

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

Louis.



Presented By Okperiruisi Louis

5<sup>th</sup> 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:

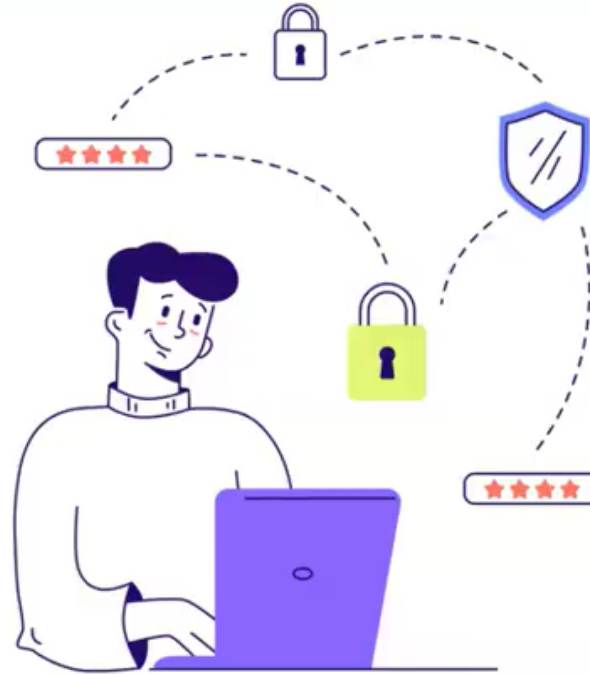
- Advanced Malware Detection Policy
- Full Scan or Custom Scan Policy
- Data Loss Prevention Policy
- Application Control Policy
- Vulnerability Management Policy
- Patch Management Policy
- Threat Monitoring Policy

## 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

chrome web store

Search extensions and themes

over **Extensions** Themes



# OPSWAT File Security for Browser

Add to Chrome

Featured 4.3 ★ (74 ratings) Share

Extension Workflow & Planning 7,000 users

OPSWAT File Security for Chrome

Scan History

3 files scanned

FILENAME	SCAN TIME	RESULTS
U067581HN 80988886672083C0D438826763841D064867D4228C4F9C0C8B819320D	3 minutes ago	No threats found ✓
1909488f10097_9e7d1dc19113e4e6980_36.png D60744383DA1C846D4B1A778067E7E3955E68AEE7720F81D0E42B42DF	3 minutes ago	No threats found ✓
T056411V5-U067581HN-2abbaad50db-48 718CF98829742864E068754925C7D083E373FC4EE0F889AC84C242C7264	3 minutes ago	No threats found ✓

OPSWAT File Security for Chrome

About

Thank you for installing OPSWAT File Security for Chrome! This extension gives you the ability to scan downloads\* for malware with 30+ anti-malware engines using OPSWAT's MetaDefender Cloud.

Your MetaDefender API KEY info

LIMIT INTERVAL: easy  
REPUTATION API LIMIT: 500  
PREVENTION API LIMIT: 3  
FEED API LIMIT: 1000  
SANDBOX API LIMIT: 1  
PAID USER: 0  
MAXIMUM FILE SIZE: 75

Add "OPSWAT File Security for Browser"?

It can:

- Read and change all your data on all websites
- Display notifications
- Manage your downloads

Add extension Cancel

1

2

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

The screenshot shows the eicar.org website interface. At the top right, there is a contact number '+49 8194 99 84 99' and a 'CONTACT' link. The main navigation includes 'TEAM', 'NEWS', 'PROJECTS', and 'MEMBERSHIP'. A prominent blue button reads 'DOWNLOAD ANTI MALWARE TESTFILE'. The central content area is titled 'DOWNLOAD AREA' and features a security notice: 'Use a secure, SSL enabled protocol HTTPS'. Below this, four download cards are displayed: 'EICAR.COM' (Com-file), 'EICAR.TXT' (1 Text-file), 'EICAR.COM-ZIP', and 'EICAR.COM2-ZIP'. A context menu is open over the 'EICAR.COM' card, with the 'Scan with OPSWAT' option highlighted in red. A red box also encloses the 'EICAR.COM' card and the context menu. Two red arrows with numbers '1' and '2' indicate the sequence of actions: arrow '1' points to the 'DOWNLOAD' button of the 'EICAR.COM' card, and arrow '2' points to the 'Scan with OPSWAT' option in the context menu.

