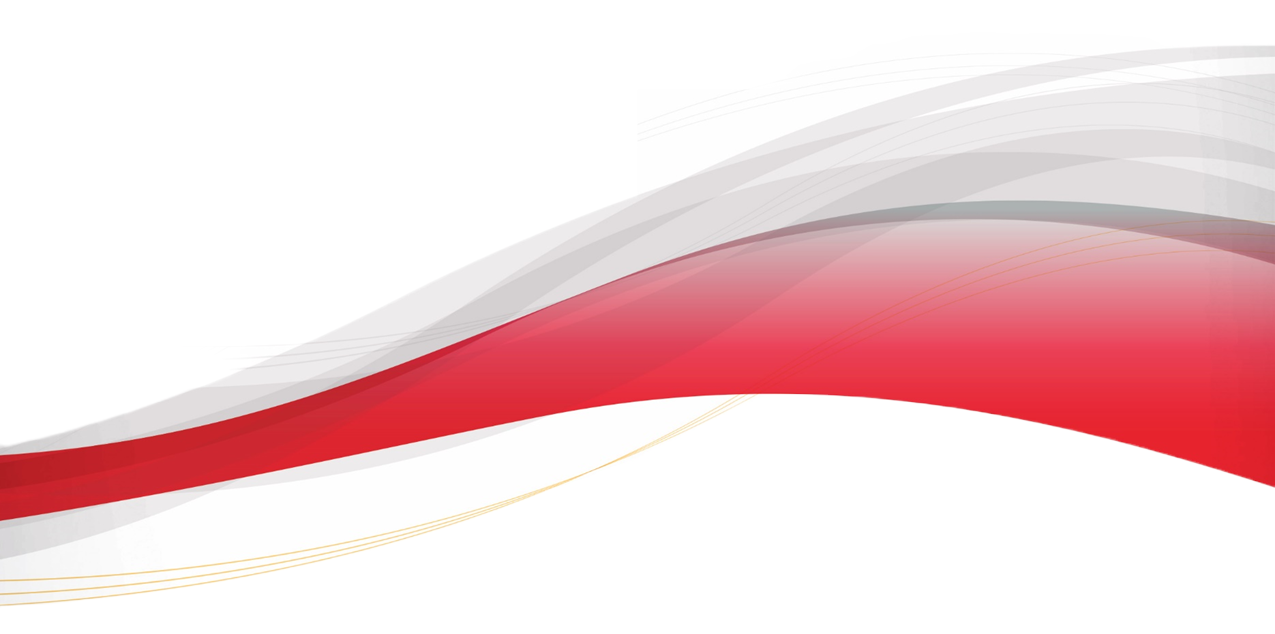
Trend Micro Health Check  
Endpoint Security for



Review of GOOGLE Apex One On-Premises Implementation



Document Version:   
  
Version Release Date: Invalid date  
  
Prepared By:   
  
Approved By:   
  
Trend Micro India Pvt Ltd

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Version** |  | **Version Date** | Invalid date |
| **Title** |  | | |

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Ver. Date** | **Revised by** | **Description** |
| 1.0 |  |  | Initial Draft |
| 1.1 |  |  | Final Report |

Content

# 1 Introduction

All best practice statements in this document are formed from base principles with the products, and many years of experience within Trend Micro, however all recommendations herein should be validated as being acceptable to meet business, regulation, and security requirements of GOOGLE to have a successful outcome.

This document provides best practice recommendations in comparison to the published Best Practice product guides from Trend Micro to the configuration at GOOGLE. Trend Micro recommends that GOOGLE evaluate each recommended setting to verify it is suitable within their environment.

This document follows an established "Red, Amber, Green" methodology for highlighting gaps in best practice.

|  |  |  |
| --- | --- | --- |
| **Status** | **Description** | **Key** |
| Good | Meets Trend Micro Minimum Requirements / Best Practice recommendations |  |
| Concern | May have a security and/or operational impact on the organization |  |
| Critical | Likely to have a high security and/or operational impact on the organization |  |
| Info | Tips and Recommendations |  |

**Note:** Status items are in context to the configuration of the Trend Micro product only and do not consider any other external mitigating feature that GOOGLE may have in place and context as if GOOGLE did not have any mitigation of any description.

Configuration is subject to the requirements of each organization. Trend Micro acknowledges that deviations from published Best Practices are within the scope of GOOGLE by their specific environment and are subject to internal security requirements. Also, Trend Micro's Best Practice recommendation is subject to change at any time.

## 1.1 Health Check Attendees

|  |  |
| --- | --- |
| Location | Remotely |
| Customer Attendance |  |
| Trend Micro Attendance |  |

# 2 Executive Summary

Trend Micro performed a Health Check on Invalid date for EVENTUS to ensure Trend Micro Product(s) are configured as per best practice and provide gap analysis feedback.

This high-level summary provides an overview of the status of your Apex One and Apex Central deployment. Detailed instructions and references can be found within the individual sections further down in the report.

