CHECK POINT™

Harmony End Point – Packing a Punch in 2024

In the details – What new in HEP 2024

Jonny Rabinowitz, Product Manager Harmony End Point

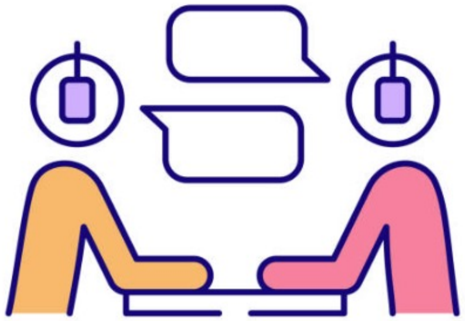
22nd May 2024

YOU DESERVE THE BEST SECURITY

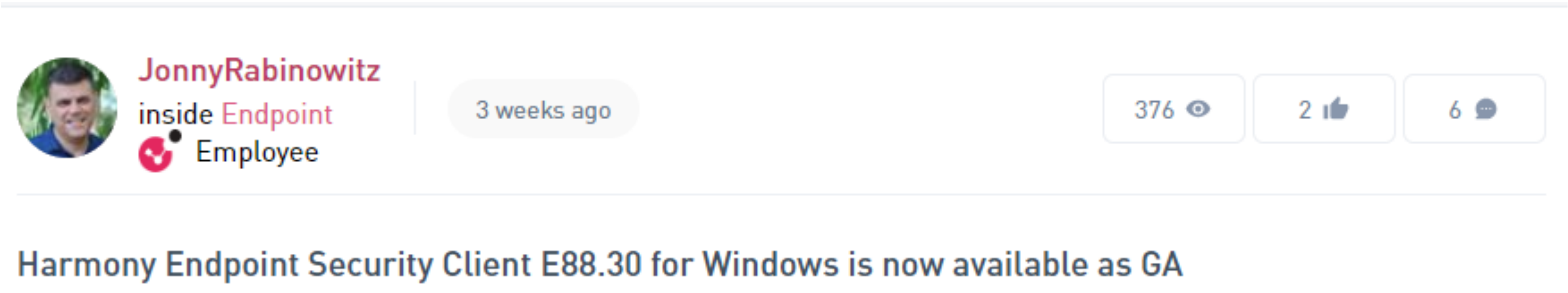
Agenda

- Opening remarks
- Management Server
- Client releases
  - Windows
  - Linux
  - Mac

Shout Out To Check Mates



- Thanks for hosting!!
- Post details of all releases and significant features
- Product Managers do their best to follow Check Mates and respond



JonnyRabinowitz
inside Endpoint
Employee

3 weeks ago

376 | 2 | 6

Harmony Endpoint Security Client E88.30 for Windows is now available as GA

This is Not a Roadmap Session

- Content includes
  - Released content RELEASED
  - Planned (*) PLANNED
  - EA (Early Availability) EA

Goals

- Not talk about features have heard before

- Measure of success
  - Learn something new!!

Releases and Features

- Latest Release: E88.30
  - Latest security capabilities
  - Most details out of scope
- Recommended Release: E87.62
  - Assess deployment KPIs
- Extended Support: E86.60
- All GA releases fully supported (within the defined timeframes)

