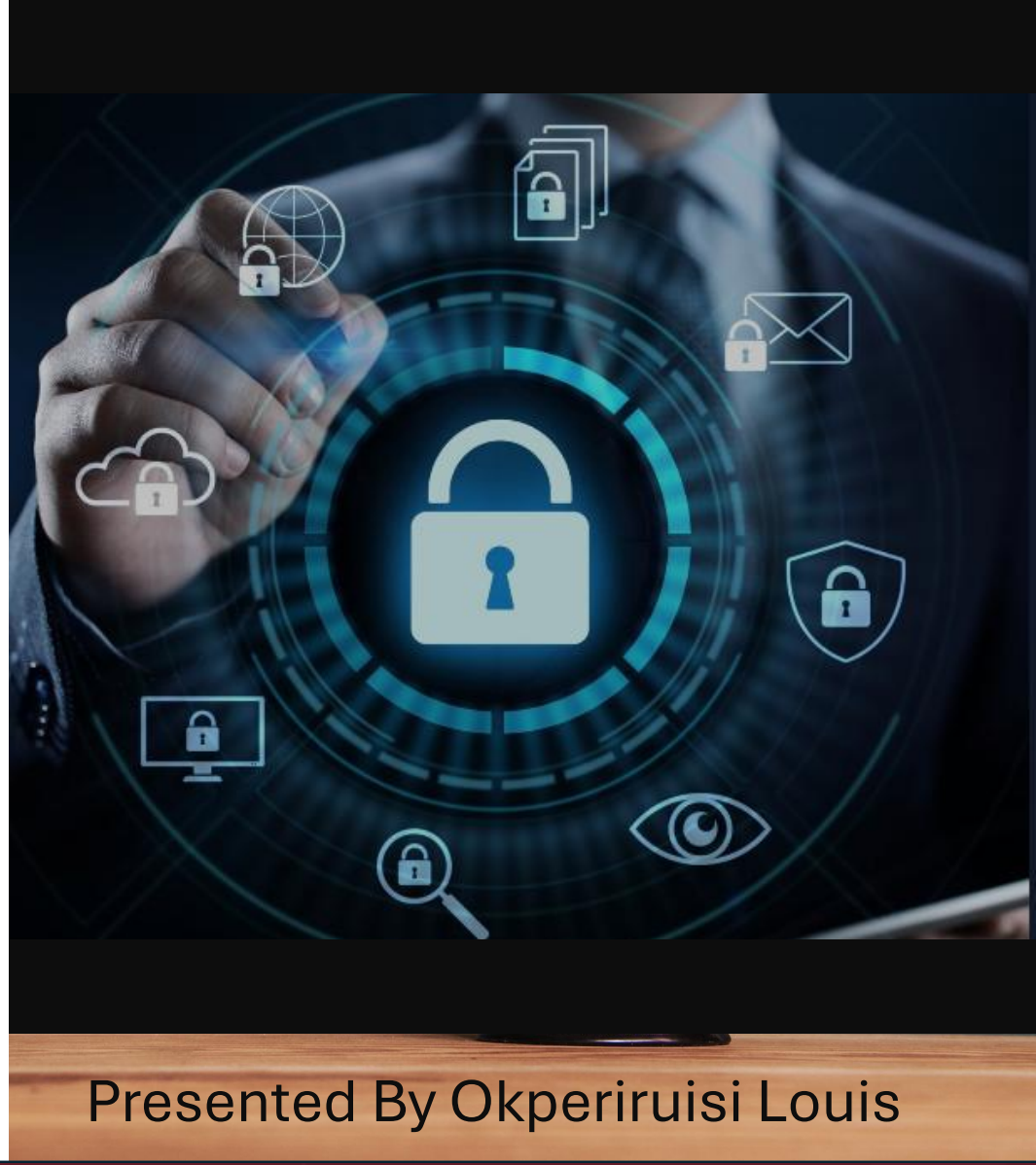
Endpoint Security Policy Configuration on OPSWAT MetaDefender IT Access Platform for in SMEs

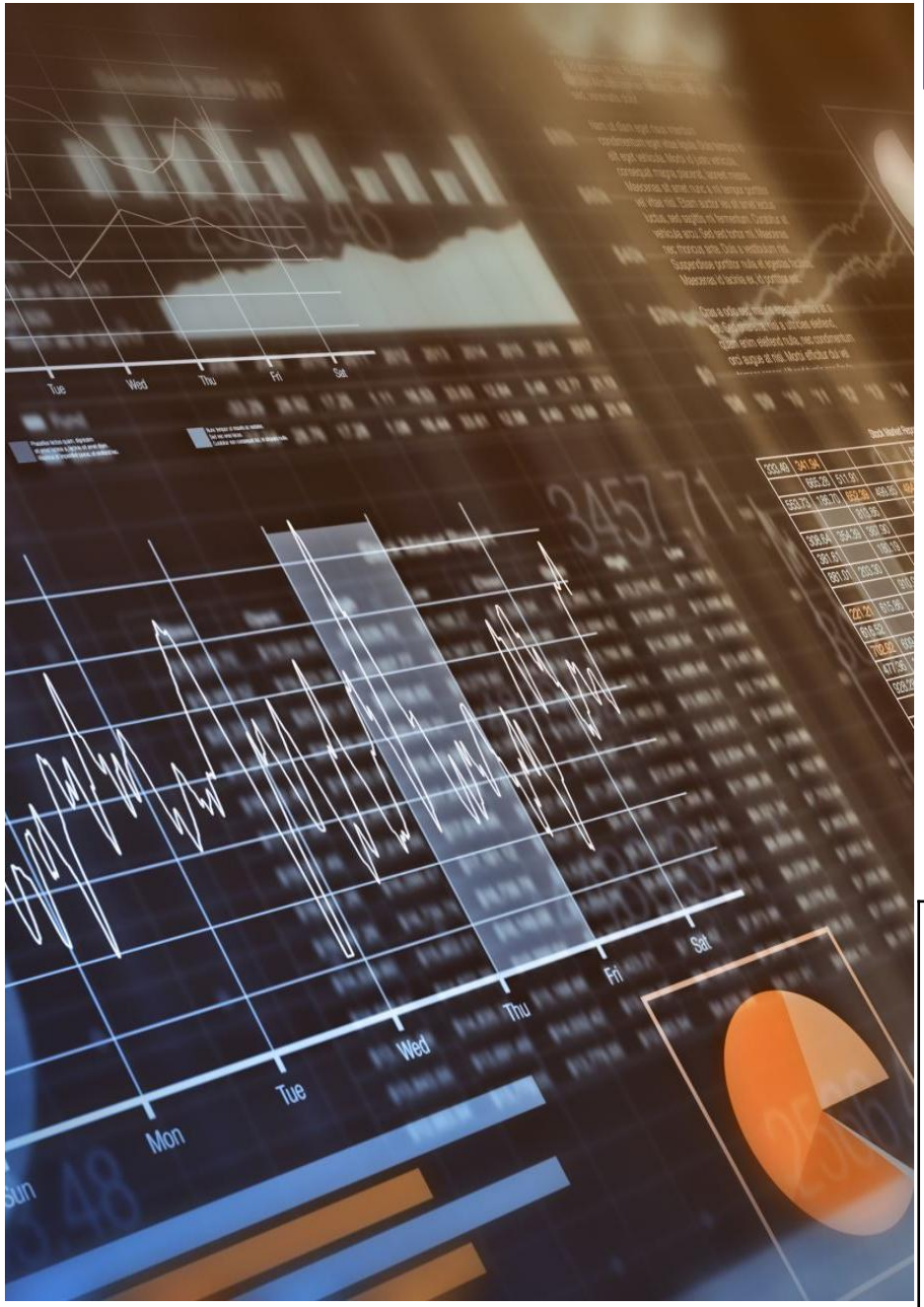


Presented By Okperiruisi Louis

5th September, 2025

Project Objective:

The goal of this project is to enhance endpoint security for SMEs by configuring security policies on OPSWAT MetaDefender IT Access Platform. The project will focus on implementing advanced malware detection, data loss prevention, vulnerability management, patch management, application control, and threat monitoring.



Scope of work

This project will cover the following configurations on OPSWAT MetaDefender IT Access Platform:

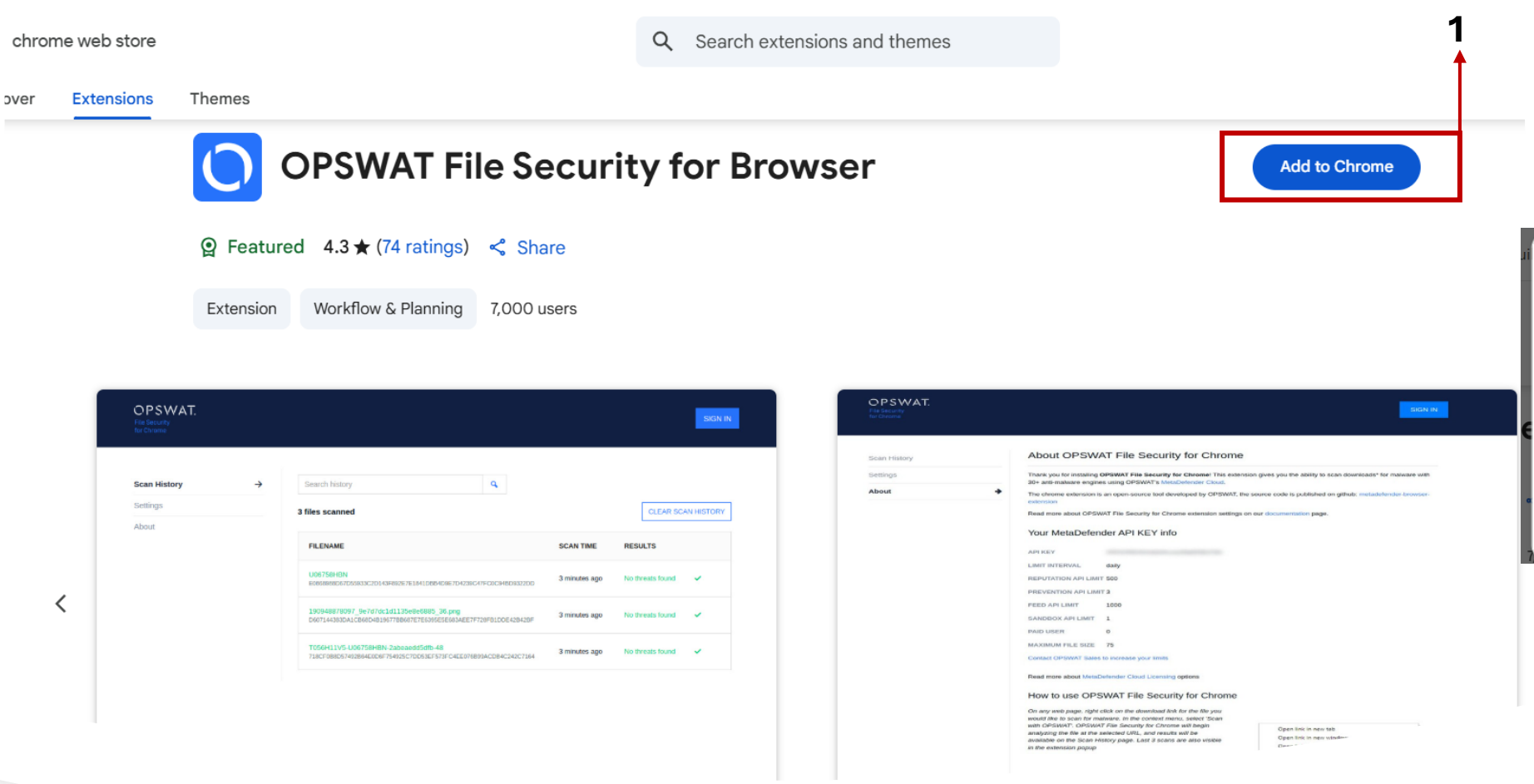
- Advanced Malware Detection Policy
- Full Scan or Custom Scan Policy
- Data Loss Prevention Policy
- Application Control Policy
- Vulnerability Management Policy
- Patch Management Policy
- Threat Monitoring Policy

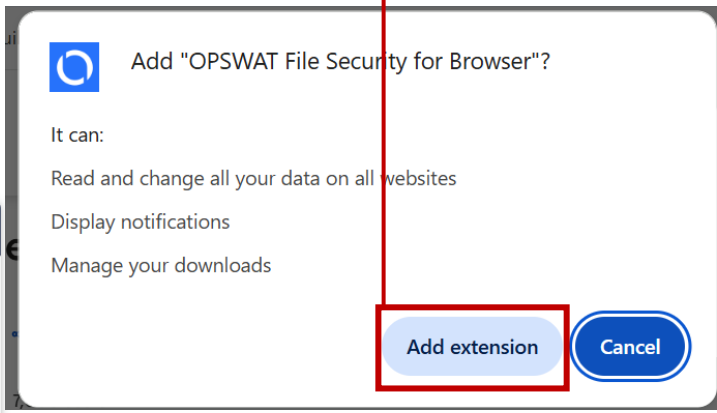
Project Deliverable

A fully configured OPSWAT MetaDefender IT Access Platform with the above security policies. Documentation detailing each policy configuration step. Reports showing policy enforcement results.

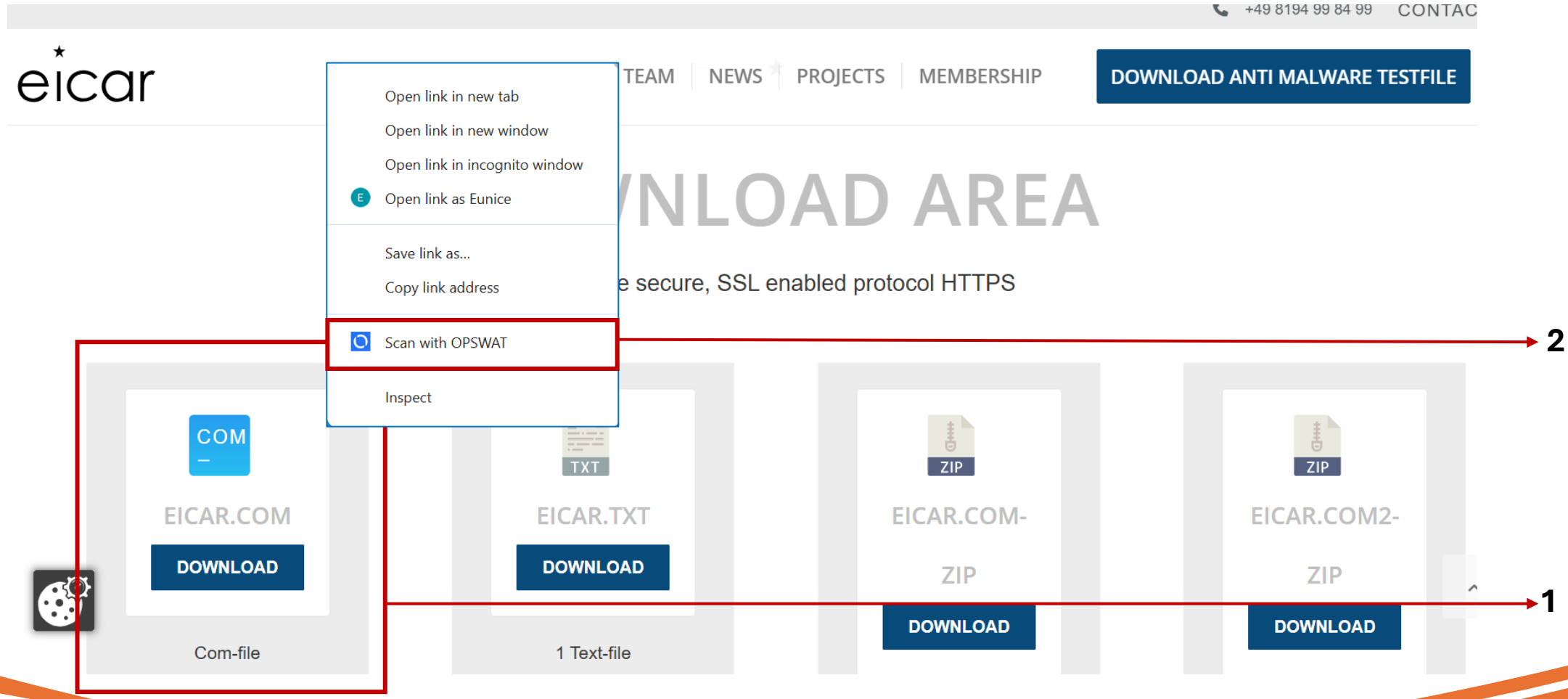
OPSWAT File Security for Browser

Visit: //chrome.google.com/webstore/detail/opswat-file-securityfor/fjampemfhdfmangifafmianhokmpjbcj