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

+49 8194 99 84 99 CONTACT



EICAR | ABOUT | TEAM | NEWS | PROJECTS | MEMBERSHIP

DOWNLOAD ANTI MALWARE TESTFILE



# DOWNLOAD AREA

using the secure, SSL enabled protocol HTTPS

COM

EICAR.COM

DOWNLOAD

Com-file



EICAR.TXT

DOWNLOAD

1 Text-file



EICAR.COM-

ZIP

DOWNLOAD



ZIP

Google Chrome



OPSWAT File Security for Browser  
eicar.com has been scanned.

Threat detected!



Scan History →

Settings





About

Search history



2 files scanned

CLEAR SCAN HISTORY

FILENAME	SCAN TIME	RESULTS
 <b>eicar.com</b> 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AA BF651FD0F	a few seconds ago	Infected / Known 
 <b>eicar.com</b> 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AA BF651FD0F	16 minutes ago	Infected / Known 

Processed file [Add to Catalogue](#) SHA-256: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

**txt** **eicar.com** Not Available (Country of Origin) [Add COO](#)

**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 16 /22 ENGINES

Threats Detected

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
File Size	30 B	Company Name	-

### Scan History

This file has been scanned 200 times

### Deep CDR™ Regeneration

No Sanitization Available

After Data Sanitization

[Download Sanitized Version](#)

Louis

## 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

OPSWAT.

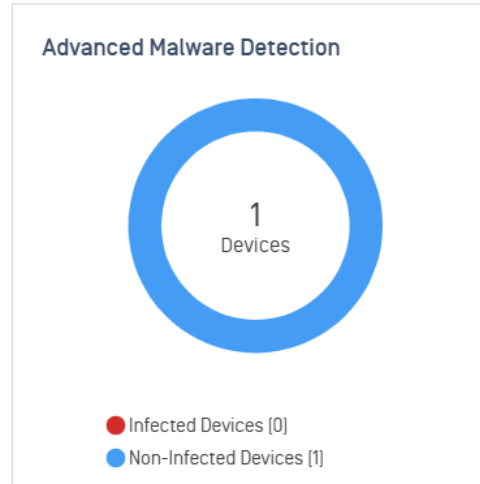
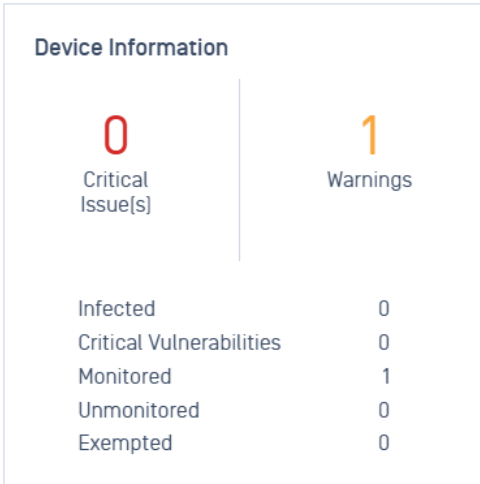
MetaDefender  
IT Access

- Dashboard
- Overview**
- Secure Access
- Vulnerabilities
- Compliance
- Threat Detection
- Secure Access
- Vulnerabilities
- Inventory
- ★ Policy Management**
- User Management
- Settings
- Logs