1

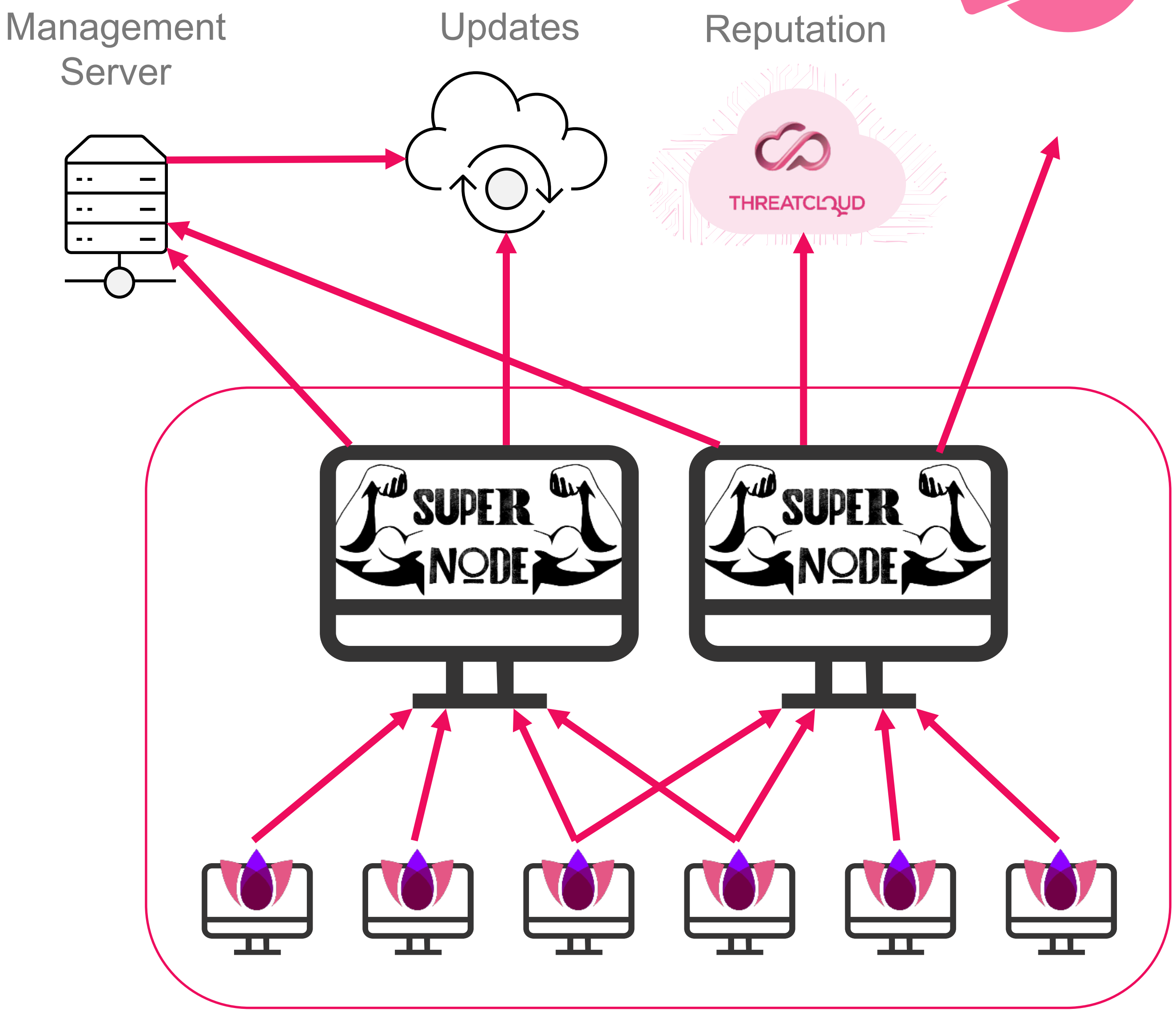
Server

- Semi Isolated Networks
- Licensing
- CPInfo to S3
- Notifications and Alerts

Semi-Isolated Networks (1)

EA: E88.20

- Additional Deployment Option
  - ✓ On premise management
  - ✓ Cloud management
  - + Semi- isolated
- Extend Super Node capability
  - Anti-Malware signatures
  - Behavioral Guard rules
  - Static Analysis ML/AI models
  - Client updates
- Added
  - Proxy all client connections on Windows
  - H2: VM/PM Support
    - Posture Management Patching
    - Super-Node – Centralized Patches



Semi-Isolated Networks (2)

- Use cases
  - ✓ Lower bandwidth consumption
    - ✓ Static data caching
  - ✓ Enables Connectivity to cloud management
    - ✓ Client isolation
    - ✓ Enables additional cloud-based use cases
  - ✓ Can also be used in network subset
    - ✓ Focus on Windows servers and Linux
- Ease of management EA PLANNED
  - Single Windows-based super node supports Windows, Linux and Mac
- Increased number of concurrent sessions EA
- Planned: Enhanced Super Node status monitoring PLANNED

Licensing

- What happens if I have mixed set of license types (Data / Basic / Extended)?
  - Match in order according to the level of the license
  - Try to assign the blade to the license with the lowest level that contains this blade
    - if there is no place for this blade in this license, then try next license by order
  - Dynamically adjusted as new capabilities are enabled

RELEASED

- License Pools

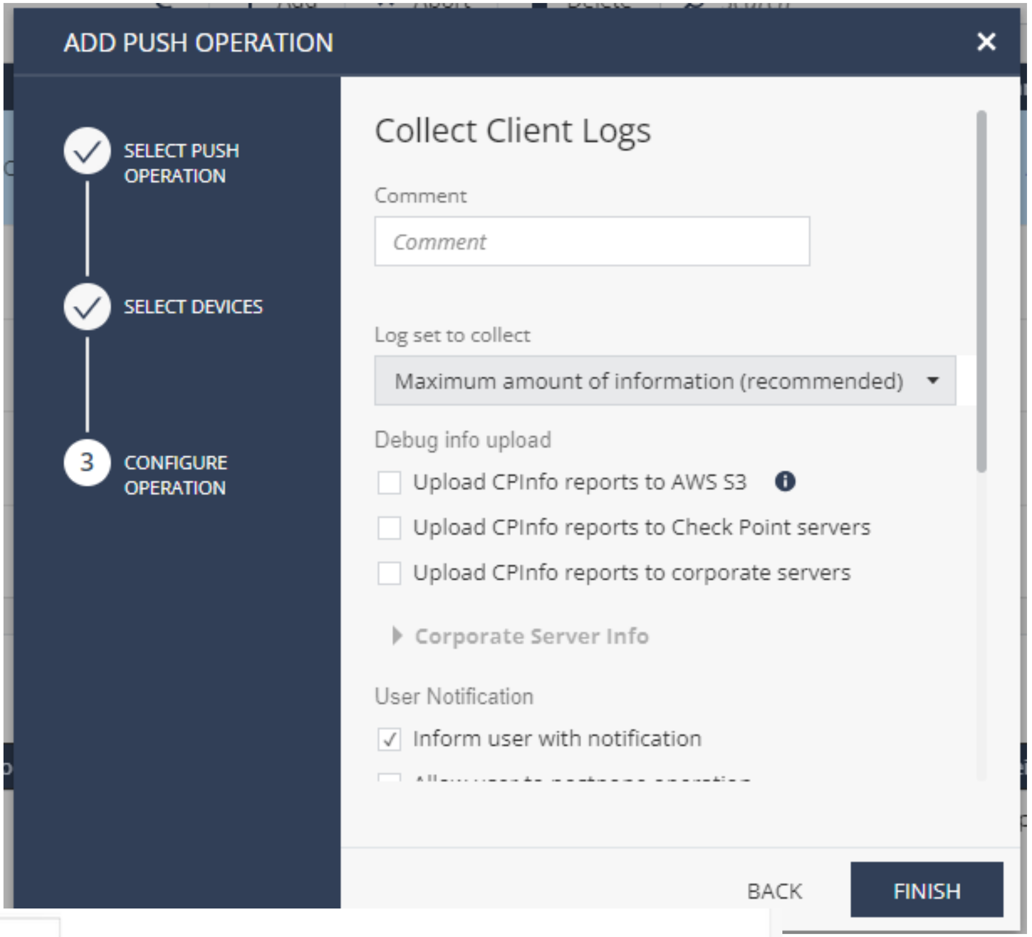
PLANNED

  - Single pool of licenses allocated to all tenants in an MSSP

RELEASED

Log Collection / CPInfo to S3

- Currently Windows only
  - Minimum release: E88.30
- Immediate collection
  - Cannot be scheduled or postponed
- The logs are saved in an S3 bucket based on the tenant location
- Log can be downloaded from UI by anyone with access to Push Operations