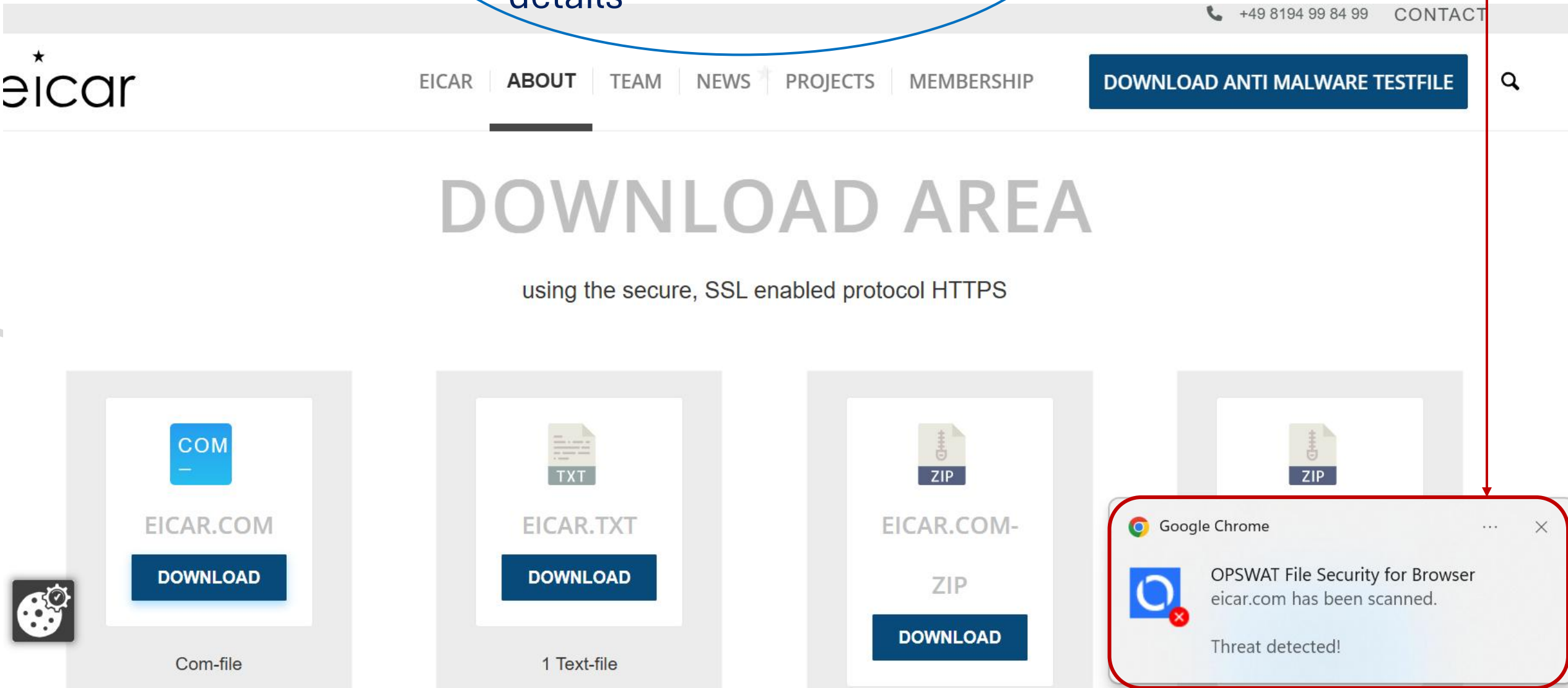




Visit: https://www.eicar.org/download-anti-malware-testfile/ to download a malicious file, **RIGHT CLICK** on download and select **SCAN WITH OPSWAT**



The file has been scanned by OPSWAT and a threat detected, Click on the pop-up to get more details



OPSWAT.
File Security for Browser

Scan History

Settings

About

Search history

2 files scanned

CLEAR SCAN HISTORY

FILENAME	SCAN TIME	RESULTS
eicar.com 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F	a few seconds ago	Infected / Known
eicar.com 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F	16 minutes ago	Infected / Known

MetaDefender Cloud Community

Analyze a File, URL, IP address, Domain, Hash, or CVE | Add a file

Limits per day 30/30 499/500 15/15 Sign in

Processed file | Add to Catalogue

eicar.com | Not Available (Country of Origin) Add COO

SHA-256: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

Multiscanning
Threats Detected

Adaptive Sandbox
Malicious

Deep CDR™
No Sanitization Available

Proactive DLP
No Results Available

Vulnerabilities
No Vulnerabilities Found

Community feedback
0 comments 7 19

Multiscanning

Threats Detected

16 /22 ENGINES

Engine Name	Verdict	Last engine update
AhnLab	Virus/EICAR_Test_File	09/05/2025 12:54 PM GMT
Avira	Eicar-Test-Signature	09/05/2025 04:40 AM GMT
Bitdefender	EICAR-Test-File (not a virus)	09/05/2025 04:40 AM GMT
NANOAV	Marker.Dos.EICAR-Test-File.dyb	09/05/2025 04:47 AM GMT
TACHYON	EICAR-Test-File	09/04/2025 14:26 PM GMT
Varist	EICAR_Test_File	09/04/2025 19:09 PM GMT
Zillya!	EICAR.TestFile	09/05/2025 04:41 AM GMT
Vir.IT eXplorer	EICAR-Test-File	09/05/2025 04:34 AM GMT
Xvirus Anti-Malware	Malware	09/04/2025 23:07 PM GMT
Lionic	No Threats Detected	09/05/2025 07:00 AM GMT
Vir.IT ML	No Threats Detected	09/05/2025 04:41 AM GMT
Agatha Anderton	Unsupported File Type	09/05/2025 04:39 AM GMT
CMC	Failed	09/05/2025 01:00 AM GMT
Quick Heal	Failed	09/05/2025 01:00 AM GMT

File Overview

Category	T	Entropy	4.8723276870872425
File Type	ASCII Text	Scanned	09/05/2025 12:57 PM GMT
File Extension	txt	Duration	a few seconds
TrID	EICAR antivirus testfile	MD5	44D88612FEA8A8F36DE82E1... BB02F
LibMagic	EICAR virus testfiles	SHA-1	3395856CE81F2B7382DEE72... 14140
Magika	PS1	SHA-256	275A021BBFB6489E54D4718... 1FD0F

Scan History

This file has been scanned 200 times

Deep CDR™ Regeneration

Download Sanitized Version

No Sanitization Available

After Data Sanitization

Sandbox

Malicious

100 /100
THREAT SCORE

Threat Indicators

Key indicators and MITRE ATT&CK techniques

Malicious Indicators 3

- Matched a malicious YARA rule
- EICAR Standard Anti-Virus detected

Suspicious Indicators 1

- Matched a relevant YARA rule

No Threat Indicators 1

- Found an interesting string artifact

+ 1 more indicators

Indicators of Compromise

Extracted and derived IOCS

No IOCs detected

YARA Rules

eicar	Malicious
SUSP_Just_EICAR	Suspicious

Sandbox

Malicious

100 /100
THREAT SCORE

Threat Indicators

Malicious Indicators 3

- Matched a malicious YARA rule
- EICAR Standard Anti-Virus detected
- OSINT source detected malicious resource

Suspicious Indicators 1

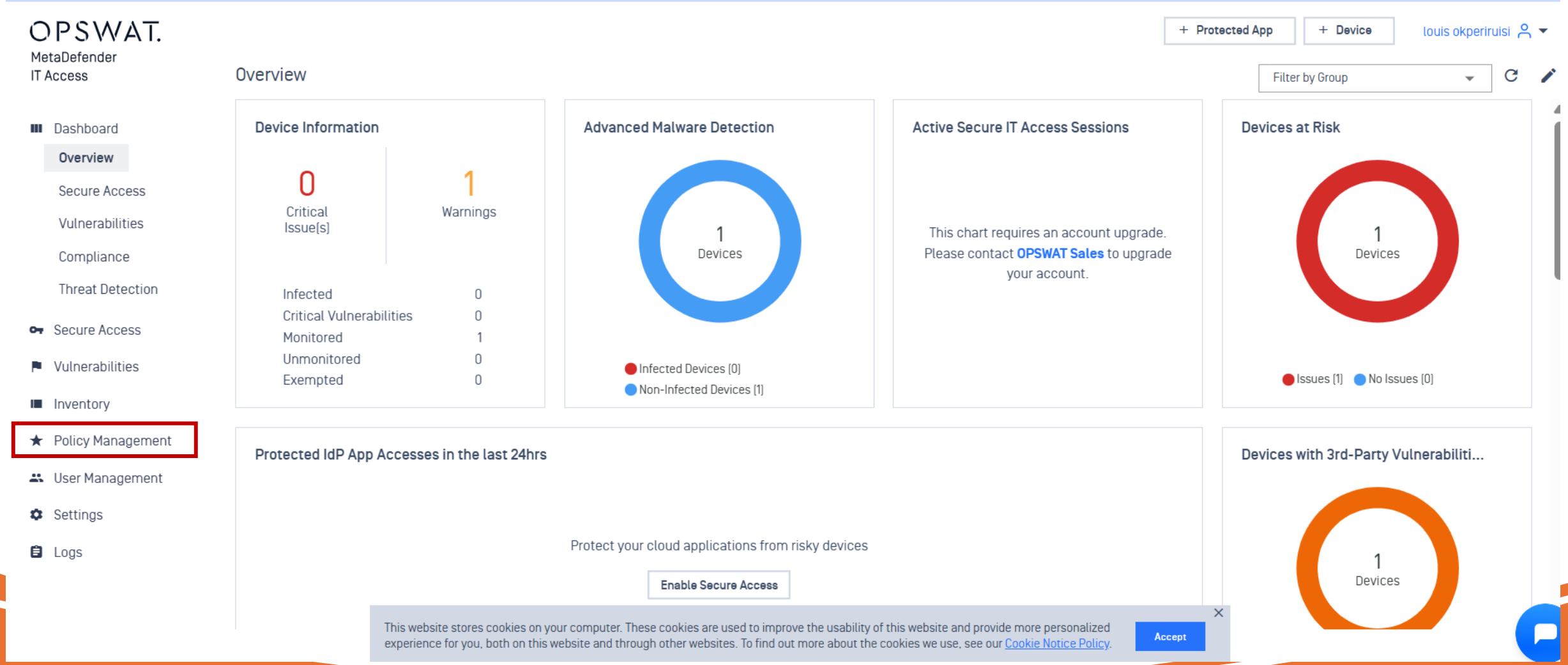
- Matched a relevant YARA rule

No Threat Indicators 1

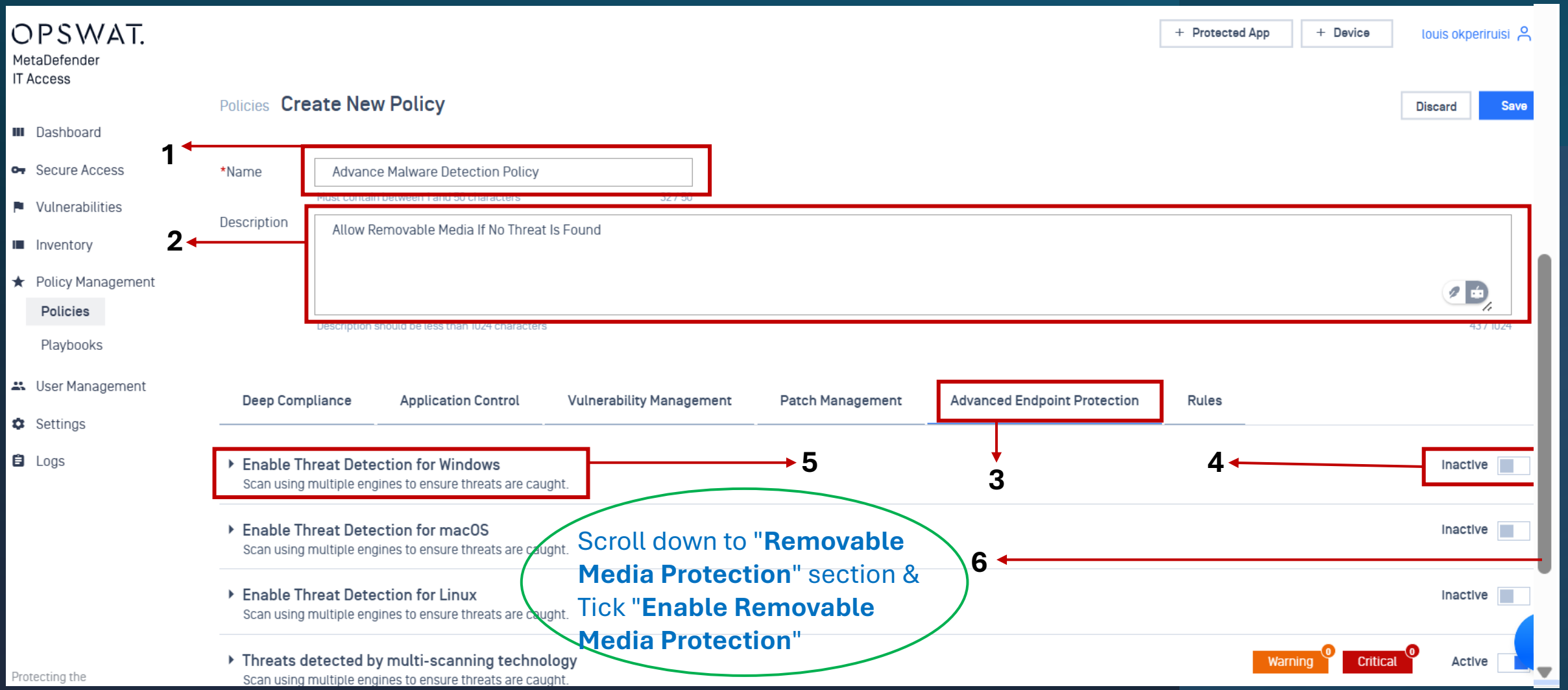
- Found an interesting string artifact

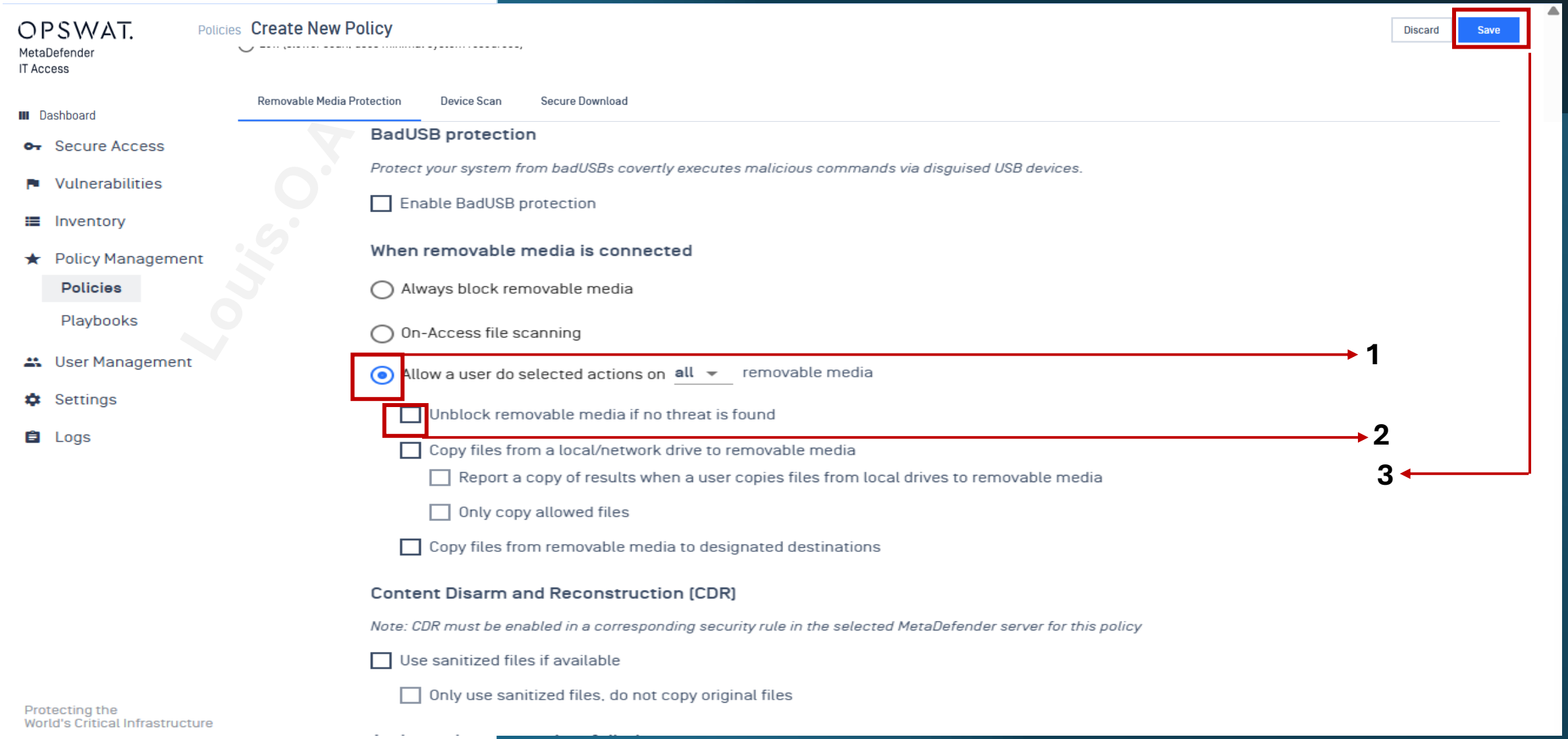
Indicators of Compromise

Sign-In to https://console.metaaccess-b.opswat.com/dashboard/overview to Configure All The Policies