+ Protected App + Device louis okperiruisi

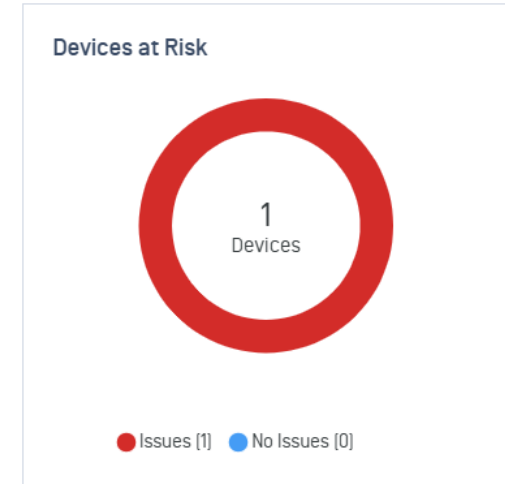
## Overview

Filter by Group



### Active Secure IT Access Sessions

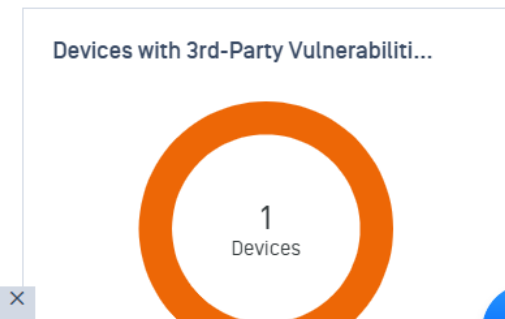
This chart requires an account upgrade. Please contact [OPSWAT Sales](#) to upgrade your account.



### Protected IdP App Accesses in the last 24hrs

Protect your cloud applications from risky devices

[Enable Secure Access](#)



This website stores cookies on your computer. These cookies are used to improve the usability of this website and provide more personalized experience for you, both on this website and through other websites. To find out more about the cookies we use, see our [Cookie Notice Policy](#). [Accept](#)



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

+ Protected App

+ Device

loui

OPSWAT.

MetaDefender  
IT Access

Create New Policy

Dashboard

Secure Access

Vulnerabilities

Inventory

★ Policy Management

Policies

Playbooks

User Management

Settings

Logs

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, 1 edit and delete a new user defined policies under the Policies tab*

Sep 05, 2025 4:35:48 AM

Policies **Create New Policy**

Discard Save

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

1  
2

\*Name   
Must contain between 1 and 50 characters

Description   
Description should be less than 1024 characters

- Deep Compliance
- Application Control
- Vulnerability Management
- Patch Management
- Advanced Endpoint Protection**
- Rules

- Enable Threat Detection for Windows**  
Scan using multiple engines to ensure threats are caught. 5
  - Enable Threat Detection for macOS 3
  - Enable Threat Detection for Linux 4
  - Threats detected by multi-scanning technology 6
- Inactive  Inactive  Inactive  Warning Critical Active

Scroll down to "Removable Media Protection" section & Tick "Enable Removable Media Protection"

### 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

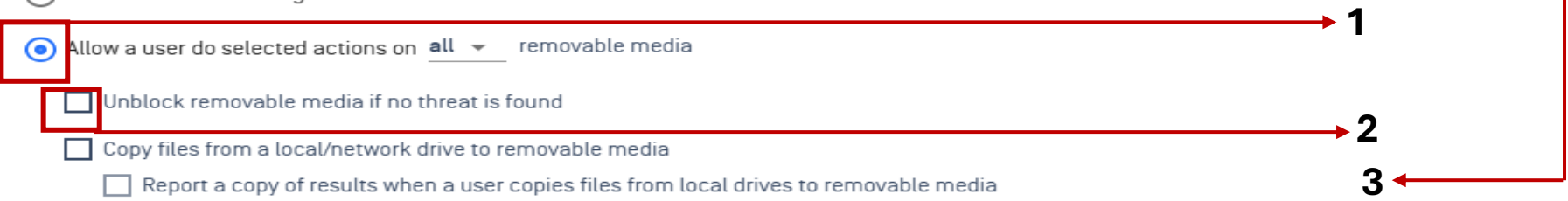
#### Content Disarm and Reconstruction (CDR)

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

Louis.O.A



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

+ Protected App

+ Device

loui

OPSWAT.

MetaDefender  
IT Access

Create New Policy

Dashboard

Secure Access

Vulnerabilities

Inventory

★ Policy Management

Policies

Playbooks

User Management

Settings

Logs

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, 1 edit and delete a new user defined policies under the Policies tab*

Sep 05, 2025 4:35:48 AM

11

1

MetaDefender IT Access \*Name Full Scan

2

Description Perform a full scan on a weekly basis.