ADD PUSH OPERATION

1. SELECT PUSH OPERATION
2. SELECT DEVICES
3. CONFIGURE OPERATION

Collect Client Logs

Comment: Comment

Log set to collect: Maximum amount of information (recommended)

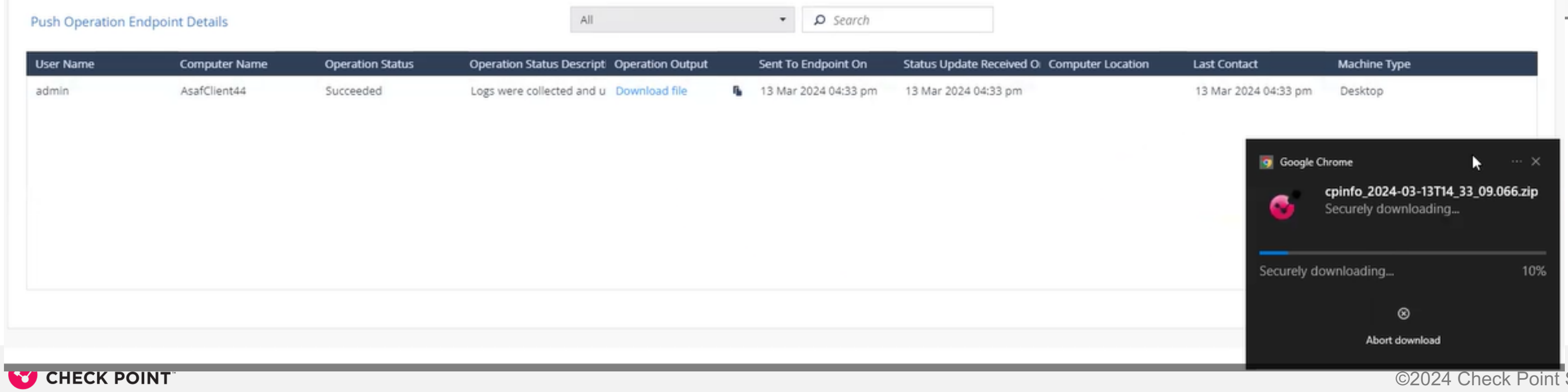
Debug info upload

- □ Upload CPInfo reports to AWS S3
- □ Upload CPInfo reports to Check Point servers
- □ Upload CPInfo reports to corporate servers

Corporate Server Info

User Notification

- ☑ Inform user with notification



Push Operation Endpoint Details

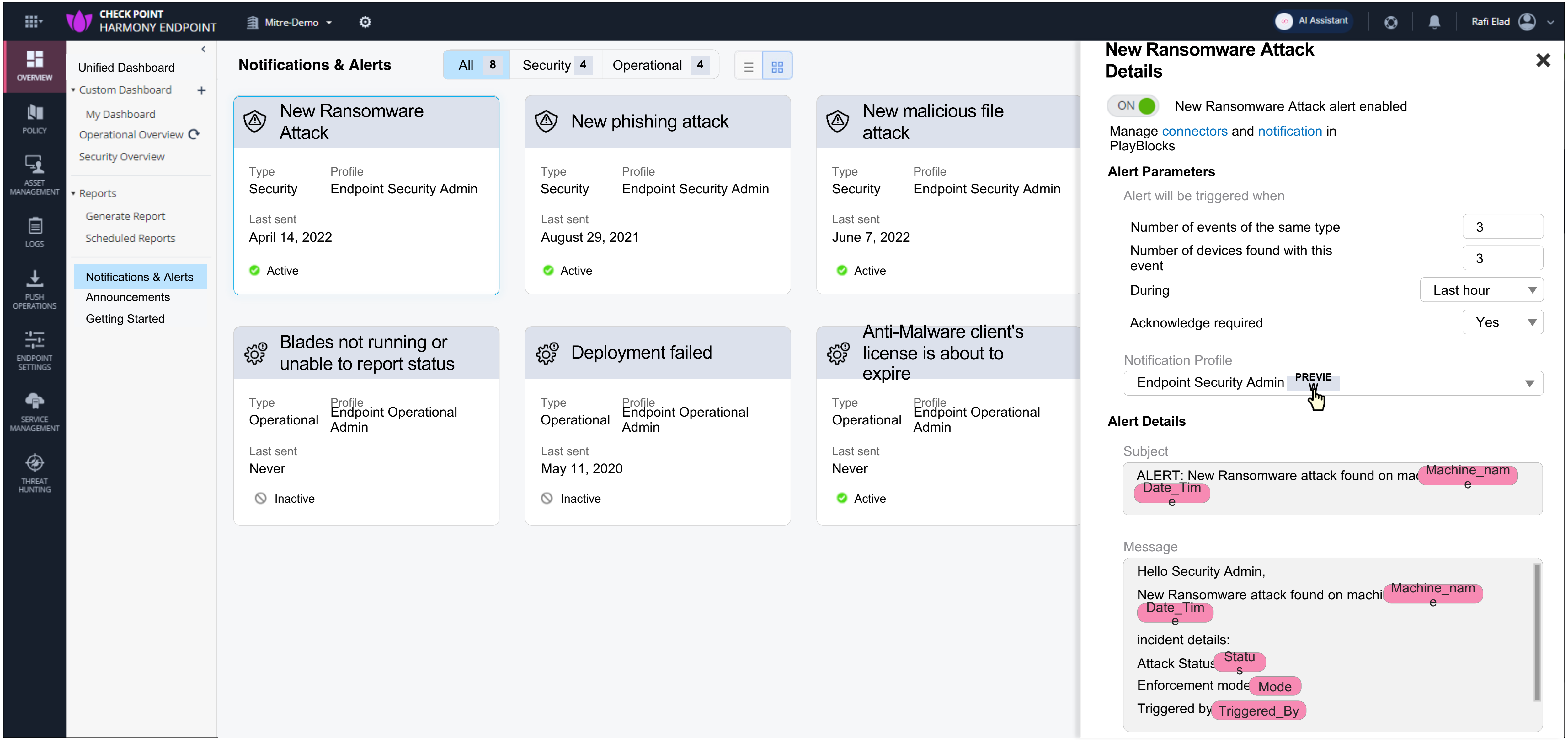
User Name	Computer Name	Operation Status	Operation Status Descript	Operation Output	Sent To Endpoint On	Status Update Received O	Computer Location	Last Contact	Machine Type
admin	AsafClient44	Succeeded	Logs were collected and u	Download file	13 Mar 2024 04:33 pm	13 Mar 2024 04:33 pm		13 Mar 2024 04:33 pm	Desktop

Google Chrome

cpinfo_2024-03-13T14_33_09.066.zip
Securely downloading...