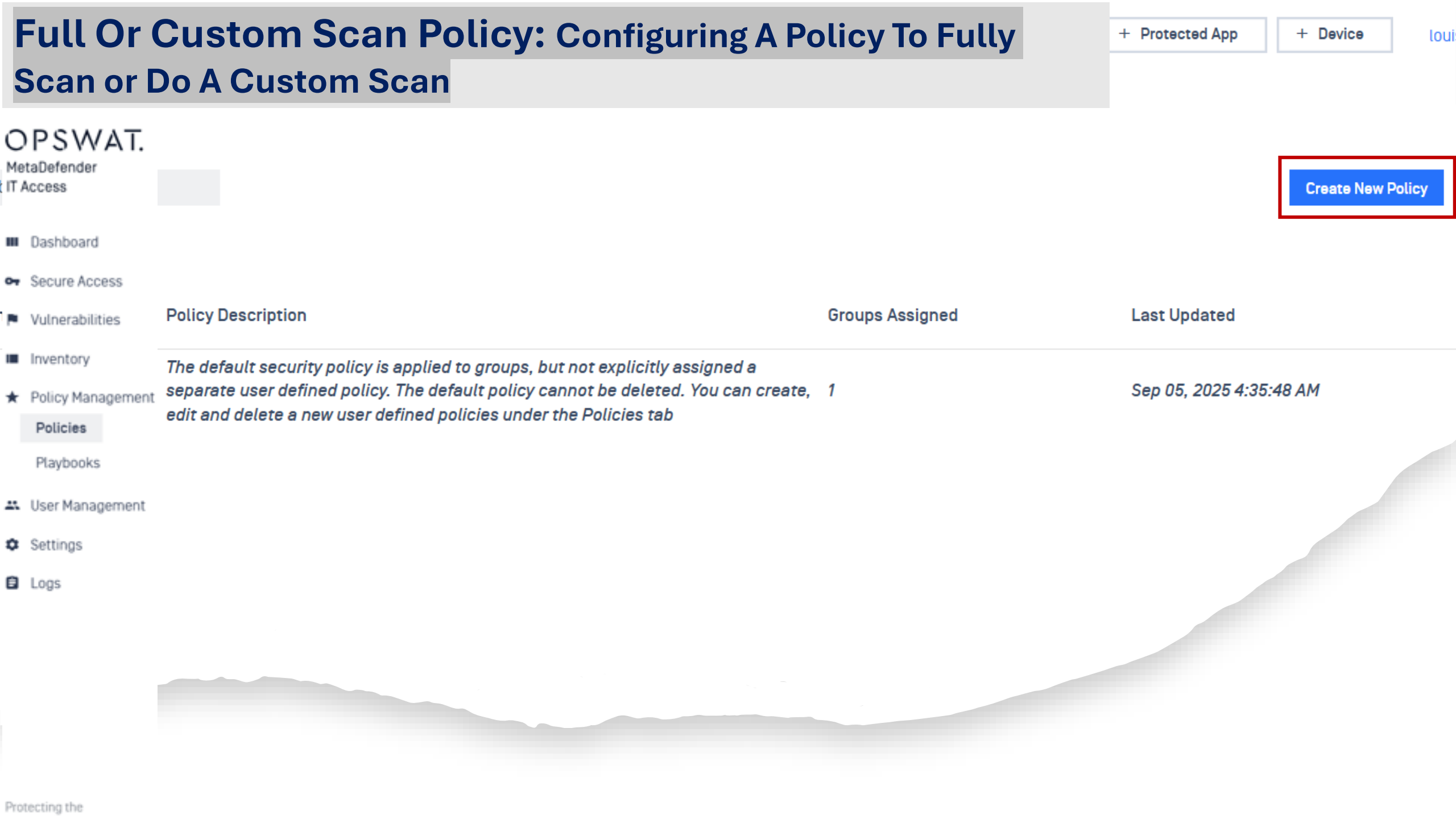


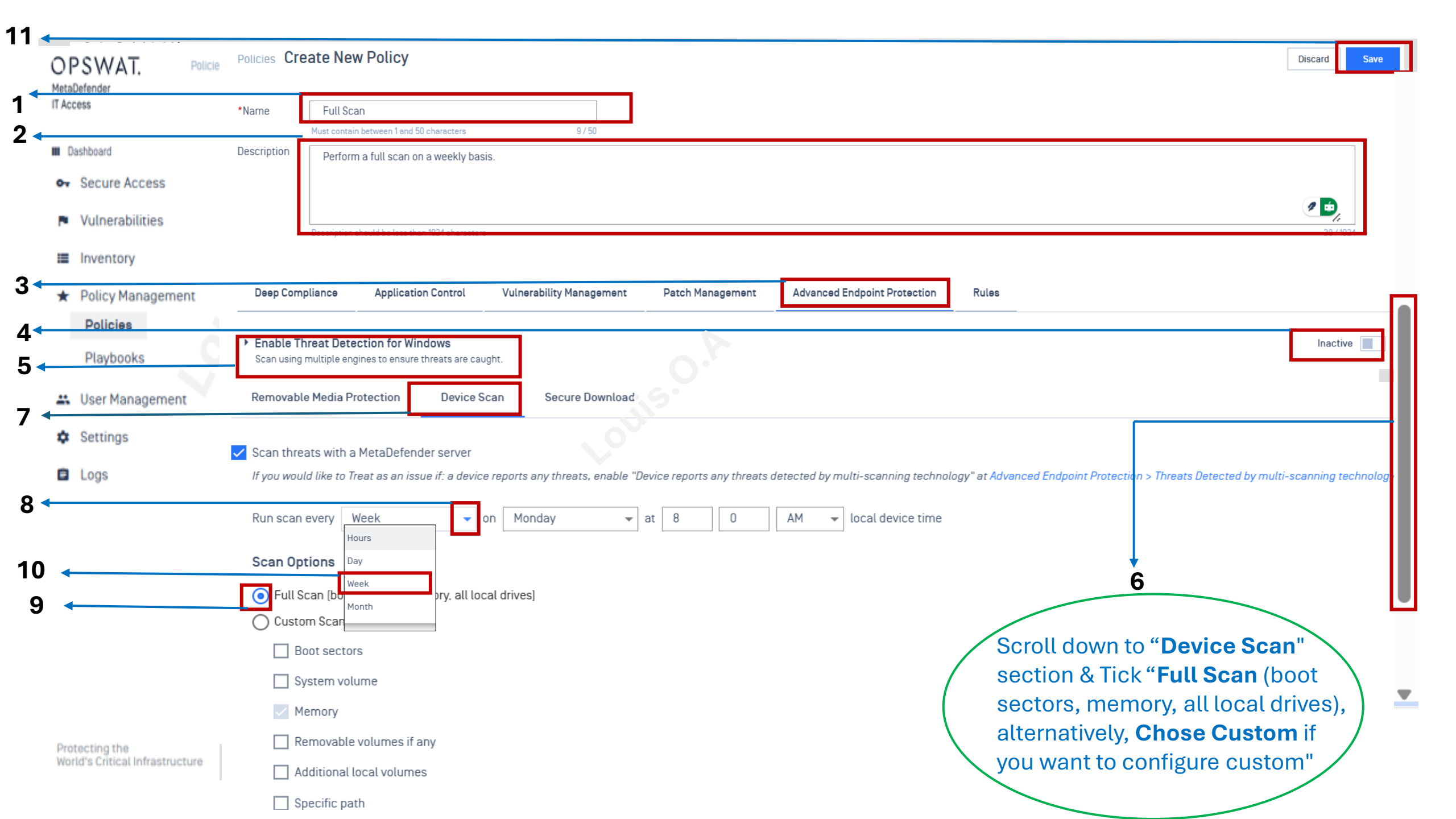
Advance Malware Detection Policy: Configuring A Policy To Unblock A Removable Media If No Threat Is Found.


OPSWAT.
MetaDefender
IT Access
+ Protected App
+ Device
louis okperiruisi
Policies
Create New Policy
Discard
Save
Dashboard
Secure Access
Vulnerabilities
Inventory
Policy Management
Policies
Playbooks
User Management
Settings
Logs
1
*Name
Advance Malware Detection Policy
2
Description
Allow Removable Media If No Threat Is Found
Deep Compliance
Application Control
Vulnerability Management
Patch Management
Advanced Endpoint Protection
Rules
3
4
5
Enable Threat Detection for Windows
Scan using multiple engines to ensure threats are caught.
Inactive
Enable Threat Detection for macOS
Scan using multiple engines to ensure threats are caught.
Inactive
Enable Threat Detection for Linux
Scan using multiple engines to ensure threats are caught.
Inactive
6
Scroll down to "Removable Media Protection" section & Tick "Enable Removable Media Protection"
Threats detected by multi-scanning technology
Scan using multiple engines to ensure threats are caught.
Warning
Critical
Active
Protecting the


OPSWAT.
MetaDefender
IT Access
Policies
Create New Policy
Discard
Save
Dashboard
Secure Access
Vulnerabilities
Inventory
Policy Management
Policies
Playbooks
User Management
Settings
Logs
Removable Media Protection
Device Scan
Secure Download
BadUSB protection
Protect your system from badUSBs covertly executes malicious commands via disguised USB devices.
Enable BadUSB protection
When removable media is connected
Always block removable media
On-Access file scanning
Allow a user do selected actions on all removable media
Unblock removable media if no threat is found
Copy files from a local/network drive to removable media
Report a copy of results when a user copies files from local drives to removable media
Only copy allowed files
Copy files from removable media to designated destinations
Content Disarm and Reconstruction (CDR)
Note: CDR must be enabled in a corresponding security rule in the selected MetaDefender server for this policy
Use sanitized files if available
Only use sanitized files, do not copy original files
1
2
3
Protecting the
World's Critical Infrastructure

Full Or Custom Scan Policy: Configuring A Policy To Fully Scan or Do A Custom Scan




11
OPSWAT.
MetaDefender
IT Access
Policies
Create New Policy
Discard
Save
1
*Name
Full Scan
Must contain between 1 and 50 characters
9 / 50
2
Description
Perform a full scan on a weekly basis.
Dashboard
Secure Access
Vulnerabilities
Inventory
3
Policy Management
Deep Compliance
Application Control
Vulnerability Management
Patch Management
Advanced Endpoint Protection
Rules
4
Policies
Playbooks
Enable Threat Detection for Windows
Scan using multiple engines to ensure threats are caught.
Inactive
5
User Management
Removable Media Protection
Device Scan
Secure Download
7
Settings
Logs
Scan threats with a MetaDefender server
If you would like to Treat as an issue if: a device reports any threats, enable "Device reports any threats detected by multi-scanning technology" at Advanced Endpoint Protection > Threats Detected by multi-scanning technolog
8
Run scan every
Week
on
Monday
at
8
0
AM
local device time
Hours
Day
Week
Month
Scan Options
10
9
Full Scan (bo
ory, all local drives)
Custom Scan
Boot sectors
System volume
Memory
Removable volumes if any
Additional local volumes
Specific path
6
Scroll down to “Device Scan" section & Tick “Full Scan (boot sectors, memory, all local drives), alternatively, Chose Custom if you want to configure custom"
Protecting the
World's Critical Infrastructure

Data Lost Prevention

+ Protected App + Device loui

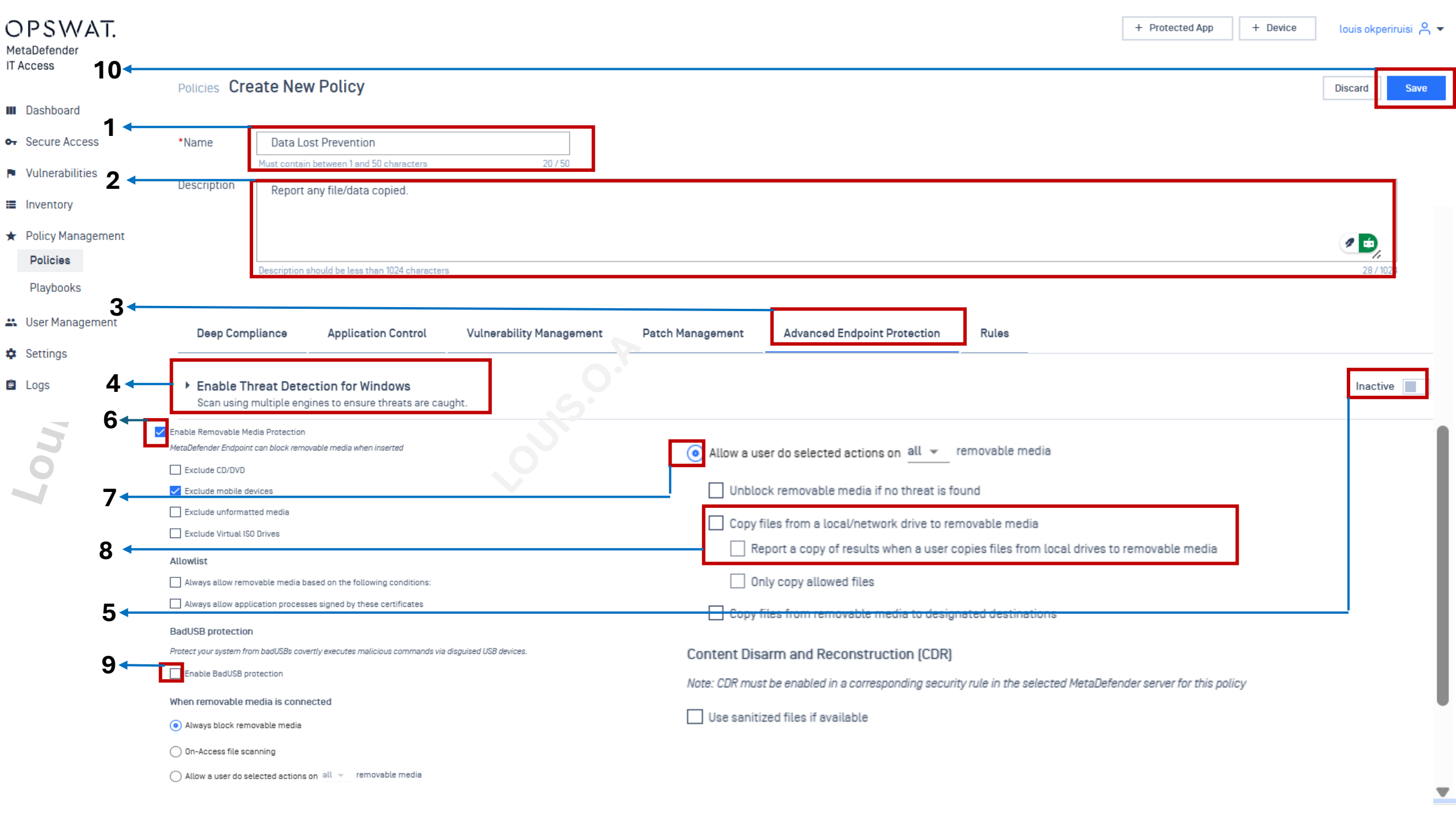
OPSWAT.
MetaDefender
IT Access

- Dashboard
- Secure Access
- Vulnerabilities
- Inventory
- Policy Management
  - Policies
  - Playbooks
- User Management
- Settings
- Logs

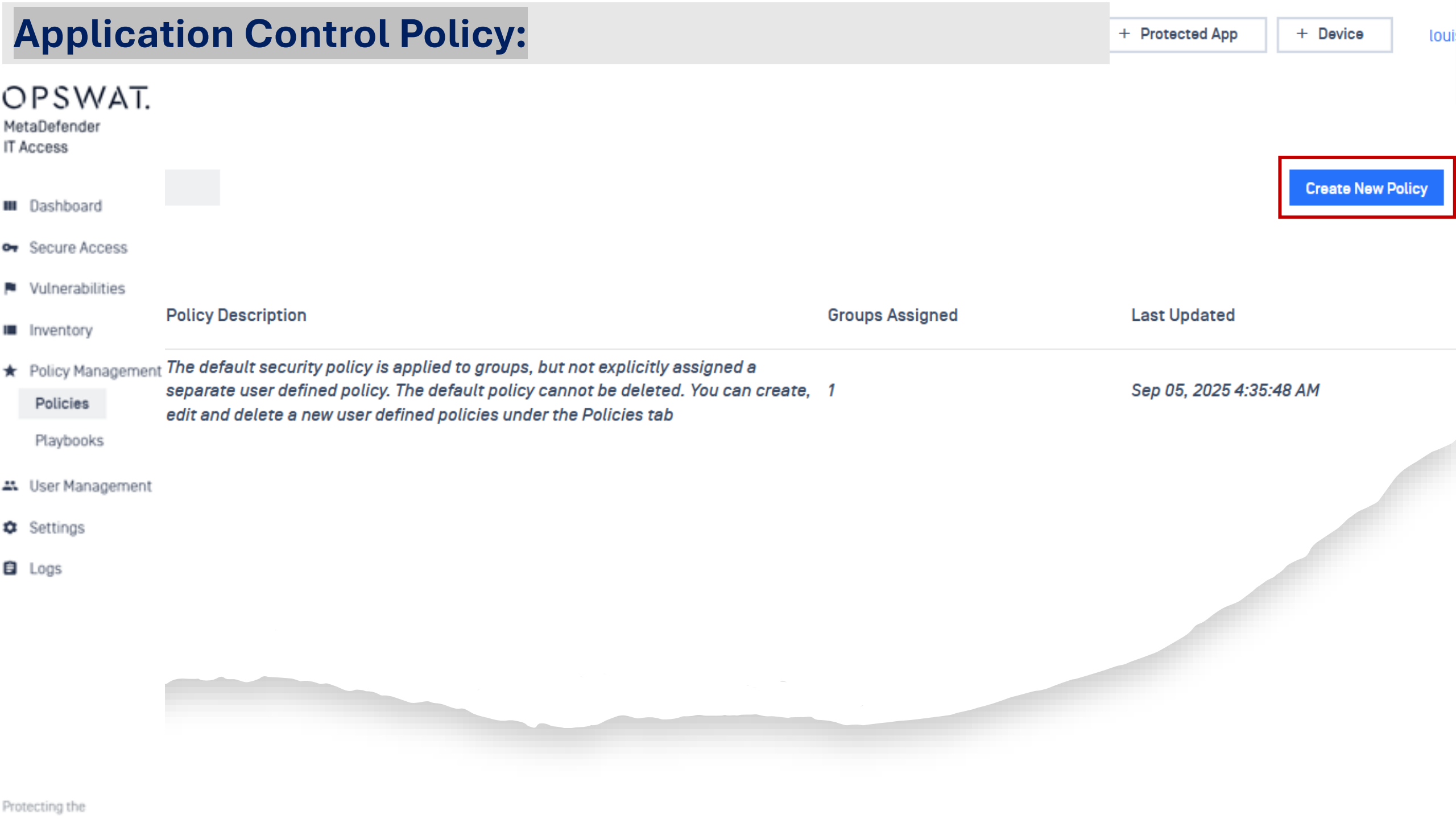
Create New Policy

Policy Description	Groups Assigned	Last Updated
The default security policy is applied to groups, but not explicitly assigned a separate user defined policy. The default policy cannot be deleted. You can create, edit and delete a new user defined policies under the Policies tab	*1*	*Sep 05, 2025 4:35:48 AM*