3

4

5

Enable Threat Detection for Windows Scan using multiple engines to ensure threats are caught. Inactive

7

8

Settings 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 technology

10

Run scan every Week on Monday at 8 0 AM local device time

9

Scan Options Full Scan (boot sectors, memory, all local drives) Custom Scan

- Boot sectors
- System volume
- Memory
- Removable volumes if any
- Additional local volumes
- Specific path

Scroll down to "Device Scan" section & Tick "Full Scan (boot sectors, memory, all local drives), alternatively, Chose Custom if you want to configure custom"

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*

Sep 05, 2025 4:35:48 AM

10

Policies Create New Policy

Discard Save

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

1

\*Name  Must contain between 1 and 50 characters 20 / 50

2

Description  Description should be less than 1024 characters 28 / 102

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

Allow a user do selected actions on **all** removable media

7

- Exclude CD/DVD
- Exclude mobile devices
- Exclude unformatted media
- Exclude Virtual ISO Drives

Unblock removable media if no threat is found

8

- Allowlist
- Always allow removable media based on the following conditions:
  - Always allow application processes signed by these certificates

- 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

5

- BadUSB protection  
Protect your system from badUSBs covertly executes malicious commands via disguised USB devices.

Copy files from removable media to designated destinations

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:

+ 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
<i>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</i>	1	Sep 05, 2025 4:35:48 AM

# No 3 – 7 is explained on the NEXT slide.

## Policies Create New Policy

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

1

2

- Deep Compliance
- Application Control
- Vulnerability Management
- Patch Management
- Advanced Endpoint Protection
- Rules

### Application Control

Decide whether an application should or should not be installed or run.

- Windows
- macOS
- Linux

Discard Save Conditions

3

- McAfee SiteAdvisor
- Microsoft Teams
- Microsoft Teams (work or school)
- Microsoft Teams classic
- Microsoft Teams Commercial
- Microsoft Teams DoD

4

All versions

Condition: All versions

Version: Enter a value

Cancel Apply

5

No Issue

If Installed: No Issue

If Running: No Issue

No Issue Warning Critical

6

None

None

Disable

Uninstall

7

Desktops, Laptops, VMs, Servers

- Desktops
- Laptops
- VMs
- Servers

## *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....

The screenshot displays the OPSWAT MetaDefender interface. On the left, a navigation menu includes 'Inventory' (highlighted with a red box and arrow 1). The main area shows a 'Devices [1]' table with one device: 'Louis-Machine' (arrow 2). The table columns include Status, Name, Username, Version, # Issues, Groups, # CVEs, Location, Last Reboot, Local IP, MAC Address, and Connected Peripherals. A 'Select Action' dropdown menu is open over the table (arrow 3), with 'Compliance Check' selected (arrow 4). A 'Compliance Check' pop-up window is shown in the foreground (arrow 5), containing three checkboxes: 'Check applications security' (checked), 'Scan threats(Scan with settings in corresponding policy of devices)' (unchecked), and 'Check for OS updates' (unchecked). The 'Check Now' button in the pop-up is highlighted with a red box and arrow 6.

Status	Name	Username	Version	# Issues	Groups	# CVEs	Location	Last Reboot	Local IP	MAC Address	Connected Peripherals
✗	Louis-Machine	louis	7.6.2508.755	2	Default Endpoint	13	Nigeria	7 days	10.252.43.1	dc:1b:a1:c9:26:79	N/A

**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:

OPSWAT.

MetaDefender  
IT Access

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

+ Protected App

+ Device

louis okperuisi 

## Policies

🔍 Search by name, description

Create New Policy

Import Policy

1 - 1 of 1 policy

Policy Name ↑	Policy Description	Groups Assigned	Last Updated	
Default	<i>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</i>	1	Sep 05, 2025 4:35:48 AM	⋮



7

### 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.

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 <sup>0</sup> Critical <sup>3</sup> Active

Windows macOS Linux

Apply to: Desktops, Laptops, VMs, Servers

#### Conditions

#### Treat as

4

Device has CISA known exploitable vulnerability

Device has KEV within 5 days of the due date

Device has KEV past the 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





**OPSWAT MetaDefender  
Platform Onboarding –  
Signing-Up**

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

App

+ Device

lou

by name, description

Create New Policy

me ↑

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, 1 edit and delete a new user defined policies under the Policies tab*

Sep 05, 2025 4:35:48 AM

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

OPSWAT.  
MetaDefender  
IT Access

Sign in  
to continue to MetaDefender IT Access

Email  
Email Address

Sign In

Don't have an account? **Register**

Protecting the  
World's Critical Infrastructure

## Create an account to use MetaDefender IT Access

Create your account with OPSWAT to enable access to the MetaDefender IT Access platform for managing multiple end-point devices and the access to your critical resources and networks.