Securely downloading... 10%

Notifications and Alerts



Notifications & Alerts

All 8 | Security 4 | Operational 4

New Ransomware Attack

Type: Security
Profile: Endpoint Security Admin
Last sent: April 14, 2022
Active

New phishing attack

Type: Security
Profile: Endpoint Security Admin
Last sent: August 29, 2021
Active

New malicious file attack

Type: Security
Profile: Endpoint Security Admin
Last sent: June 7, 2022
Active

Blades not running or unable to report status

Type: Operational
Profile: Endpoint Operational Admin
Last sent: Never
Inactive

Deployment failed

Type: Operational
Profile: Endpoint Operational Admin
Last sent: May 11, 2020
Inactive

Anti-Malware client's license is about to expire

Type: Operational
Profile: Endpoint Operational Admin
Last sent: Never
Active

New Ransomware Attack Details

ON New Ransomware Attack alert enabled

Manage connectors and notification in PlayBlocks

Alert Parameters

Alert will be triggered when

Number of events of the same type	3
Number of devices found with this event	3
During	Last hour
Acknowledge required	Yes

Notification Profile: Endpoint Security Admin PREVIEW

Alert Details

Subject

ALERT: New Ransomware attack found on mac Machine_name Date_Time

Message

Hello Security Admin,

New Ransomware attack found on machi Machine_name Date_Time

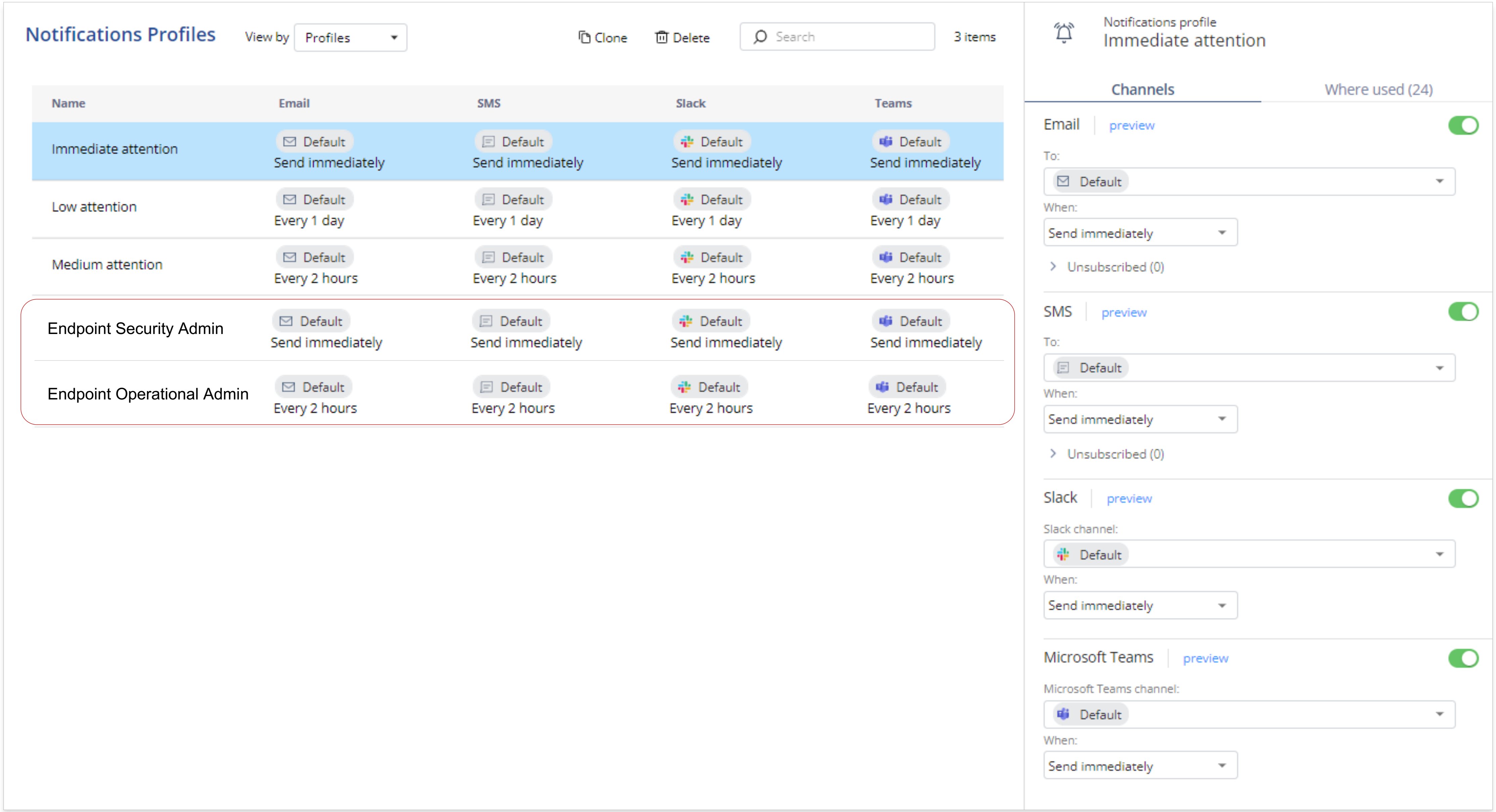
incident details:

Attack Status Status

Enforcement mode Mode

Triggered by Triggered_By

PlayBlocks – HEP Profiles



Notifications Profiles

View by: Profiles

Clone | Delete | Search | 3 items

Name	Email	SMS	Slack	Teams
Immediate attention	Default Send immediately	Default Send immediately	Default Send immediately	Default Send immediately
Low attention	Default Every 1 day	Default Every 1 day	Default Every 1 day	Default Every 1 day
Medium attention	Default Every 2 hours	Default Every 2 hours	Default Every 2 hours	Default Every 2 hours
Endpoint Security Admin	Default Send immediately	Default Send immediately	Default Send immediately	Default Send immediately
Endpoint Operational Admin	Default Every 2 hours	Default Every 2 hours	Default Every 2 hours	Default Every 2 hours

Notifications profile

Immediate attention

Channels | Where used (24)

Email | preview

To: Default

When: Send immediately

Unsubscribed (0)

SMS | preview

To: Default

When: Send immediately

Unsubscribed (0)

Slack | preview

Slack channel: Default

When: Send immediately

Microsoft Teams | preview

Microsoft Teams channel: Default

When: Send immediately

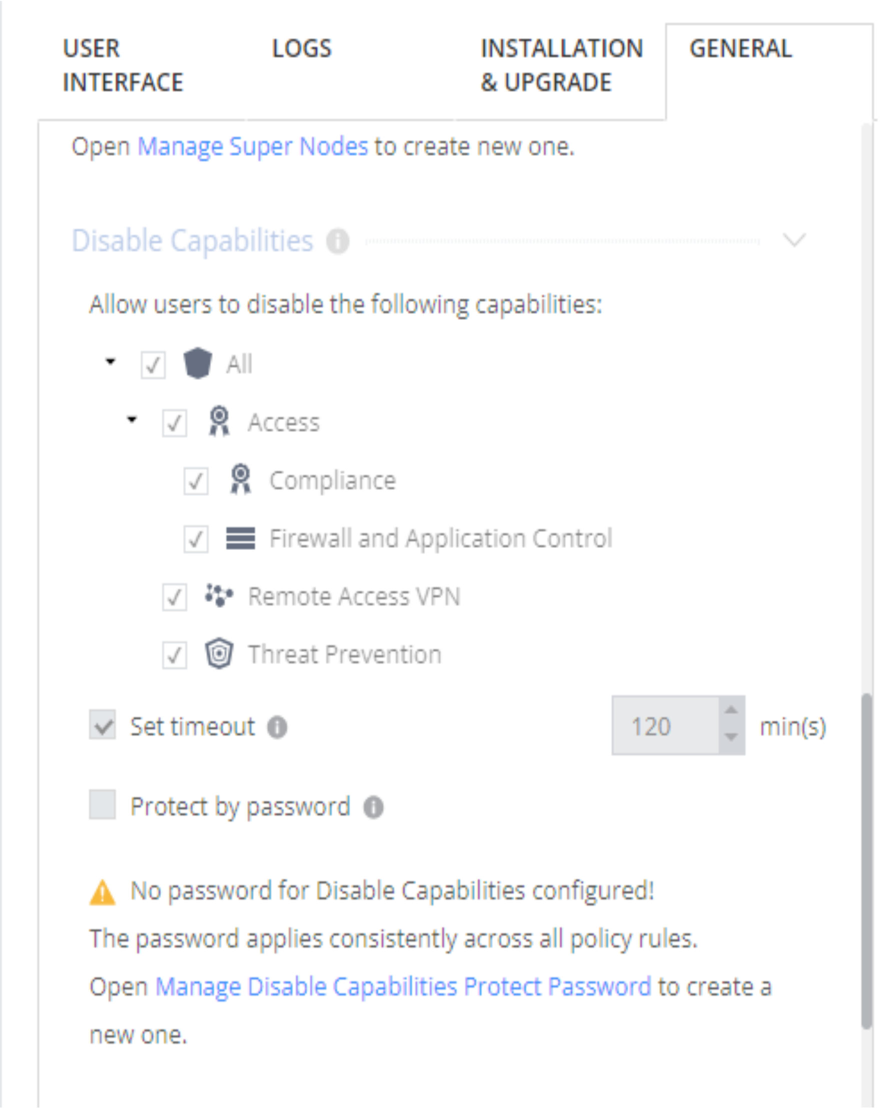
2

Windows Client

- Disable Capabilities Enhancements
- Client Language Settings
- Changes to Threat Emulation blade
- DNS Inspection Support

Disable Capabilities Enhancements

- Existing option to disable capabilities on a client
  - Available in Client Settings Policy – General
  - Useful to temporarily disable protection capabilities; for example, while performing IT operations at client
- Enhanced Control When Disabling
  - (Policy) Timeout interval after which capabilities are automatically reenabled
    - Fallback if not re-enabled manually
  - (Policy) Password Protection
    - Optional global setting of password to be entered before disable
      – Global setting for ease of management



Open Manage Super Nodes to create new one.

Disable Capabilities

Allow users to disable the following capabilities:

☑ All
☑ Access
☑ Compliance
☑ Firewall and Application Control
☑ Remote Access VPN
☑ Threat Prevention