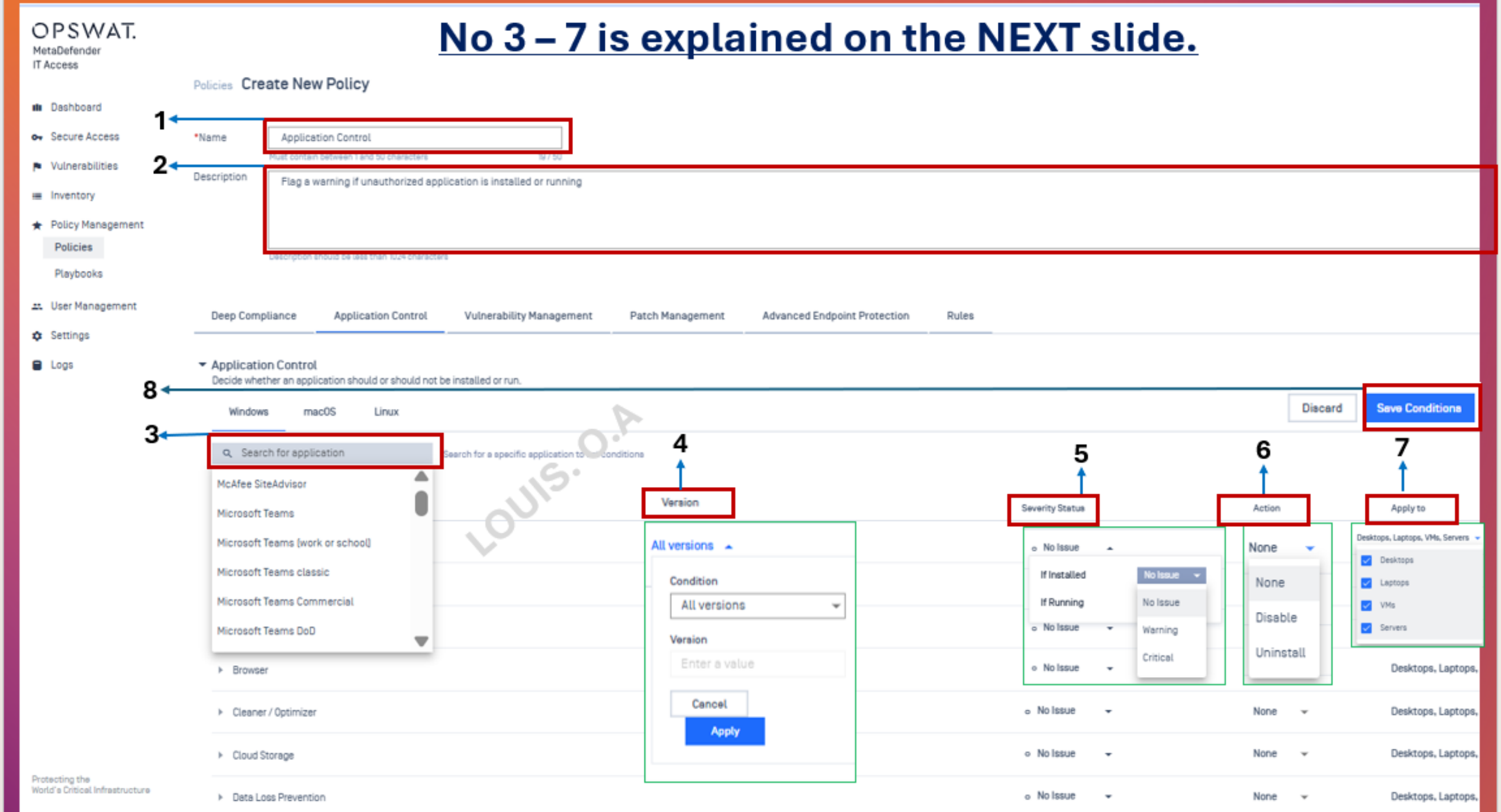
Protecting the


OPSWAT.
MetaDefender
IT Access
+ Protected App
+ Device
louis okperiruisi
10
Policies
Create New Policy
Discard
Save
Dashboard
Secure Access
Vulnerabilities
Inventory
Policy Management
Policies
Playbooks
User Management
Settings
Logs
1
*Name
Data Lost Prevention
Must contain between 1 and 50 characters
20 / 50
2
Description
Report any file/data copied.
Description should be less than 1024 characters
28 / 1024
3
Deep Compliance
Application Control
Vulnerability Management
Patch Management
Advanced Endpoint Protection
Rules
4
Enable Threat Detection for Windows
Scan using multiple engines to ensure threats are caught.
Inactive
6
Enable Removable Media Protection
MetaDefender Endpoint can block removable media when inserted
Exclude CD/DVD
Exclude mobile devices
Exclude unformatted media
Exclude Virtual ISO Drives
7
Allow a user do selected actions on all removable media
Unblock removable media if no threat is found
Copy files from a local/network drive to removable media
Report a copy of results when a user copies files from local drives to removable media
Only copy allowed files
8
Allowlist
Always allow removable media based on the following conditions:
Always allow application processes signed by these certificates
5
Copy files from removable media to designated destinations
BadUSB protection
Protect your system from badUSBs covertly executes malicious commands via disguised USB devices.
9
Enable BadUSB protection
When removable media is connected
Always block removable media
On-Access file scanning
Allow a user do selected actions on all removable media
Content Disarm and Reconstruction (CDR)
Note: CDR must be enabled in a corresponding security rule in the selected MetaDefender server for this policy
Use sanitized files if available

Application Control Policy:



No 3 – 7 is explained on the NEXT slide.



Explanation of the previous slide from No 3 - 7.

3. In the **Search for Application** field, you can use the search engine to search for any application (e.g AnyDesk) to flag if installed or start running in a device

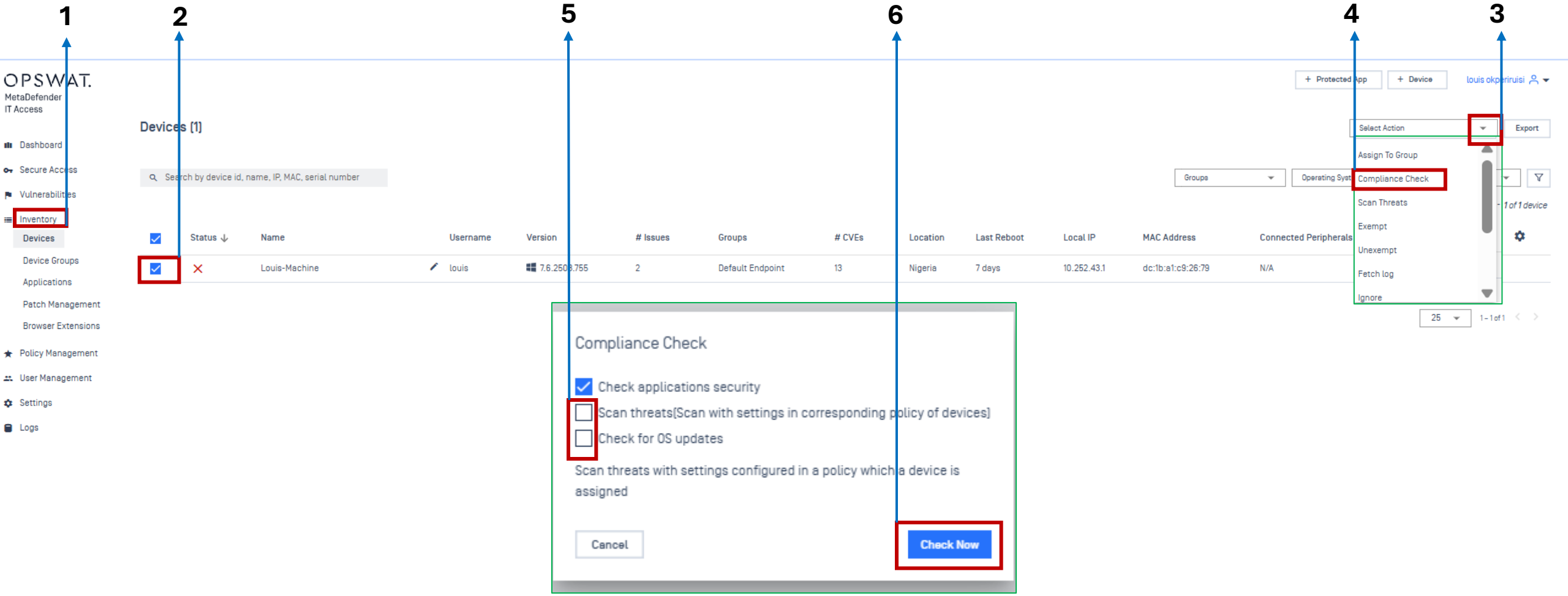
4. Here you can choose the **version** of the application you would like OPSWAT to flag if installed or if it's running in any computer in your environment.

5. In the **Severity Status**, it is configured to flag No issue or Warning or Critical if any application is either installed or running

6. The **Action** drop down field Uninstall or Disable or None to unwanted installed or running application. Depend on the action you would like OPSWAT to take.

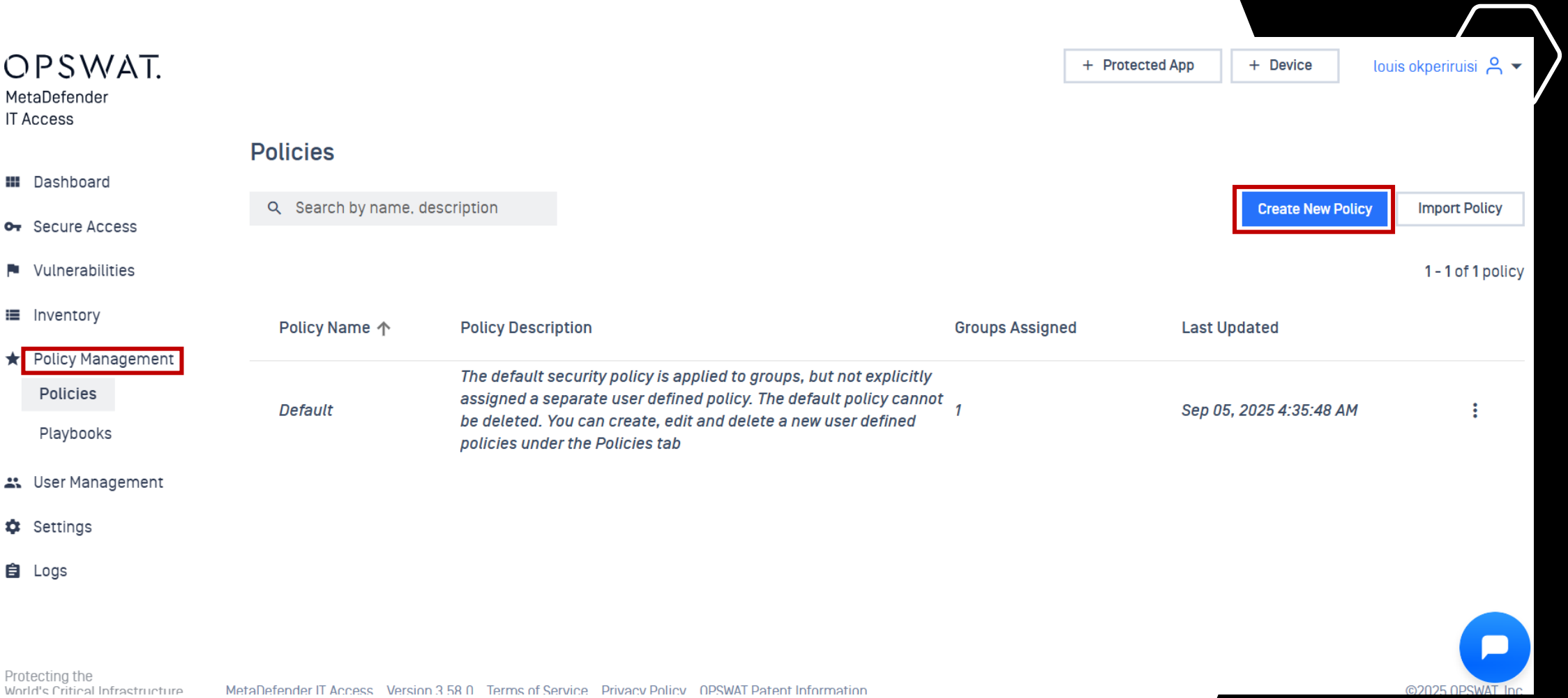
7. In this case the **Apply To** choose if the above stated conditions should apply to only, Servers or VMs or Desktop or Laptops

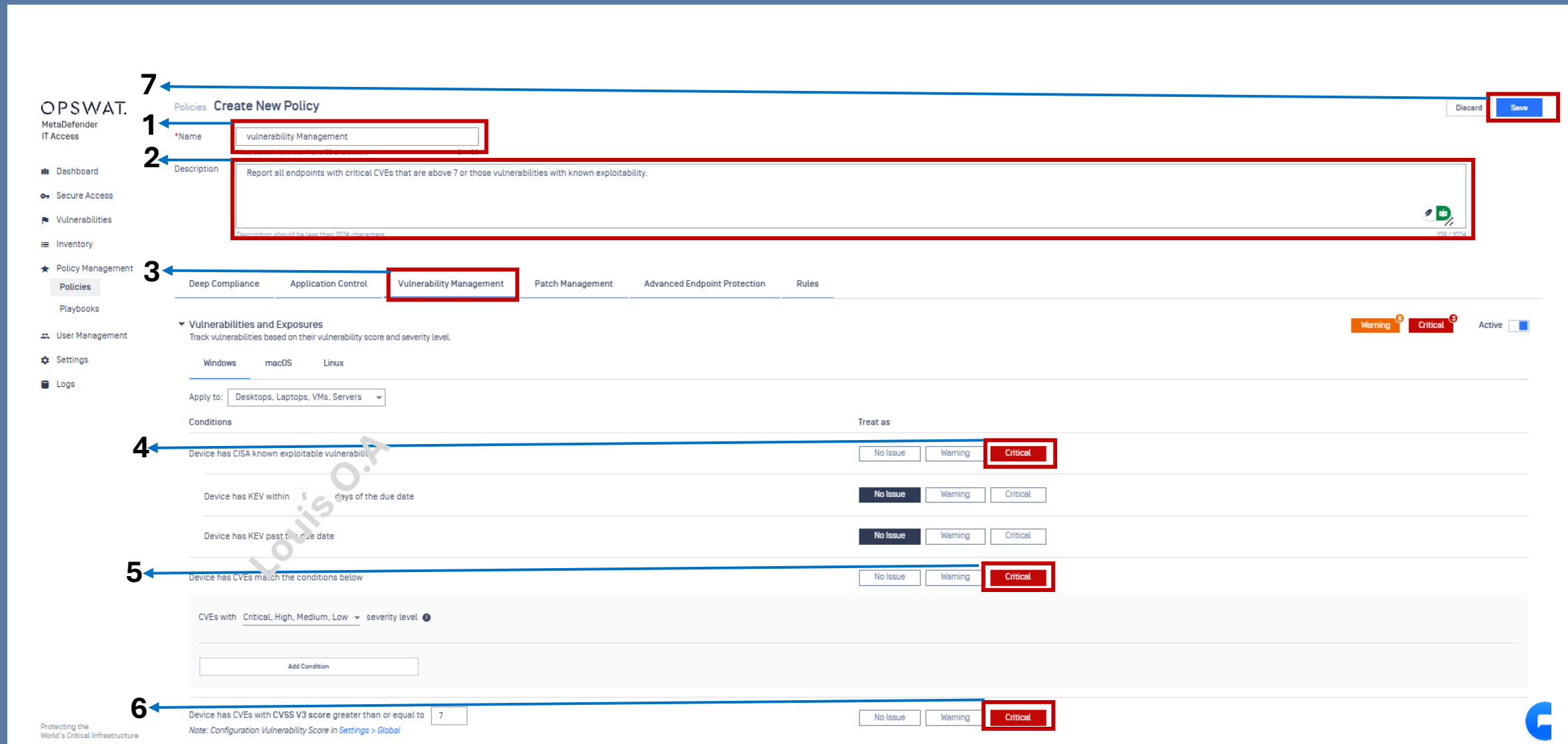
Continuation....



N:B. This Compliance Check pop-up Ensure that the device capture the information on time, and if you have more than one device, you can select them all at ones, then click on Select Action drop-down and select Fetch Log this will enforce the agent and the server communication, the new policy will be captured by the agent.