If you have an OPSWAT account already - [sign in](#) to get started.

First Name: Louis  
Last Name: OKPERIRUISI

Email: louistinteds2001@proton.me

Password: [masked]  
Password: 13 characters including 1 lowercase, 1 uppercase, 1 number, 1 special.

Confirm Password: [masked]

Company Name: ovomeru limited  
Country: Nigeria

I agree to the OPSWAT Inc. [Terms of Service and Privacy Policy](#)

Subscribe to OPSWAT email communications (Optional).

I'm not a robot

**Sign Up**

# Confirmation Link Sent to Email-Box To Continue The Installation

Proton Mail

New message

Inbox 15

Drafts

Sent

Starred

More

Views

Newsletters

Folders

Labels

3.48 MB / 500.00 MB 5.0.78.7

← | ✉ | 🗑 | 📁 | 🔒 | 📧 | 📌 | ⌚

To louistinteds2001@proton.me

✉ | 🗑 | 📧 | 📌 | 🔍 | ⋮

**OPSWAT.**  
MetaDefender  
IT Access

2 ←

Hi louis okperiruis

Thank you for signing up. Your OPSWAT account has been created. Click the button below to activate your free trial period.

1 ← **Activate MetaDefender IT Access**

Need further assistance? Contact support: [opswat.com/support/contact-support](https://opswat.com/support/contact-support)

### Link confirmation

You are about to open another browser tab and visit: <https://id.opswat.com/active?code=874253&email=H4sIAAAAAAAAAAAwXBiQEAMAEsJXQcozjqf1HallU6tdlGoo40qDhILvwyvMeVuEFwVCtiqXy0li5XKYW%2FjKWpYFAAAAA&app=appMA0001&redirect=https%3A%2F%2Fconsole.metaaccess-b.opswat.com&samlrequest=null&SAMLRequest=null&SigAlg=null&Signature=null>

Don't ask again

Cancel **Confirm**

## 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 device will be linked to 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.

This website stores cookies on your computer. These cookies are used to improve the usability of this website and provide more personalized experience for you, both on this website and through other websites. To find out more about the cookies we use, see our [Cookie Notice Policy](#).

**Accept**

X

## 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](#)

## 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

- You **have admin permission to the device**
- Run the MetaDefender Endpoint **perpetually**

↓ Persistent Client

#### On-Demand MetaDefender Endpoint

- You **have admin permission to the device**
- Run the MetaDefender Endpoint **temporarily**

↓ On-Demand Client

#### Limited On-Demand MetaDefender Endpoint

- You **do not have admin permission to the device**
- Run the MetaDefender Endpoint **temporarily**

↓ Limited Client

3

2

1

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

**OPSWAT.**  
MetaDefender Endpoint

## **Installer MetaDefender Endpoint**

By installing you agree to our [EULA](#) and [Privacy Policy](#)

**INSTALL NOW**

7.6.2508.755

---

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

---



Policies **Create New Policy**

Discard Save

- 1
- 2
- 3
- 4
- 5
- 6
- 7

\*Name Patch Management Policy

Must contain between 1 and 50 characters 25 / 50

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

- Deep Compliance
- Application Control
- Vulnerability Management
- Patch Management**
- Advanced Endpoint Protection
- Rules

Patch Management  
Verify that a patch management agent is installed or running.

Warning 5 Critical 3 Active

- Windows
- macOS
- Linux

Apply to: Desktops, Laptops, VMs, Servers

Conditions	Treat as
No patch management application is installed	No Issue Warning <b>Critical</b> Advanced
Patch management agent is disabled	No Issue Warning <b>Critical</b>
Patch management agent has reported	No Issue Warning <b>Critical</b>

Any missing patches in all categories with specific severity level : critical, important, moderate over 1 day(s)



5

Policies Create New Policy

Discard

Save

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

1

Application Updates

Automatically update applications that can be updated.