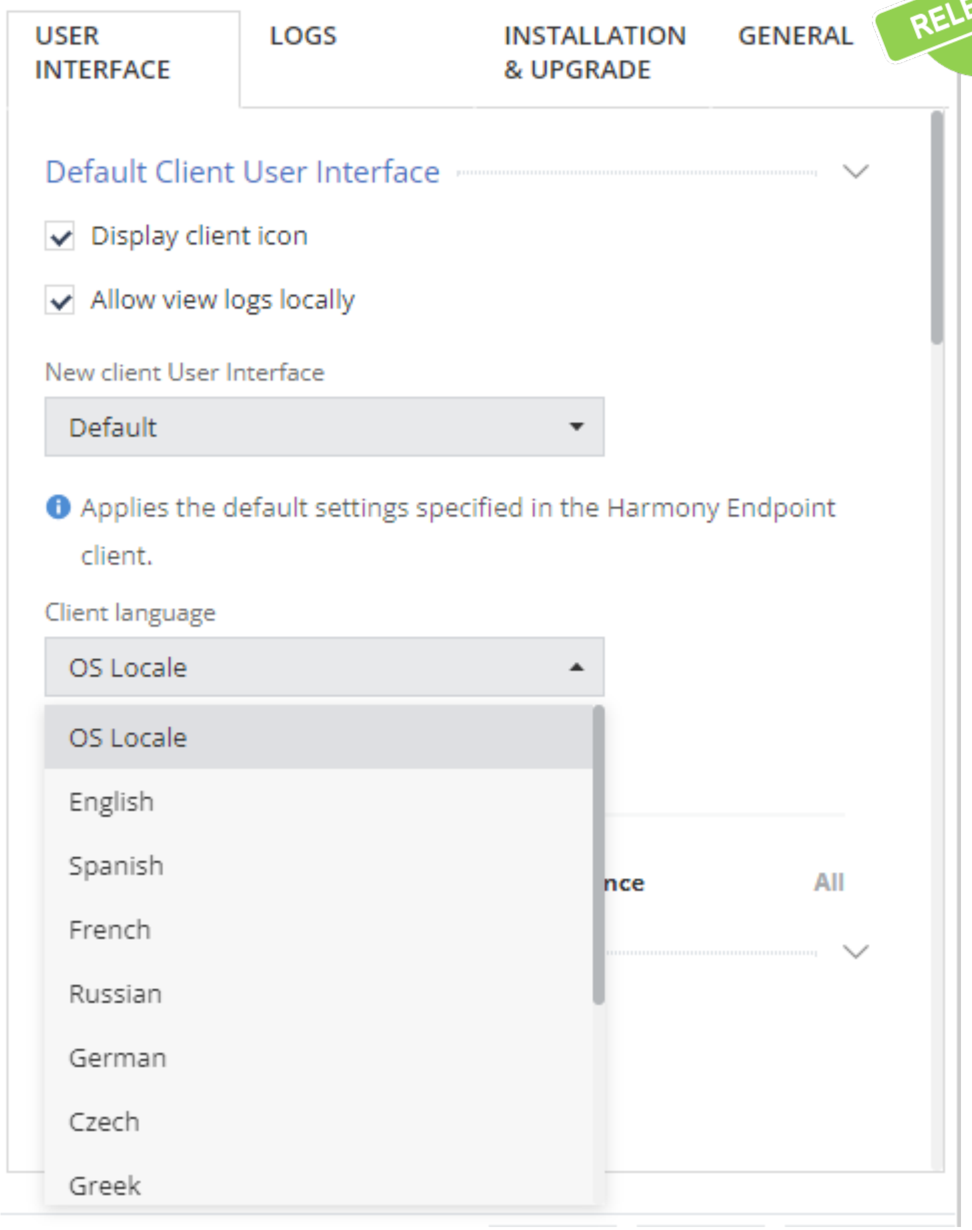
☑ Set timeout 120 min(s)

□ Protect by password

No password for Disable Capabilities configured!
The password applies consistently across all policy rules.
Open Manage Disable Capabilities Protect Password to create a new one.

Client Language Settings

- Additional options for explicit selection of a language for use in the client UI
- "OS Locale" option enables previous functionality
  - Utilize the language as determined by Windows O/S locale
  - If language is not supported – use English
- Languages supported (unchanged): Czech, German, English, Spanish, French, Greek, Italian, Japanese, Polish, Portuguese, Russian, Ukrainian



Default Client User Interface

☑ Display client icon

☑ Allow view logs locally

New client User Interface: Default

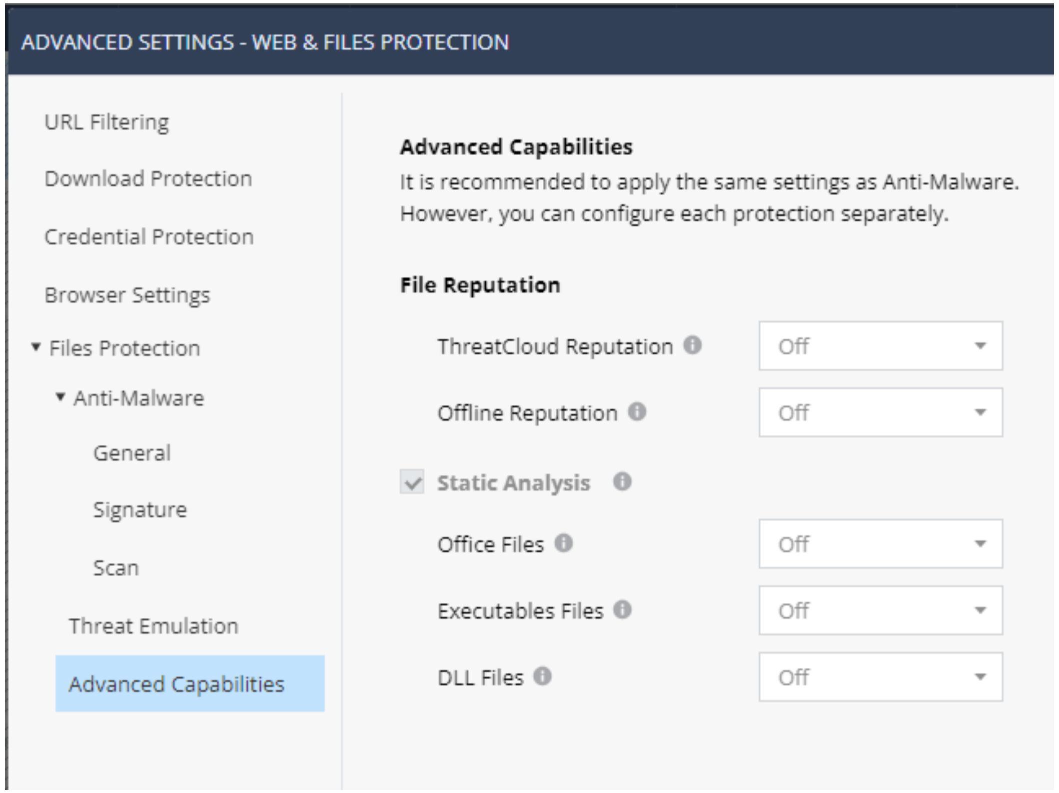
Applies the default settings specified in the Harmony Endpoint client.