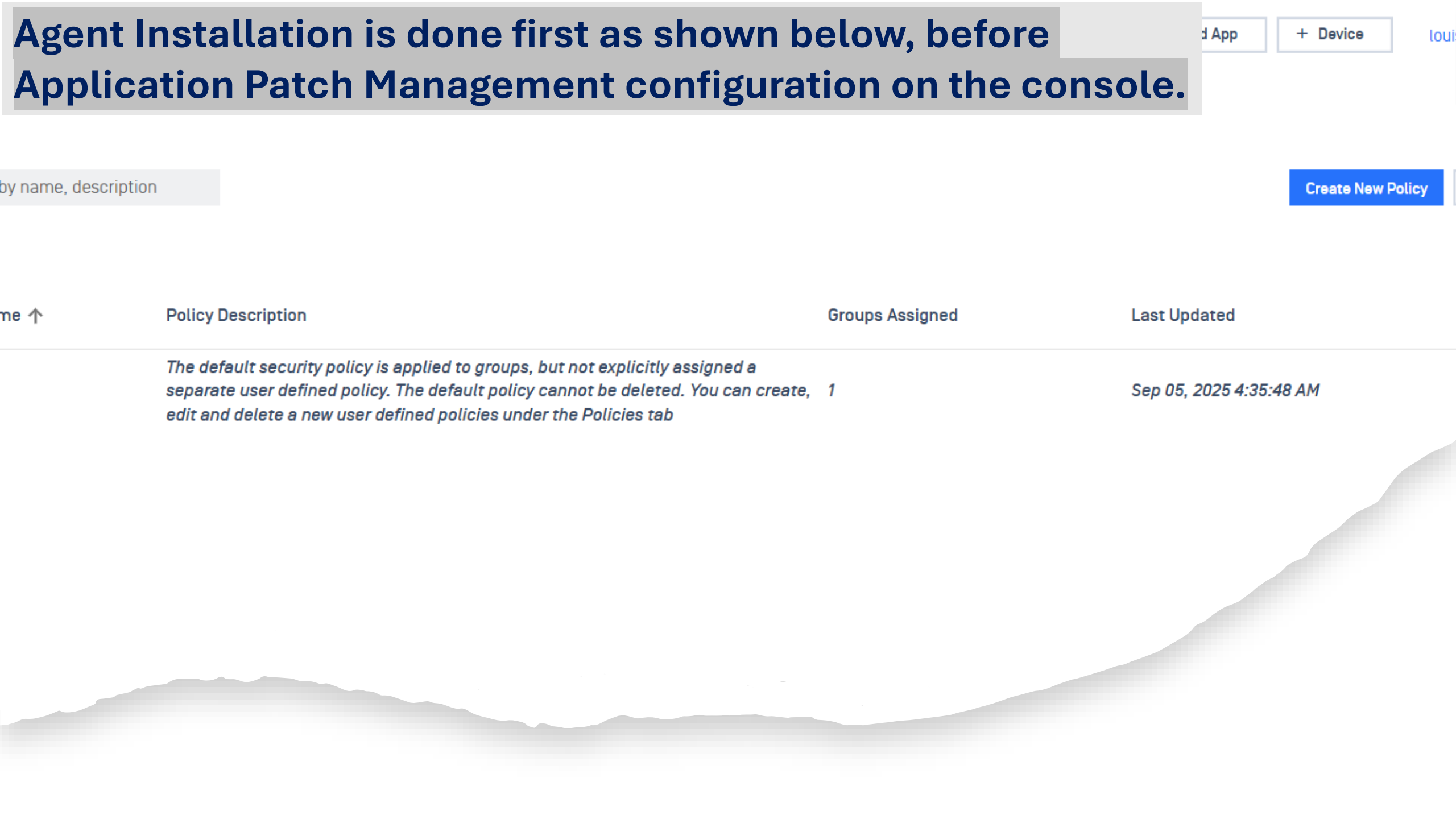
Vulnerability Management Policy:



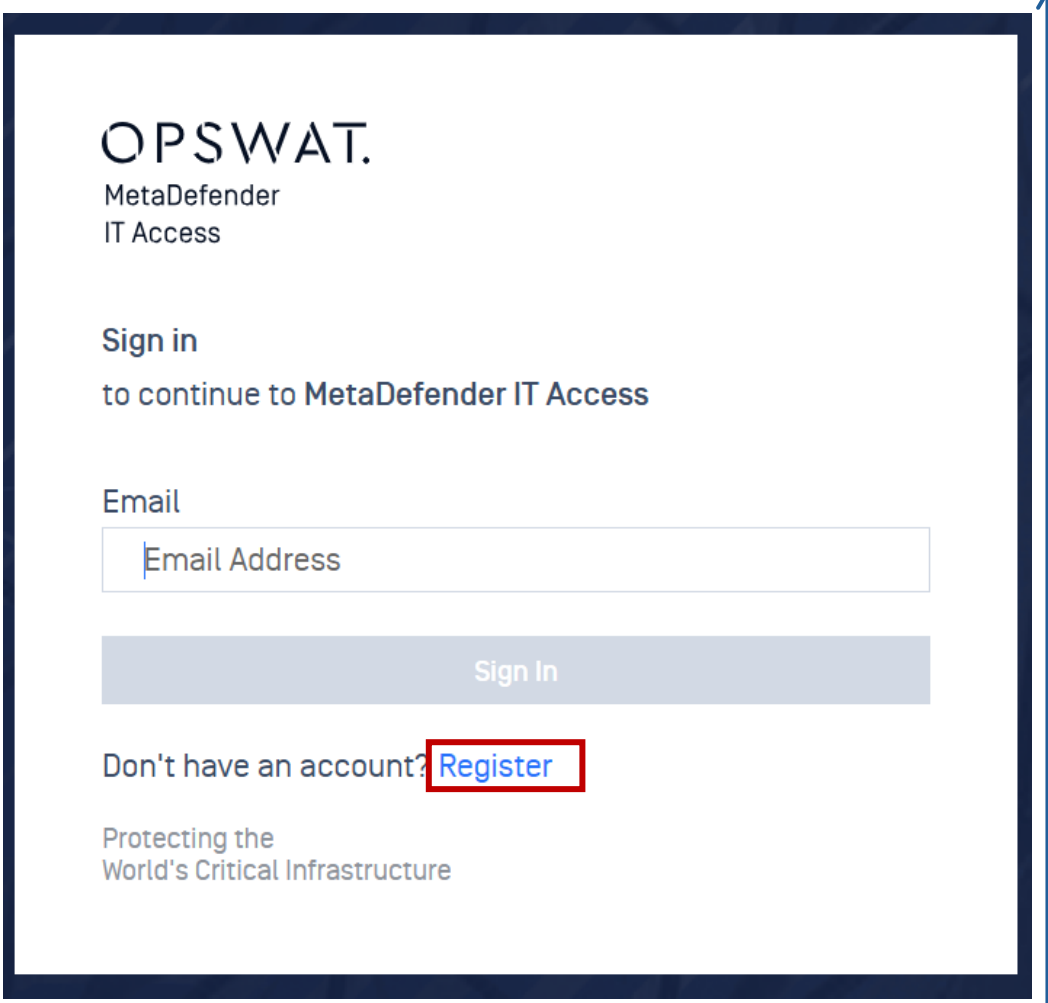

7
OPSWAT.
MetaDefender
IT Access
Policies
Create New Policy
Discard
Save
1
*Name
vulnerability Management
2
Description
Report all endpoints with critical CVEs that are above 7 or those vulnerabilities with known exploitability.
Dashboard
Secure Access
Vulnerabilities
Inventory
Policy Management
Policies
Playbooks
User Management
Settings
Logs
3
Deep Compliance
Application Control
Vulnerability Management
Patch Management
Advanced Endpoint Protection
Rules
Vulnerabilities and Exposures
Track vulnerabilities based on their vulnerability score and severity level.
Warning
Critical
Active
Windows
macOS
Linux
Apply to:
Desktops, Laptops, VMs, Servers
Conditions
Treat as
4
Device has CISA known exploitable vulnerabili
No Issue
Warning
Critical
Device has KEV within
5
days of the due date
Device has KEV past due date
5
Device has CVEs match the conditions below
CVEs with
Critical, High, Medium, Low
severity level
Add Condition
6
Device has CVEs with CVSS V3 score greater than or equal to
7
Note: Configuration Vulnerability Score in Settings > Global
Protecting the
World's Critical Infrastructure
Louis O.A

OPSWAT MetaDefender Platform Onboarding – Signing-Up

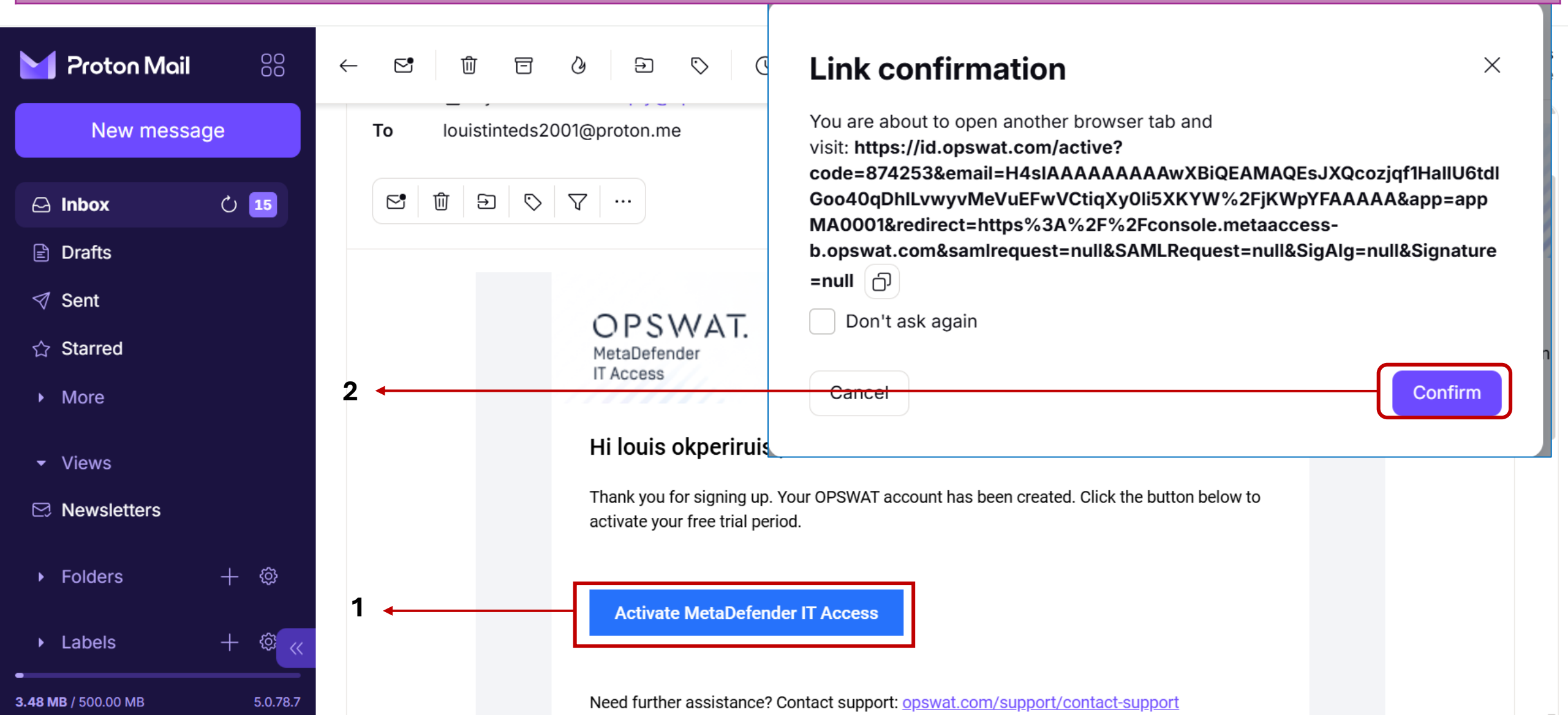
Agent Installation is done first as shown below, before Application Patch Management configuration on the console.



Visit: https://console.metaaccess-b.opswat.com/signin to register and Download OPSWAT



Confirmation Link Sent to Email-Box To Continue The Installation



OPSWAT.
MetaDefender
IT Access

1 Install MetaDefender Endpoint 2 Scan Device 3 Device Report

Connect your first device

Welcome louis okperiruisi,
Start by downloading and installing the MetaDefender Endpoint, it will automatically connect to MetaDefender IT Access, then you can access your device report in MetaDefender IT Access.

Windows

Download MetaDefender Endpoint for Windows

SHA256 16f3dda0bb6411a0880ab31a...

*The do... ...your account, to

+ Protected App + Device louis okperiruisi

Complete the registration of the MetaDefender Endpoint on this device.

Complete Registration

No Devices Monitored. You can monitor up to 50 devices.

Add Devices

In order to monitor additional devices, please contact us to upgrade your account.

nfrastructure

Add Devices

Endpoint Devices

To monitor devices, simply download the MetaDefender Endpoint and run it on the endpoint machine.

☑ Devices will be automatically assigned to this group: Default Endpoint

Download MetaDefender Endpoint for Distribution

Windows, macOS, Linux, Android & Chrome OS, iOS

Copy the download link to clipboard

OPSWAT.
MetaDefender
IT Access

Download MetaDefender Endpoint®

The MetaDefender Endpoint allows your MetaDefender IT Access administrator to view the security status of your device. It does not enable remote control, remote management or access to your private information and documents.

Windows | macOS | Linux | Mobile & Chrome OS | IoT

MetaDefender Endpoint For Windows®

Windows 7-11, Server 2008-2022

The MetaDefender Endpoint is preconfigured for: louis okperiruisi, do not alter the filename

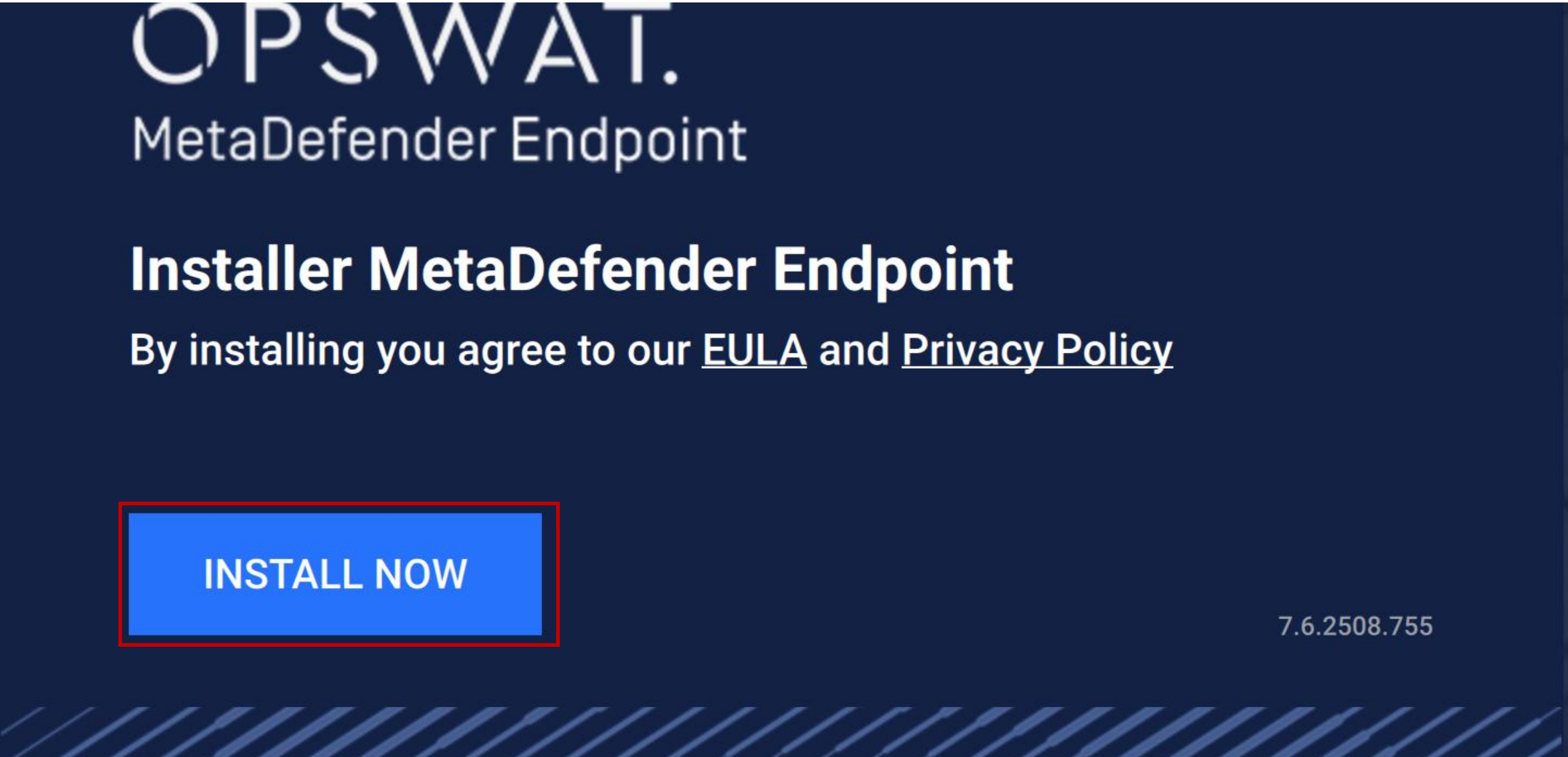
Persistent MetaDefender Endpoint	On-Demand MetaDefender Endpoint	Limited On-Demand MetaDefender Endpoint
• You **have admin permission to the device** • Run the MetaDefende **perpetually**	• You **have admin permission to the device** • Run the MetaDefender Endpoint **temporarily**	• You **do not have admin permission to the device** • Run the MetaDefender Endpoint **temporarily**
.msi .exe Persistent Client .exe	On-Demand Client	Limited Client

