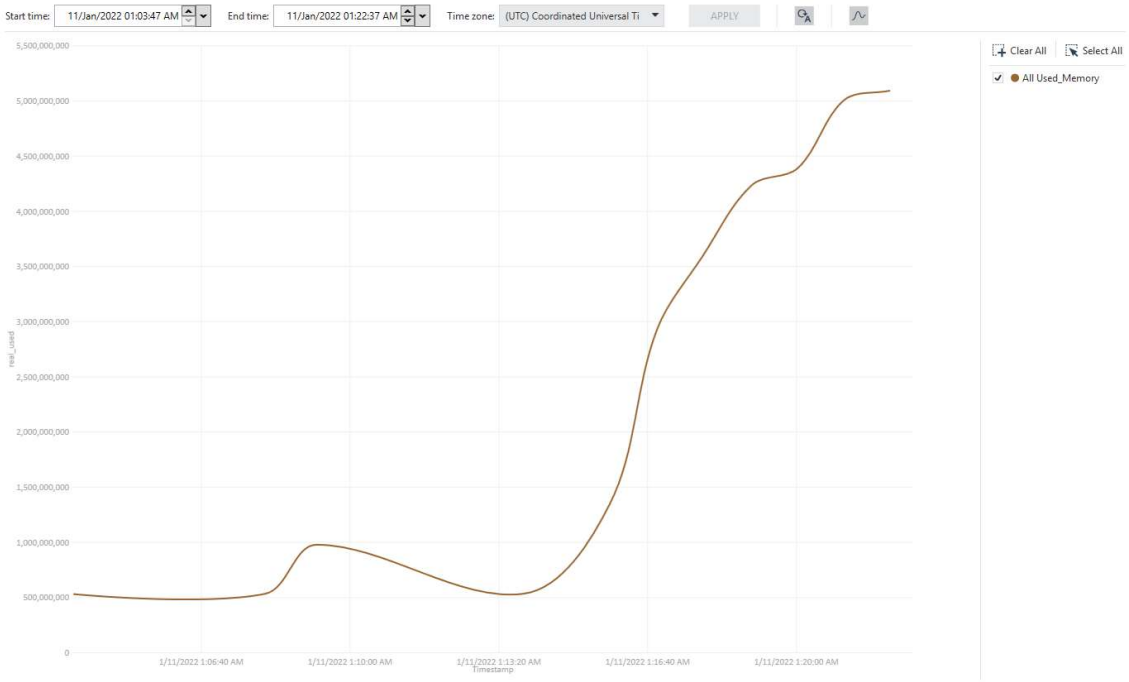
there are multiple fixes for FWM process on latest **R80.40 JHF take 139**:

PRJ-30883, PMTR-62059	Security Management	In rare scenarios, during an upgrade, the *FWM* process may unexpectedly exit with a core dump file.

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

- The RAM memory level usage is in a good state.



- Interface health in a good state, there are 0.04% of packet drop, so is not relevant or implies any issue for Endpoint Client communication:

```
eth0      Link encap:Ethernet  HWaddr 00:50:56:89:46:18
          inet addr:10.1.15.169  Bcast:10.1.15.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:204662 errors:0 dropped:0 overruns:0 frame:0
          TX packets:193411 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50052470 (47.7 MiB)  TX bytes:63718820 (60.7 MiB)
```

- Clean log files, the /var/log/partition reach 84%:

Filesystem	Type	Size	Used	Avail	Use%	Mounted on
/dev/mapper/vg_splat-lv_current	xfs	50G	18G	33G	36%	/
proc	proc	0	0	0	-	/proc
sysfs	sysfs	0	0	0	-	/sys
devpts	devpts	0	0	0	-	/dev/pts
/dev/sda1	ext3	291M	43M	233M	16%	/boot
tmpfs	tmpfs	16G	2.4M	16G	1%	/dev/shm
/dev/mapper/vg_splat-lv_log	xfs	30G	26G	5.0G	84%	/var/log
none	binfmt_misc	0	0	0	-	/proc/sys/fs/binfmt_misc

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

Check Point
Harmony
Highest Level of Security for Remote Users
MOBILE EMAIL & OFFICE CONNECT (SASE) BROWSER

APPENDIX 1 – RELATED SK

Endpoint Security Homepage - sk117536

SandBlast Agent Best Practice Configuration - sk154052

APPENDIX 2 – DOCUMENTATION

Harmony Endpoint Administration Guide

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

CONCLUSION

The general feedback is that the Check Point configuration is adequate but improvements must be made to reach the standard of "best practice". The steps below and in the supporting documentation will help [COMPANY_NAME] significantly.

The transformation could take several weeks of effort. Check Point Professional Services can support [COMPANY_NAME] through this transition and ensure that the Check Point installed products are optimally utilized.

On behalf of Check Point Professional Services, I would like to say thank you for being a loyal customer. It has been a pleasure supplying you with these observations. Should you have any questions please do not hesitate to reach out.

John Smith
Check Point Professional Services Consultant
jsmith@checkpoint.com

Report Completed on:

Friday, July 8, 2022

SAMPLE

©2022 Check Point Software Technologies Ltd. All rights reserved 2022

Check Point

Harmony

Highest Level of Security for Remote Users

ENDPOINT MOBILE EMAIL & OFFICE CONNECT (SASE) BROWSER

Worldwide Headquarters
5 Ha'Solelim 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; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

CHECK POINT™

YOU DESERVE THE BEST SECURITY

©2022 Check Point Software Technologies Ltd. All rights reserved 2022