Client language: OS Locale

Changes to “Threat Emulation” Blade

RELEASED

- Set of capabilities now configured as part of “File Options”
  - Threat Emulation (TE) is just one of the capabilities
  - With basic license, blade can run with TE “Off”
- Separate configuration for all the following capabilities and no dependency on TE:
  - Threat Cloud Reputation
  - Offline Reputation (OFR)
  - Static Analysis (SA)
    - Office Files
    - Executable Files
    - DLL Files



Advanced Capabilities

It is recommended to apply the same settings as Anti-Malware. However, you can configure each protection separately.

File Reputation

ThreatCloud Reputation: Off

Offline Reputation: Off

☑ Static Analysis

Office Files: Off

Executables Files: Off

DLL Files: Off

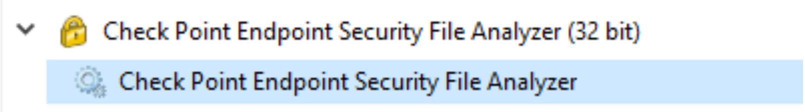
Files Protection - Advanced Capabilities

RELEASED

- By default, settings are same as “Threat Emulation” (for upgrade considerations)
- Visibility / control to additional existing capabilities
  - ThreatCloud Reputation: Verify reputation of files based on their hash in Check Point’s ThreatCloud (TC)
  - Offline Reputation
    - Verify reputation of files based on their hash against data stored locally on the client
    - Most common hashes accessed in TC are stored on client with ongoing updates
    - Allows for detections when client is offline
    - Allows for fast detection when client is online – verdict is double-checked with TC
  - Separate Static Analysis settings for each model type
    - For SA Office files detection, for "right click" option to create exclusions, the excluded hash will be the hash of the macro (and not the hash of the file).

TE – Other Changes

- On client UI, the corresponding tray in main Client UI page is renamed “File Protections”
- Corresponding process has been renamed



Check Point Endpoint Security File Analyzer (32 bit)

Check Point Endpoint Security File Analyzer

DNS Traffic Inspection

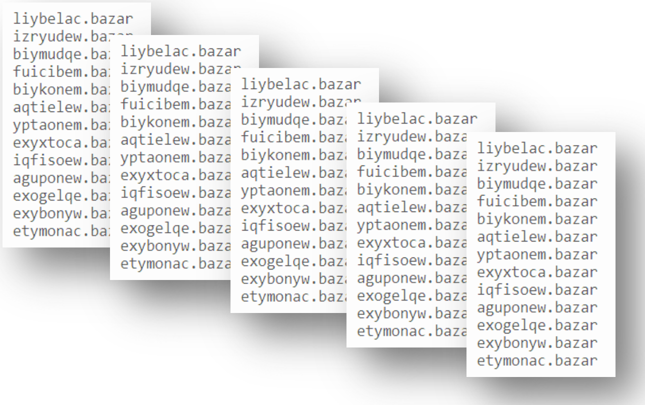
RELEASED

Block C&C communications and Data theft with Deep Learning engines

- Anti-Bot blade extended to include DNS traffic inspection support
- Leverages Threat Cloud based engines for traffic analysis
  - Aligned with similar capabilities on Quantum

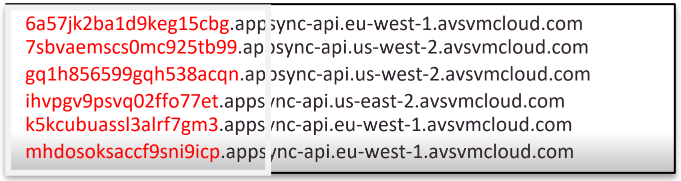
Client Machine

#1 DGA (Domain Generation Algorithm)

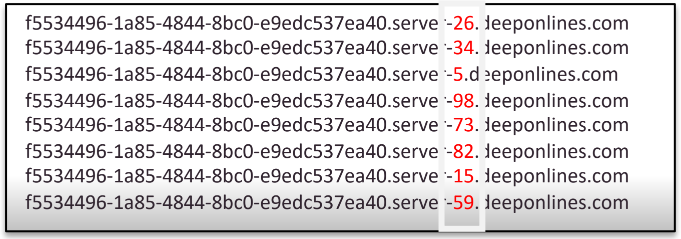


```
liybelac.bazar
izryudew.bazar
biymudqe.bazar
fuicibem.bazar
biykonem.bazar
aqtielew.bazar
yptaonem.bazar
exyxtoca.bazar
iqfisoew.bazar
aguponew.bazar
exogelqe.bazar
exybonyw.bazar
etymonac.bazar
```

#2 DNS Tunneling



```
6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud.com
7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud.com
gq1h856599gqh538acqn.appsync-api.us-west-2.avsvmcloud.com
ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud.com
k5kcubuassl3alrf7gm3.appsync-api.eu-west-1.avsvmcloud.com
mhdosoksaccf9sni9icp.appsync-api.eu-west-1.avsvmcloud.com
```



```
f5534496-1a85-4844-8bc0-e9edc537ea40.server-26.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-34.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-5.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-98.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-73.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-82.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-15.deeponlines.com
f5534496-1a85-4844-8bc0-e9edc537ea40.server-59.deeponlines.com
```

3

Linux Client

- Anti-Malware Engine
- New distributions / kernel support
- Anti-Ransomware
- Installation: Universal / Offline Package

New distributions / kernel support

- Infrastructure changes
  - Universal package minimizes dependencies on underlying distribution
  - Reduces changes for new distribution / kernel support
  - Continue to recommend RFE for prioritization of additional support
- 1.15.7: Additional support