Active

2

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.

- 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

4

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.

- 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.*

- Overview
- Security Score
- Deep Compliance
- Application Patches
- Vulnerabilities
- Application Remover
- OPSWAT Academy

Overview

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

Louis.O

- Overview
- Security Score
- Deep Compliance
- Application Patches**
- Vulnerabilities
- Application Remover
- OPSWAT Academy

### Application Patches

Auto-Update  Refresh Alert More

Enable seamless patching of your 3rd party applications, keeping your systems secure and up to date. [Learn More](#)

Application	Current Version	Available Version	Update	Remove	Info
Adobe Acrobat Reader DC Continuous	25.001.20643	25.001.20672	<input type="checkbox"/>	<input type="checkbox"/>	
Advanced IP Scanner	2.5.3850	2.5.4594.1	<input type="checkbox"/>	<input type="checkbox"/>	
Google Chrome	140.0.7339.80	140.0.7339.81	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Microsoft Visual C++ 2015-2022 Redistributable (x64)	14.44.35208.0	14.44.35211.0	<input type="checkbox"/>	<input type="checkbox"/>	
Microsoft Visual C++ 2015-2022 Redistributable (x86)	14.42.34433.0	14.44.35211.0	<input type="checkbox"/>	<input type="checkbox"/>	
VMware Player	17.6.0	17.6.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VMware Workstation	17.6.0.61175	17.6.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Update Application

Would you like to update all of the applications in the auto-update list

- Adobe Acrobat Reader DC Continuous
- Advanced IP Scanner
- Google Chrome
- Microsoft Visual C++ 2015-2022 Redistributable (x64)
- Microsoft Visual C++ 2015-2022 Redistributable (x86)

1

2

[Update All](#)

Overview

Overview



Security Score

Deep Compliance

Application Patches

Vulnerabilities

Application Remover

OPSWAT Academy

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 →

Louis.0

- ✓ Deep Compliance
- ↓ Application Patches
- 🎯 Vulnerabilities
- 🗑️ Application Remover
- 🏠 OPSWAT Academy

Browser Security  
15 out of 15

Unwanted Applications  
5 out of 5

Vulnerabilities  
0 out of 10

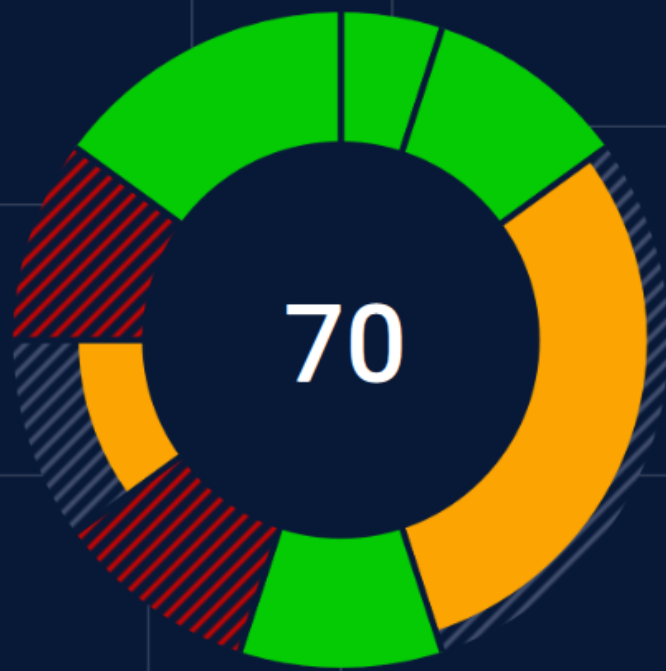
Firewall  
10 out of 10

Windows Update  
5 out of 10

Malware Protection  
25 out of 30

Device Encryption  
0 out of 10

Backup  
10 out of 10



- 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 →

Louis.0

- 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. [View details](#)

**⚠ 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).

Louis.O

- 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 →

Louis.0

- 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



  
**VirtualBox**  
Pending Update  
10

  
**VMware Workstation**  
Pending Update  
1

- 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 →

Louis.O













- 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

Louis.O

Thank you!