3

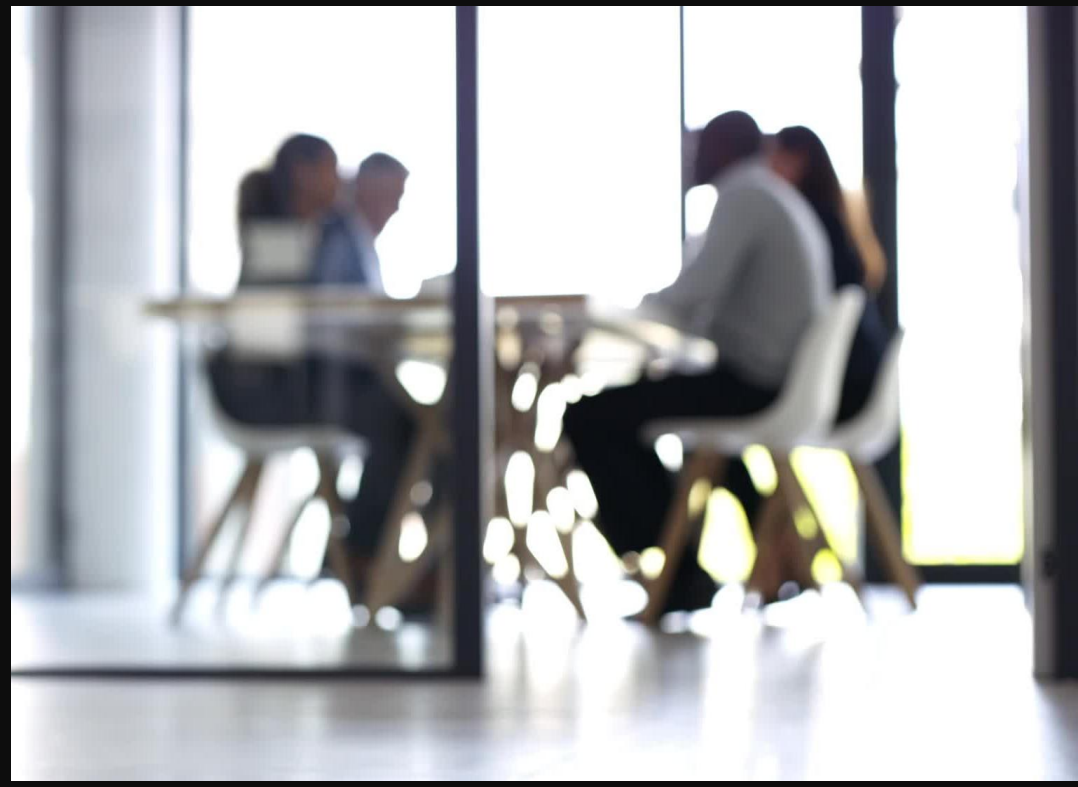
2

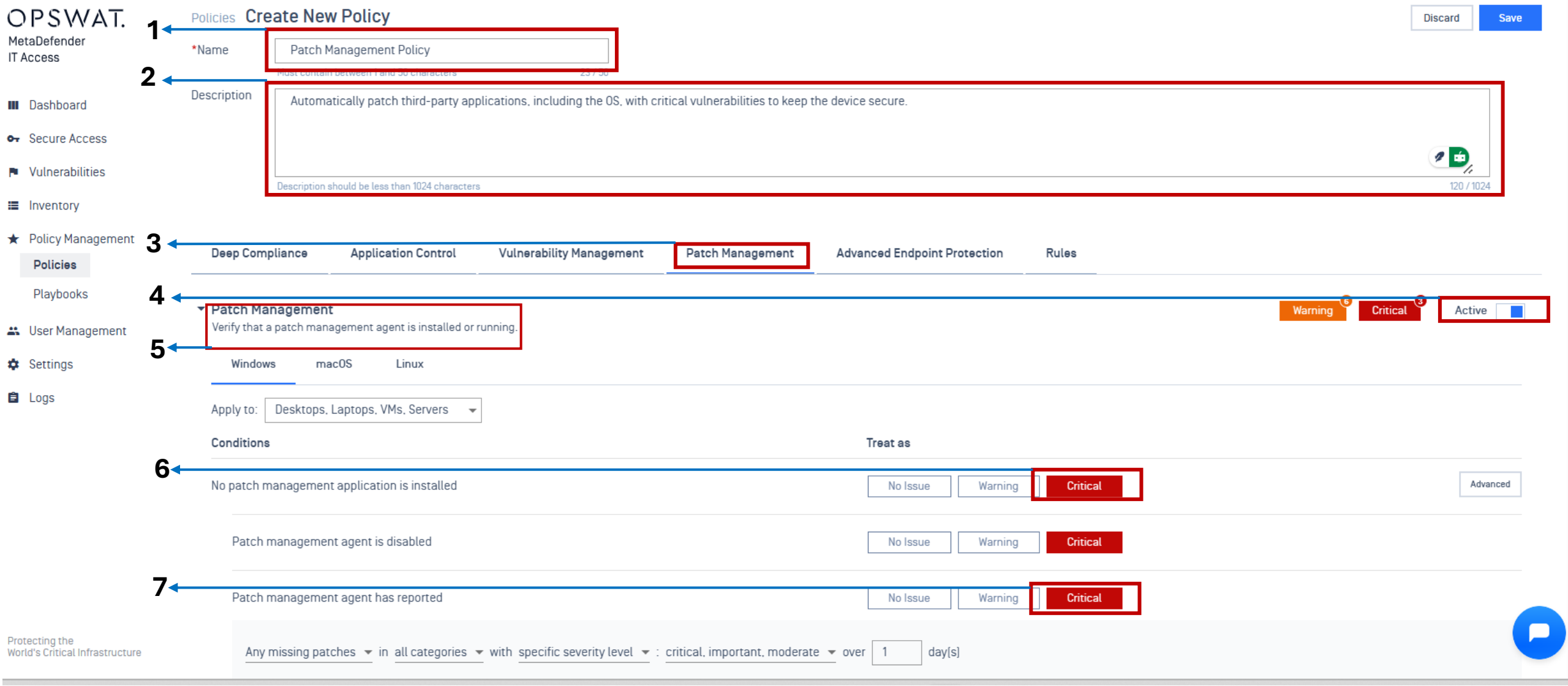
1

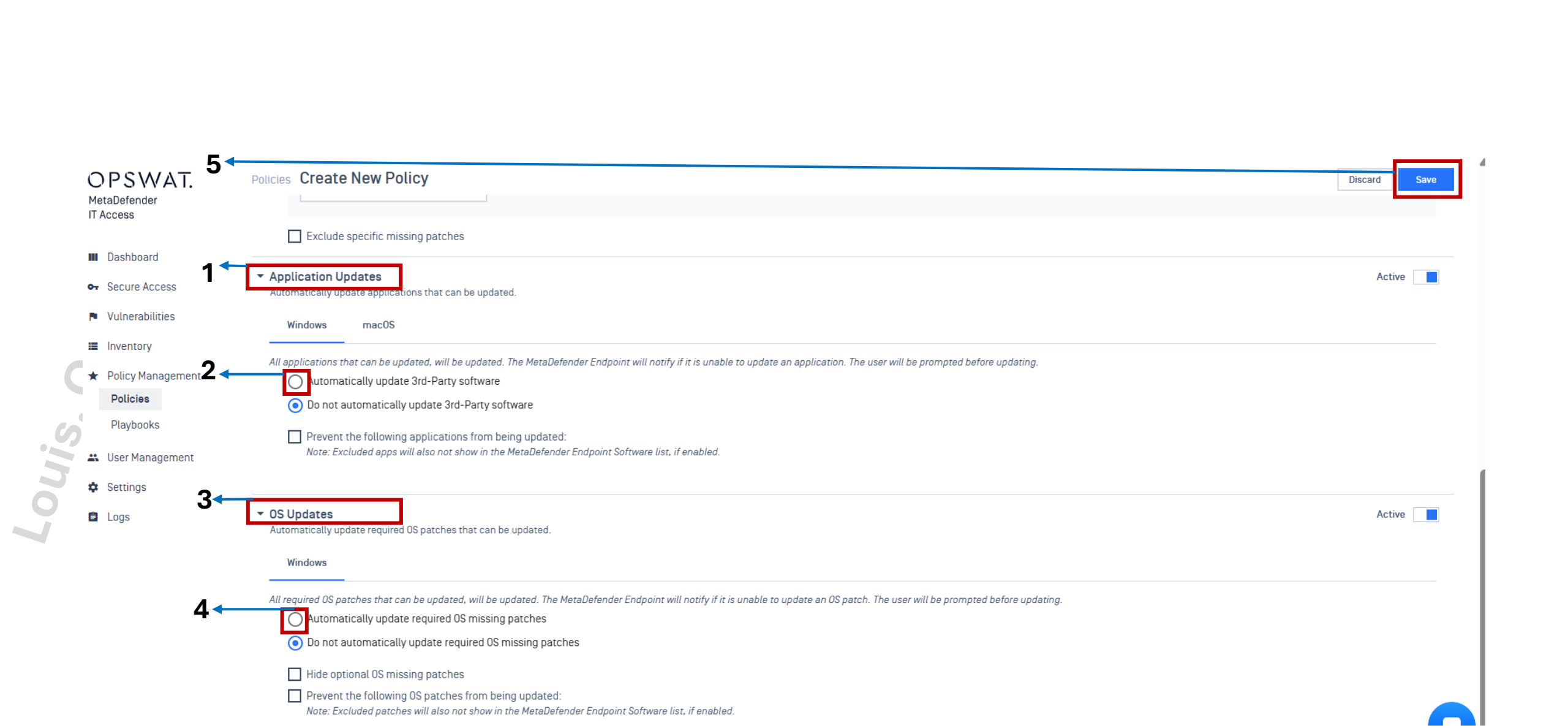
Install the downloaded OPSWAT MetaDefender Endpoint Agent Used for Application Patching/ Update.

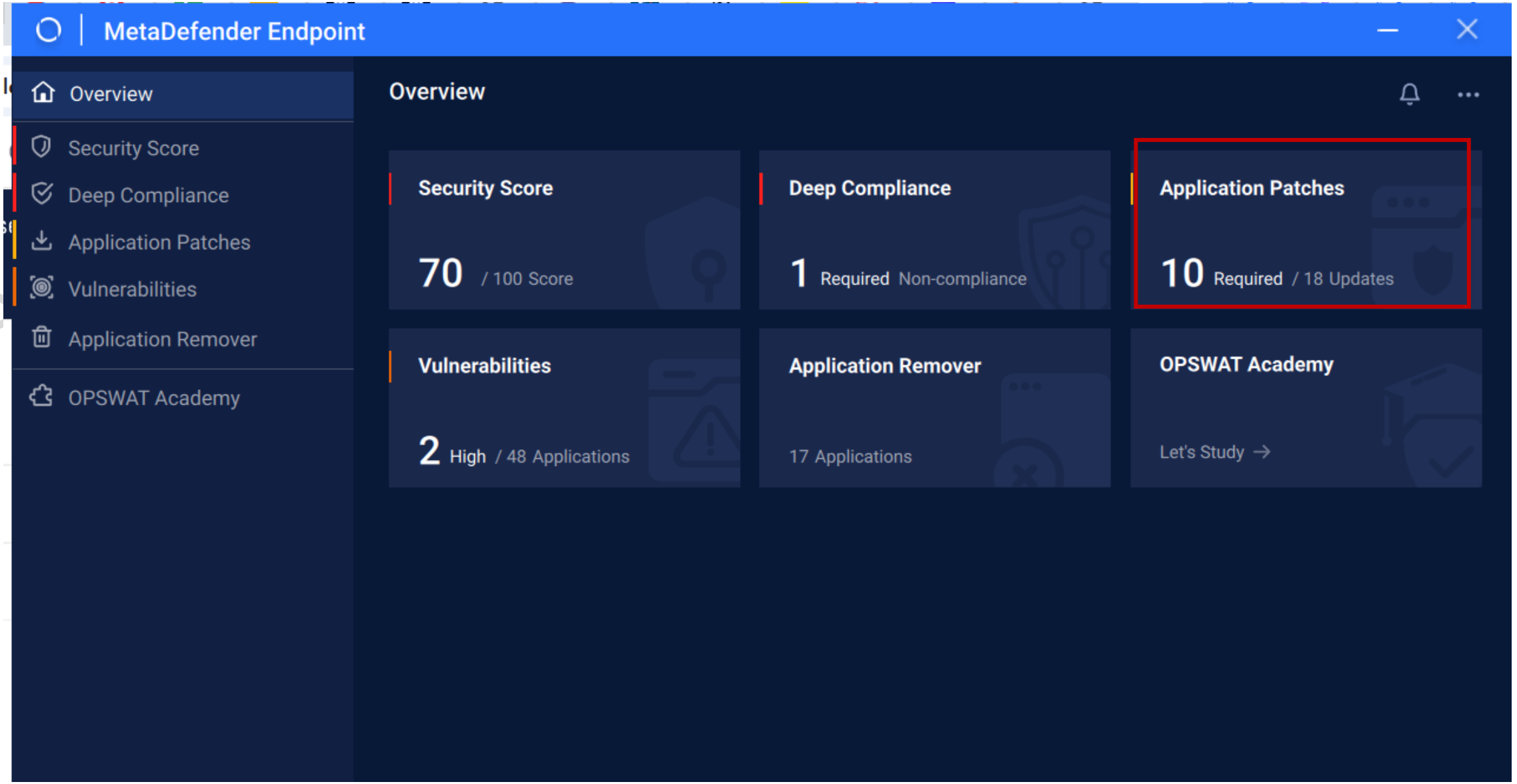


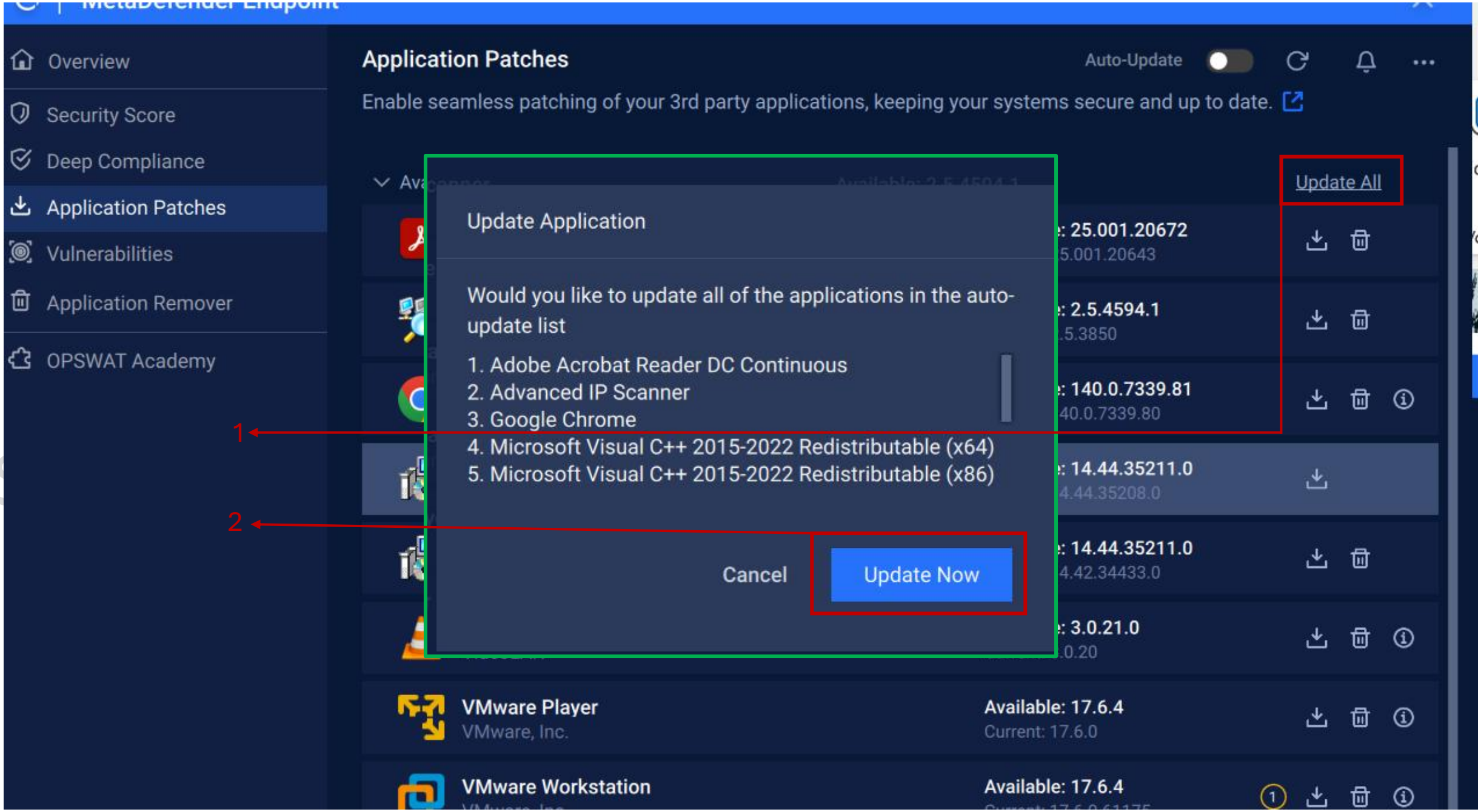
Patch management Agent installed, now we can proceed to Patch Management Policy configurations as shown below.