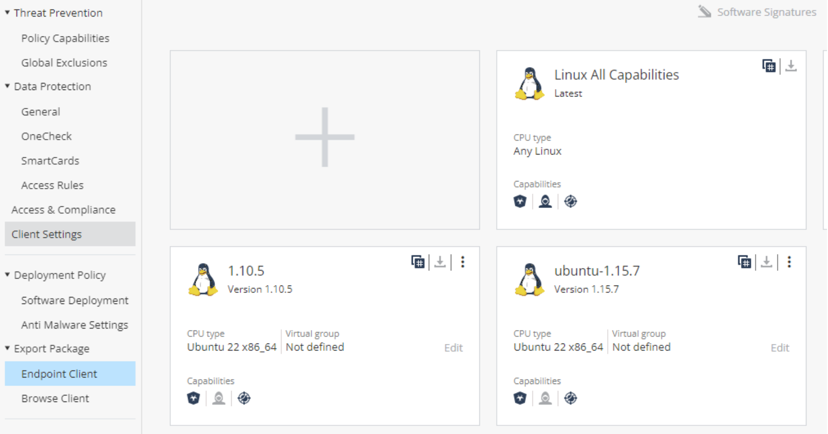
  RELEASED

  - Support for additional versions of Red Hat Enterprise Linux (RHEL): 8.9 and 9.3. Current RH support covers 7.8-8.9, 9.0-9.3
  - Support for new Linux distribution: Alma Linux. We are initially supporting versions 8.9,9.0-9.3
  - Existing Ubuntu support has been expanded to include support of Kernel version 6.2
- Upcoming
  - OpenSuse 15.4 + 15.5
  - Fedora releases 36 - 39

PLANNED

Installation / Upgrade

- Universal Package:
  - Initially different package provided for each distribution.
  - Now combined to one of two “Universal Packages”, per whether package manager is ‘.deb’ or ‘.rpm’ based
- Offline Package:
  - Exporting package creates “Offline Package” that can be installed using 3rd deployment software or manual methods
- Evergreen / “Latest”:
  - When installing the Linux client there is an option to select a version called “latest”.
  - Installs latest version and automatically upgrades client whenever a new Linux client version is available.
  - Requires internet connectivity to upgrade



Linux All Capabilities
Latest
CPU type: Any Linux
Capabilities

1.10.5
Version 1.10.5
CPU type: Ubuntu 22 x86_64
Virtual group: Not defined
Capabilities

ubuntu-1.15.7
Version 1.15.7
CPU type: Ubuntu 22 x86_64
Virtual group: Not defined
Capabilities

Other Updates

RELEASED

- Anti-Malware Engine
  - Linux client now leverages E2
    - Aligned with Windows E2 and Mac clients
    - Offline signature update procedure now covers new Linux engine (sk180690)
  - Added CP reputation look up
- Anti-Ransomware Blade
  - Originally added in “Detect Mode”
  - Now can be enabled in “Prevent Mode”
  - Pending
    - Include in listing as part of blade selection UI for export/deployment policy. Currently:
      - For new installations AR will be enabled by default
      - For upgrade scenarios AR needs to be enabled manually in the policy following the upgrade
    - Exceptions should be defined as Legacy Exceptions and is not yet supported as part of the “Smart Exclusions” capability

4

Mac Client

- ❖ Installation Improvements
- ❖ Other Enhancements

Installation Improvements

- Simplified installation for non-MDM deployments
  - Significant reduction in number of approvals required in installation process
  - "Anti-Bot" network extension is also unified into the "Check Point" network extension. In non-MDM deployments, there are reduced number of approvals required during installation
  - Kernel extensions are deprecated for Endpoint Security on Mac Related installation steps, such as booting into recovery and adjusting security settings, are no longer necessary
    - Related Server setting: "Use Port Protection without kernel extensions“

Other Enhancements

- Reconnect Tool
  - Option added to the Reconnect Tool that results in creation of a zip archive of the reconnect tool that contains the uninstall password.
  - Allows tool to be run without requiring (interactive) input of the uninstall password for the currently installed endpoint client.
  - The uninstall password included in the archive is obfuscated
- Events for network related traffic stored in the internal forensics database (EFR.db) and are available for searching within Threat Hunting capabilities
- Authenticated Proxy
  - Existing Authenticated Proxy configuration in the Management interface can now be defined to apply to the Mac security client
  - Un-authenticated proxy support in progress

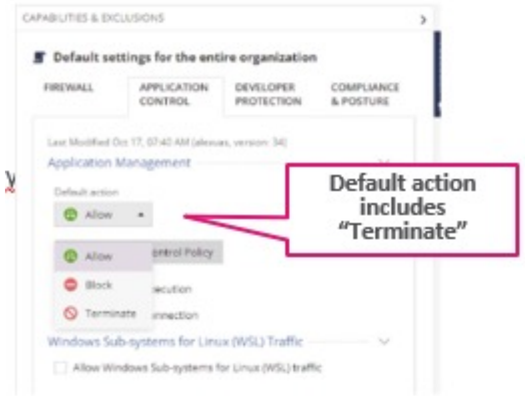
PLANNED

4

EAs in Progress

Early Access (EA) Activities in Progress

- Semi-isolated networks
- HTTPS Inspection
  - Affects IOC, URLF and Anti-Bot
- FDE Smart Pre-boot
  - Seamless remote help and improving the operational efficiency of managing a deployment with Full Disk Encryption (FDE)
- Application Whitelisting
  - Default Deny All Rule



Default settings for the entire organization

Last Modified Oct 17, 07:40 AM (alexuas, version: 34)

Application Management

Default action: Allow

Windows Sub-systems for Linux (WSL) Traffic

☐ Allow Windows Sub-systems for Linux (WSL) traffic

Default action includes "Terminate"

Summary

- Lots delivered!!
- Lots to come!!
- Look on CheckMates

- For any follow up: jonnyr@checkpoint.com

CHECK POINT™

Thank You!

YOU DESERVE THE BEST SECURITY