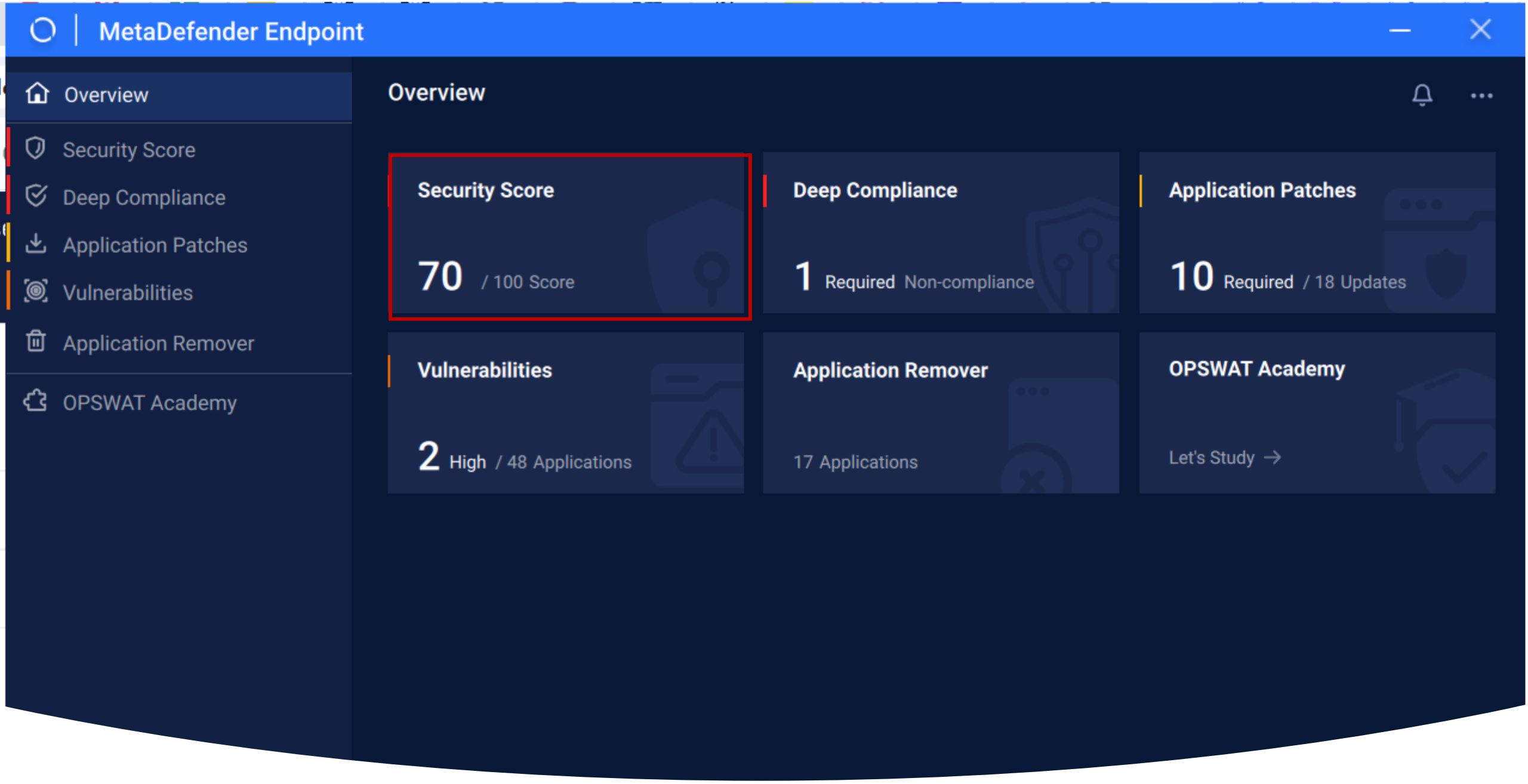


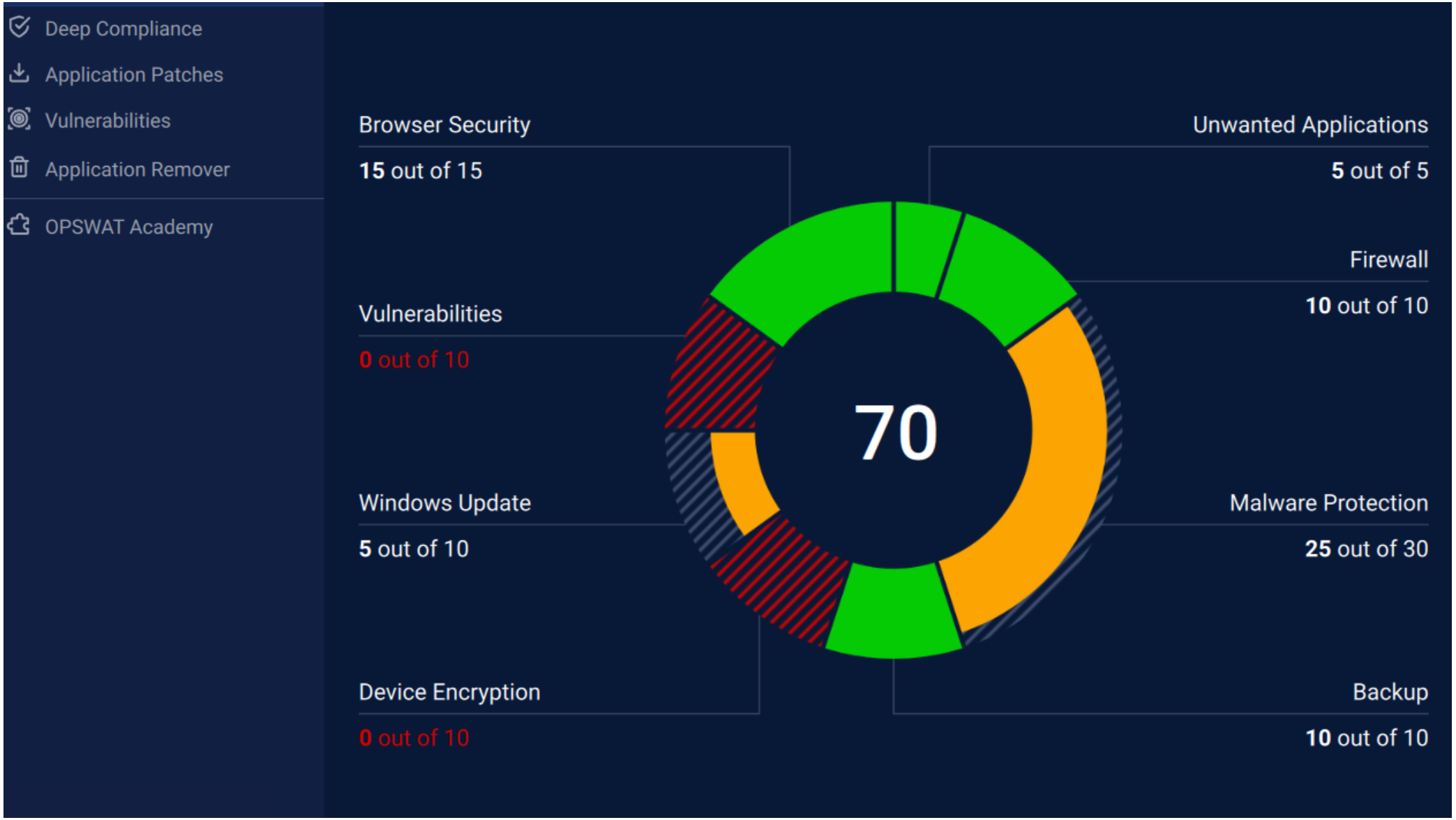

OPSWAT.
MetaDefender
IT Access
Dashboard
Secure Access
Vulnerabilities
Inventory
Policy Management
Policies
Playbooks
User Management
Settings
Logs
Protecting the
World's Critical Infrastructure
Policies
Create New Policy
Discard
Save
1
*Name
Patch Management Policy
2
Description
Automatically patch third-party applications, including the OS, with critical vulnerabilities to keep the device secure.
Description should be less than 1024 characters
120 / 1024
3
Deep Compliance
Application Control
Vulnerability Management
Patch Management
Advanced Endpoint Protection
Rules
4
Patch Management
Verify that a patch management agent is installed or running.
Warning
Critical
Active
5
Windows
macOS
Linux
Apply to:
Desktops, Laptops, VMs, Servers
Conditions
Treat as
6
No patch management application is installed
No Issue
Warning
Critical
Advanced
Patch management agent is disabled
No Issue
Warning
Critical
7
Patch management agent has reported
No Issue
Warning
Critical
Any missing patches
in
all categories
with
specific severity level
:
critical, important, moderate
over
1
day(s)

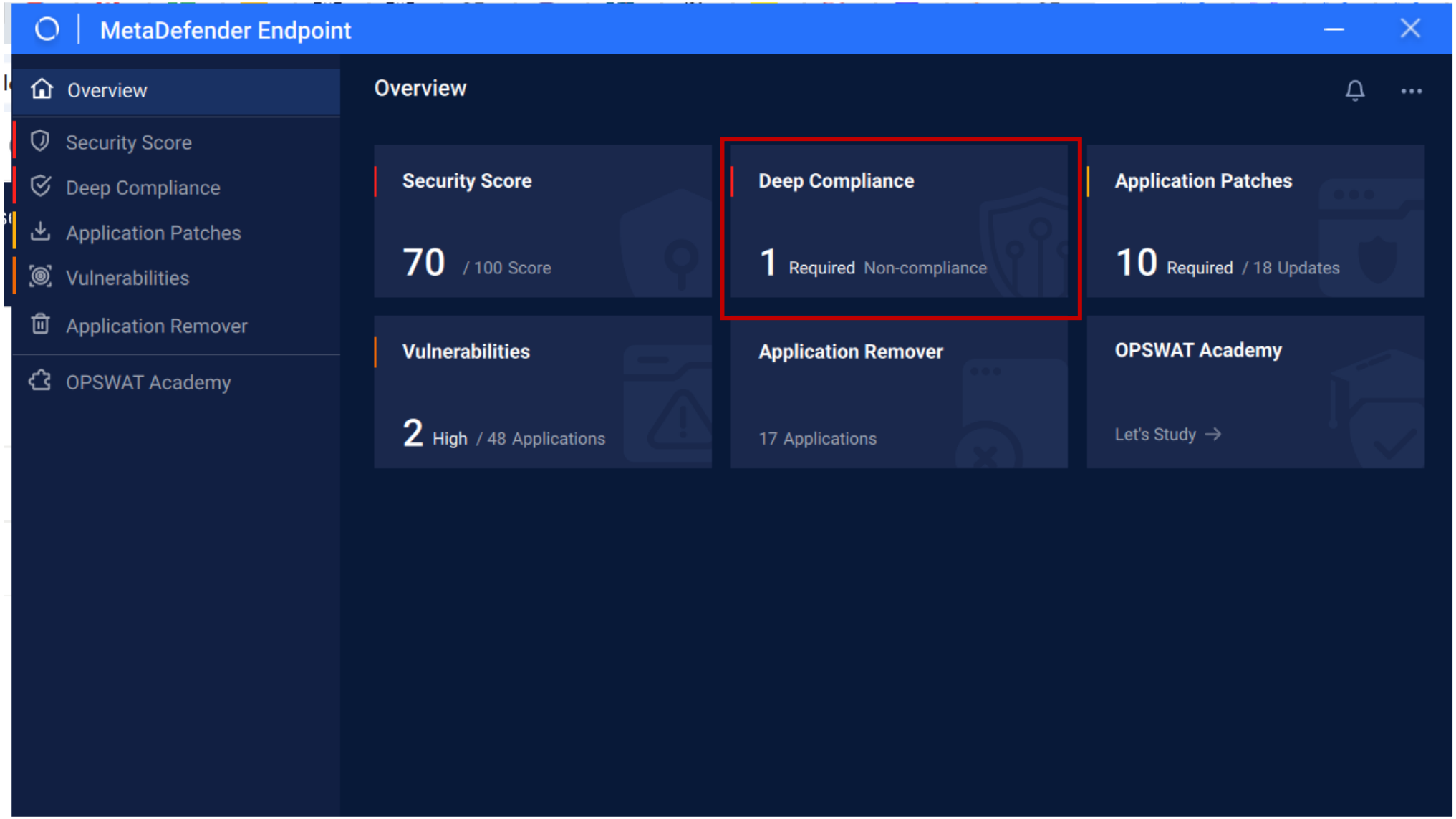

OPSWAT.
MetaDefender
IT Access
Dashboard
Secure Access
Vulnerabilities
Inventory
Policy Management
Policies
Playbooks
User Management
Settings
Logs
Policies
Create New Policy
Discard
Save
5
Exclude specific missing patches
1
Application Updates
Automatically update applications that can be updated.
Active
Windows
macOS
All applications that can be updated, will be updated. The MetaDefender Endpoint will notify if it is unable to update an application. The user will be prompted before updating.
2
Automatically update 3rd-Party software
Do not automatically update 3rd-Party software
Prevent the following applications from being updated:
Note: Excluded apps will also not show in the MetaDefender Endpoint Software list, if enabled.
3
OS Updates
Automatically update required OS patches that can be updated.
Active
Windows
All required OS patches that can be updated, will be updated. The MetaDefender Endpoint will notify if it is unable to update an OS patch. The user will be prompted before updating.
4
Automatically update required OS missing patches
Do not automatically update required OS missing patches
Hide optional OS missing patches
Prevent the following OS patches from being updated:
Note: Excluded patches will also not show in the MetaDefender Endpoint Software list, if enabled.

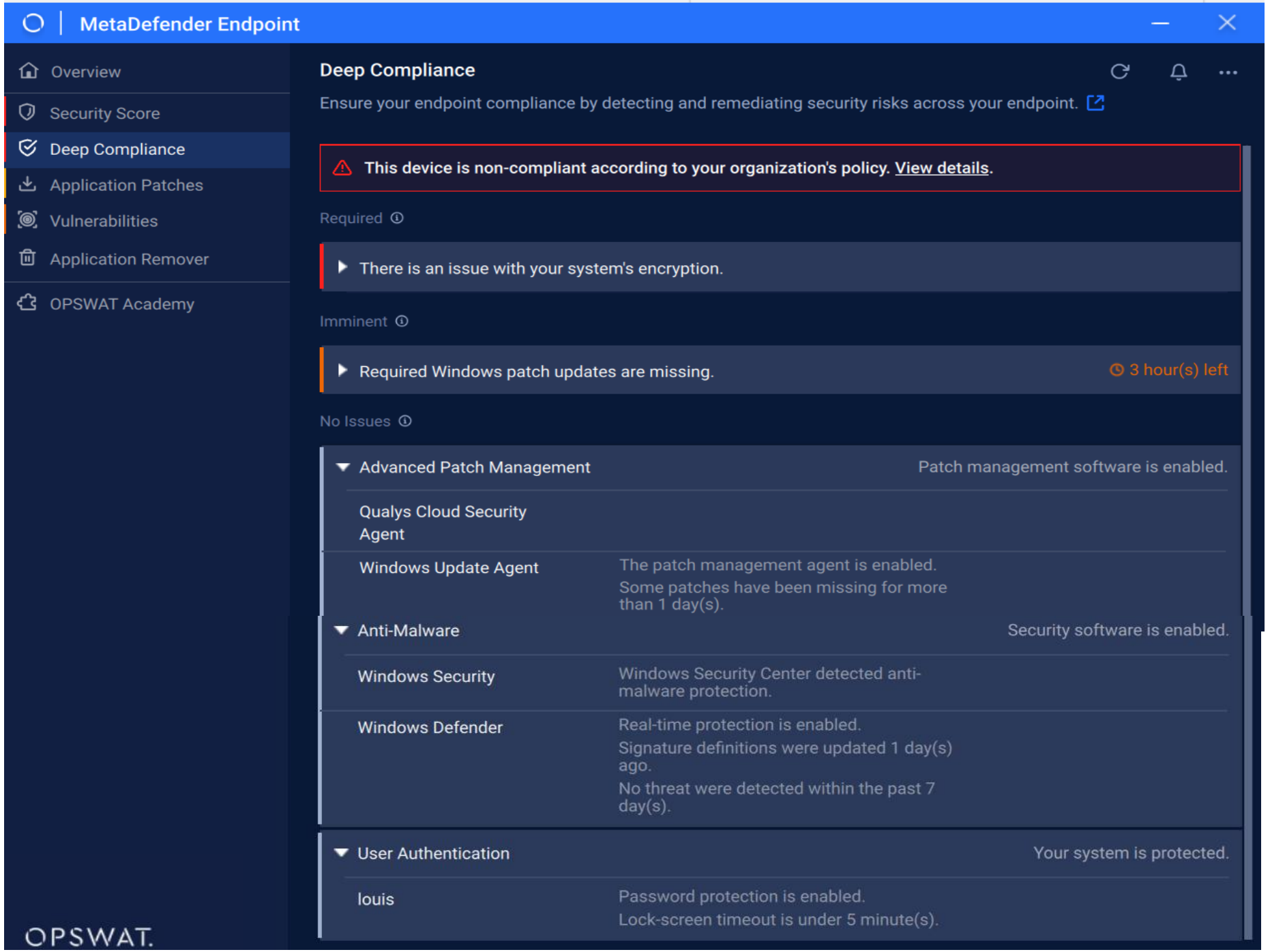

MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Overview
Security Score
70 / 100 Score
Deep Compliance
1 Required Non-compliance
Application Patches
10 Required / 18 Updates
Vulnerabilities
2 High / 48 Applications
Application Remover
17 Applications
OPSWAT Academy
Let's Study

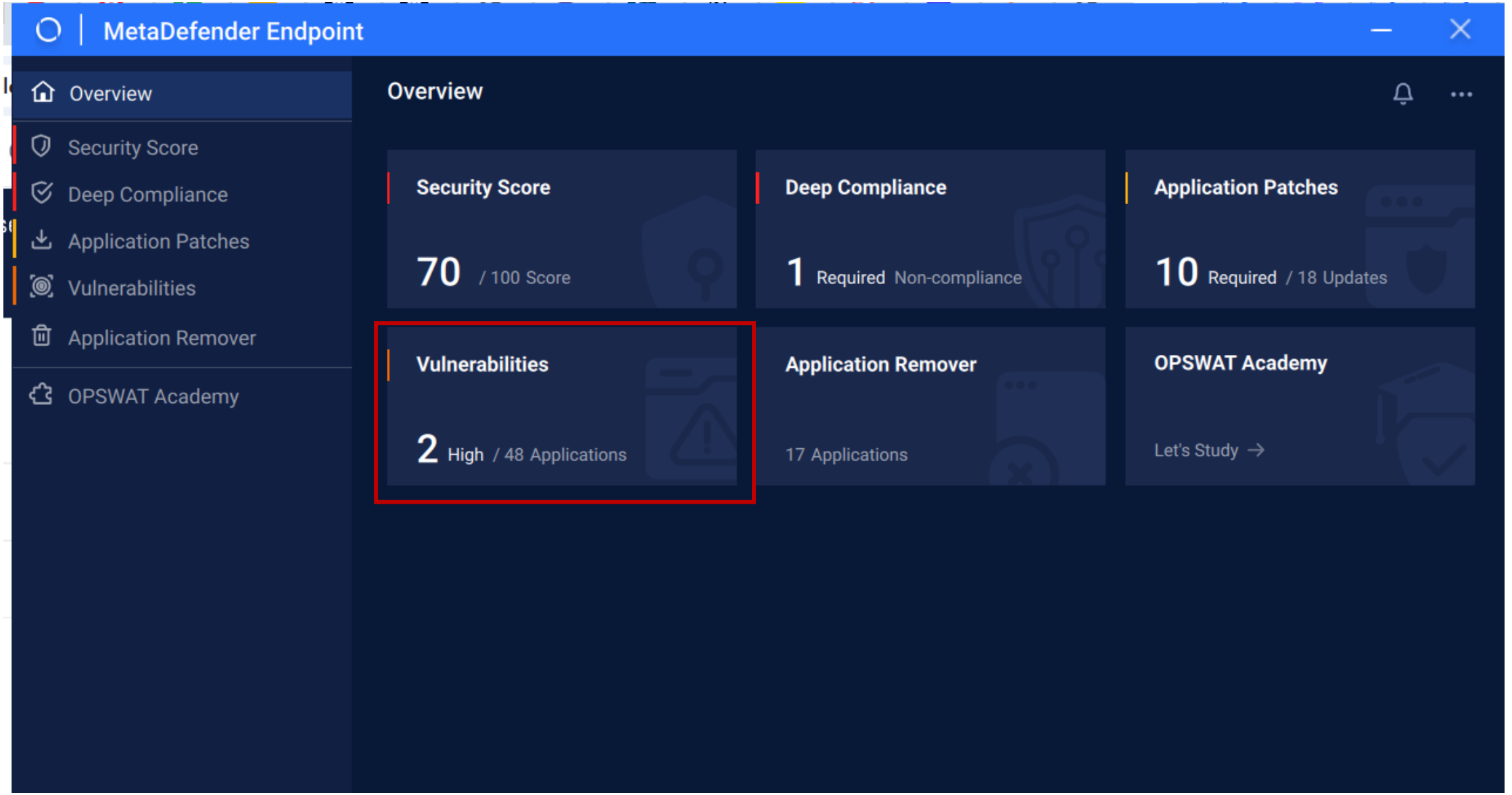

Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Application Patches
Auto-Update
Enable seamless patching of your 3rd party applications, keeping your systems secure and up to date.
Update All
Update Application
Would you like to update all of the applications in the auto-update list
1. Adobe Acrobat Reader DC Continuous
2. Advanced IP Scanner
3. Google Chrome
4. Microsoft Visual C++ 2015-2022 Redistributable (x64)
5. Microsoft Visual C++ 2015-2022 Redistributable (x86)
Cancel
Update Now
1
2
: 25.001.20672
5.001.20643
: 2.5.4594.1
.5.3850
: 140.0.7339.81
40.0.7339.80
: 14.44.35211.0
4.44.35208.0
: 14.44.35211.0
4.42.34433.0
: 3.0.21.0
.0.20
VMware Player
VMware, Inc.
Available: 17.6.4
Current: 17.6.0
VMware Workstation
Available: 17.6.4

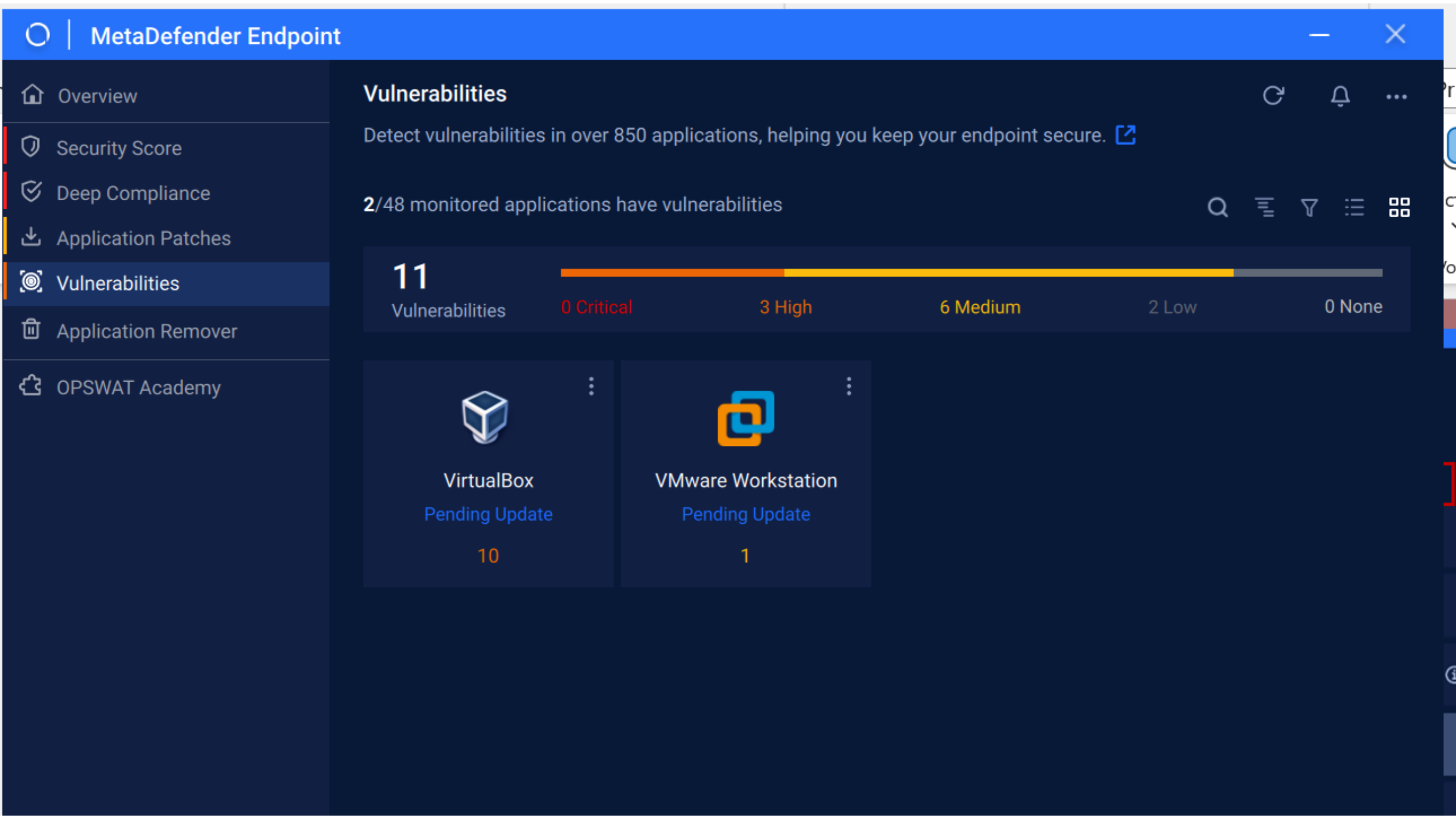

MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Overview
Security Score
70 / 100 Score
Deep Compliance
1 Required Non-compliance
Application Patches
10 Required / 18 Updates
Vulnerabilities
2 High / 48 Applications
Application Remover
17 Applications
OPSWAT Academy
Let's Study →

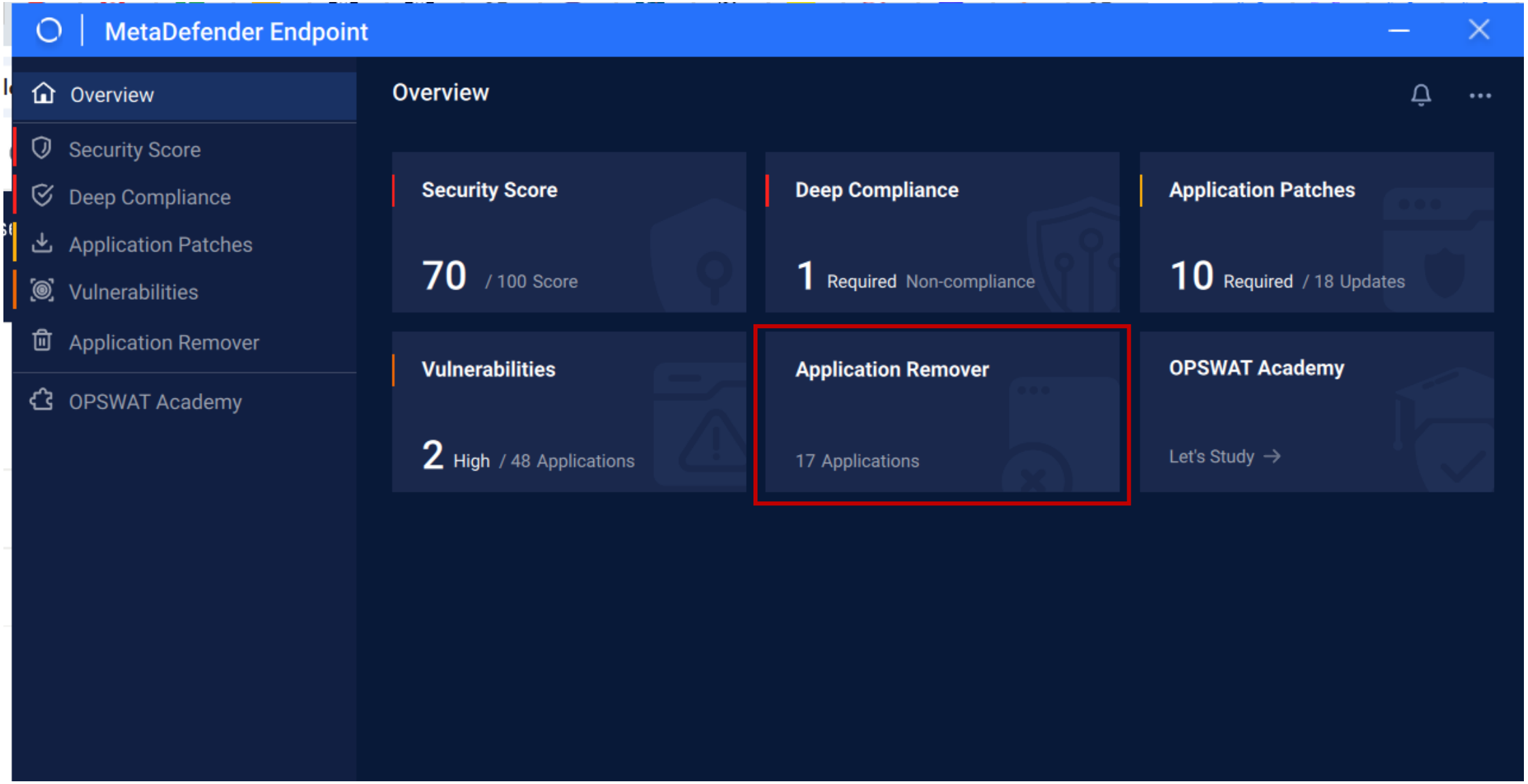

Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Browser Security
15 out of 15
Vulnerabilities
0 out of 10
Windows Update
5 out of 10
Device Encryption
0 out of 10
Unwanted Applications
5 out of 5
Firewall
10 out of 10
Malware Protection
25 out of 30
Backup
10 out of 10
70

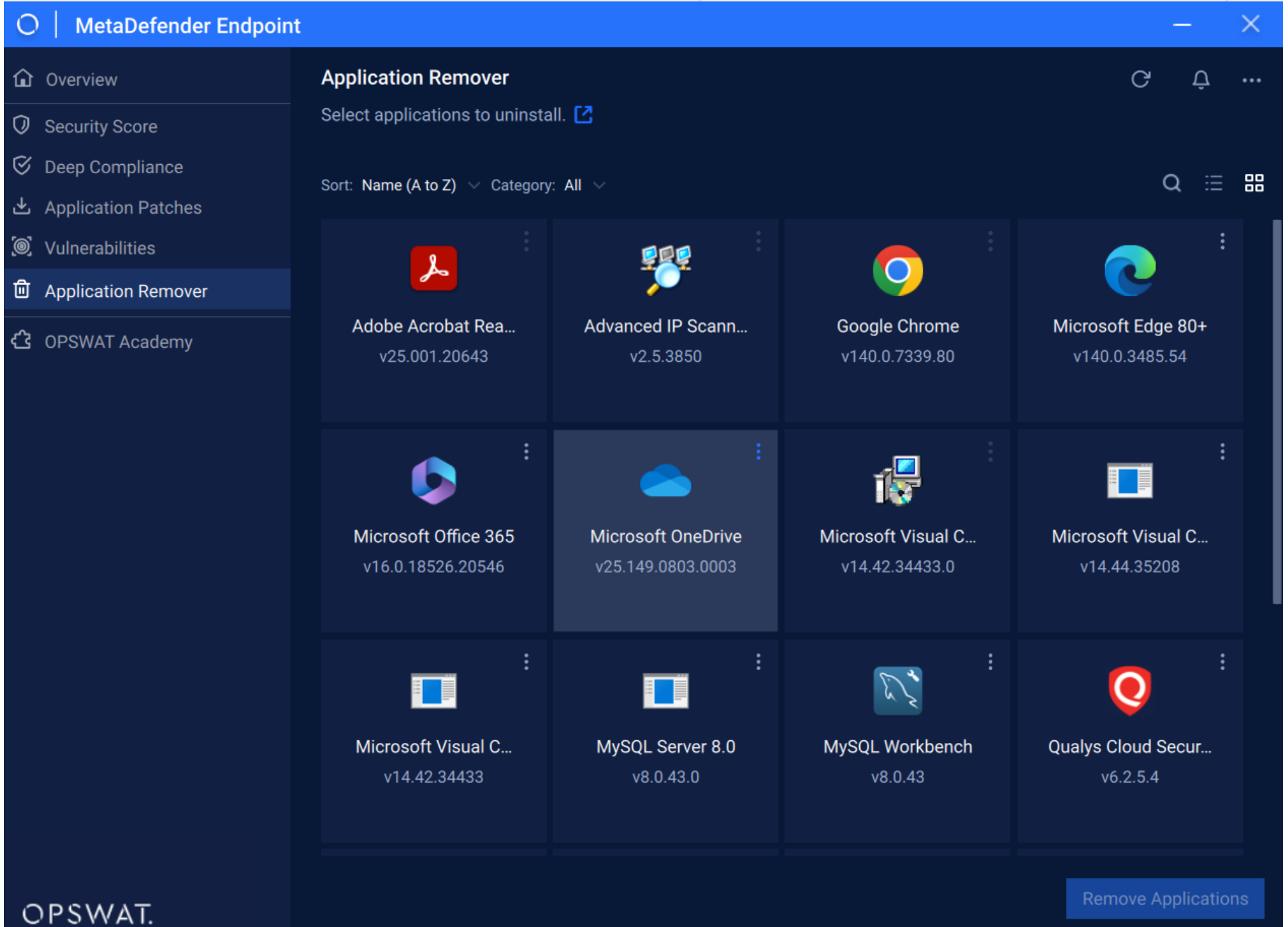

MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Overview
Security Score
70 / 100 Score
Deep Compliance
1 Required Non-compliance
Application Patches
10 Required / 18 Updates
Vulnerabilities
2 High / 48 Applications
Application Remover
17 Applications
OPSWAT Academy
Let's Study


MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Deep Compliance
Ensure your endpoint compliance by detecting and remediating security risks across your endpoint.
This device is non-compliant according to your organization's policy. View details.
Required
There is an issue with your system's encryption.
Imminent
Required Windows patch updates are missing.
3 hour(s) left
No Issues
Advanced Patch Management
Patch management software is enabled.
Qualys Cloud Security Agent
Windows Update Agent
The patch management agent is enabled.
Some patches have been missing for more than 1 day(s).
Anti-Malware
Security software is enabled.
Windows Security
Windows Security Center detected anti-malware protection.
Windows Defender
Real-time protection is enabled.
Signature definitions were updated 1 day(s) ago.
No threat were detected within the past 7 day(s).
User Authentication
Your system is protected.
louis
Password protection is enabled.
Lock-screen timeout is under 5 minute(s).
OPSWAT.


MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Overview
Security Score
70 / 100 Score
Deep Compliance
1 Required Non-compliance
Application Patches
10 Required / 18 Updates
Vulnerabilities
2 High / 48 Applications
Application Remover
17 Applications
OPSWAT Academy
Let's Study →


MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Vulnerabilities
Detect vulnerabilities in over 850 applications, helping you keep your endpoint secure.
2/48 monitored applications have vulnerabilities
11
Vulnerabilities
0 Critical
3 High
6 Medium
2 Low
0 None
VirtualBox
Pending Update
10
VMware Workstation
Pending Update
1


MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Overview
Security Score
70 / 100 Score
Deep Compliance
1 Required Non-compliance
Application Patches
10 Required / 18 Updates
Vulnerabilities
2 High / 48 Applications
Application Remover
17 Applications
OPSWAT Academy
Let's Study


MetaDefender Endpoint
Overview
Security Score
Deep Compliance
Application Patches
Vulnerabilities
Application Remover
OPSWAT Academy
Application Remover
Select applications to uninstall.
Sort: Name (A to Z)
Category: All
Adobe Acrobat Rea...
v25.001.20643
Advanced IP Scann...
v2.5.3850
Google Chrome
v140.0.7339.80
Microsoft Edge 80+
v140.0.3485.54
Microsoft Office 365
v16.0.18526.20546
Microsoft OneDrive
v25.149.0803.0003
Microsoft Visual C...
v14.42.34433.0
Microsoft Visual C...
v14.44.35208
Microsoft Visual C...
v14.42.34433
MySQL Server 8.0
v8.0.43.0
MySQL Workbench
v8.0.43
Qualys Cloud Secur...
v6.2.5.4
Remove Applications
OPSWAT.

Thank you!