(input) Agents have outdated Program versions out of (input) agents.

(input) endpoints are required to restart for the update.

(input) endpoints (input-name-of-endpoints) are required to restart for cleanup.

(input) agents (input) are using the Windows servers platform.

(input) agents are installed on Windows 7 (Legacy OS) platform.

(input) endpoints are without policy.

Memory Allocated to the Apex One server is not as per the Trend Micro Requirement.

Apex One is running on an older version i.e., 112(Deployed). (Latest available version is 1132).

Your Trend Micro Apex One license has expired.

Apex One seat count is 12 and is managing 23 endpoints.

Certified Safe Software Service is Disabled.

Apex Central is not registered with Apex One.

33 agents have outdated patterns older than 7 days out of 123 agents.

Notification is not Enabled.

PUBLIC Policy is not configured as per the Trend Micro best practice.

In Apex Central Active Directory is not configured.

In Apex Central Scheduled Report is not configured.

Syslog is configured in Apex Central.

Apex central is running on an older version i.e., 24. (Latest Version available is 123).

Your Trend Micro Apex central license is valid till Oct 3,2023.

In Apex Central Log Retention is not configured.

In Apex Central Event Notifications are not Enabled.

We have captured 30 Days of logs on 4th Mar 2024 detections are below:

1237 Virus/Malware Detected

22 Spyware/Grayware Detected

2024 Web Reputation Detected

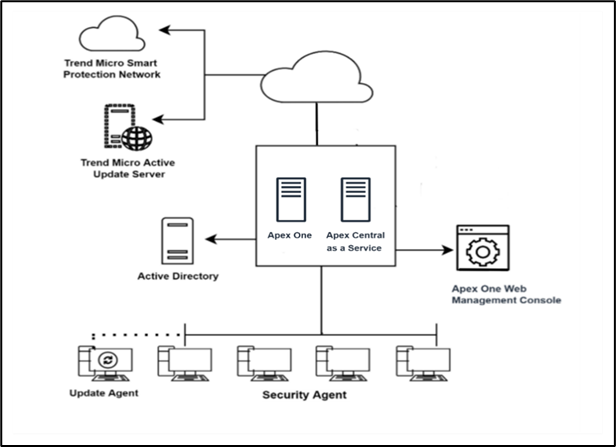
368 Device Control Detected

101715 Intrusion Prevention Detected

126 C&C Callback Detected

114 Behaviour Monitoring Detected

# 3 Product Architecture



# 4 Apex One & Apex Central

Trend Micro Apex One protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. Apex One Server consists of Apex One agent program that resides at the endpoint OS and a server OS. The Apex One Security agent guards the endpoint and reports its security status to the server. Through the web-based management console, the Apex One server makes it easy to set coordinated security policies and deploy updates to every agent.

Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

## 4.1 Apex One Configuration Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Apex one Administration Configuration Health-Overview** | |  |  |
| System Health-Overview | Minimum Requirements |  |  |
| Memory | 8 GB (This would depend on the number of agents customer deployed. Please refer sizing guide) | 2 |  |
| Operating System | Supported OS | Windows Server 2019 |  |
| CPU | 3 cores | 5 cores |  |
| Hostname / IP |  | 00.00.00.00 |  |
| Apex One Build Version | 1132 | 112 |  |
| Agent Management tree | AD / Custom / NetBIOS grouping | AD |  |
| License | Within Term | 31/08/2023 |  |
| Deployed Agents | Total Purchased Licensed Seat is 12 | 23 |  |
| Certified Safe Software Service | Enable Certified Safe Software Service | Disabled |  |
| Patterns Update Status | Up to Date | Up to Date- 123 Outdated- 33 |  |
| Apex Central Integration | Register Apex One to Apex Central | No |  |
| Global Agents Settings | Enable Clean / Delete Infected Files within Compressed Files | Yes |  |
| Enable resume schedule scan options under global agent settings | Resume an Interrupted Scheduled Scan- Enabled and Resume a missed Scheduled Scan at the same time the next day- Enabled |  |
| Enable Smart Protection Service Proxy | Enabled |  |
| Agent scheduled updates | Enabled |  |  |
| Smart Protection Server | Integrated/Standalone SPS Server/Global SPS | Standalone SPS Server |  |
| Notification | Enabled | Disabled |  |

## 4.2 Policy Overview: PUBLIC Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Policy Configuration - Overview PUBLIC Policy** | | | |
| Agent Scan Mode | Smart scan | Conventional Scan |  |
| Manual Scan - Policy | Files to Scan > All Scannable files | All Scannable files |  |
| Scan Hidden Folders | Disabled |  |
| Select - Scan compressed files. > Maximum layers: 2 | Select- Scan compressed files. > Maximum layers: 3 |  |
| Select - Scan OLE objects. > Maximum layers: 3 | Select- Scan OLE objects. > Maximum layers: 3 |  |
| Enable - Detect exploit code in the OLE file | Disabled Detect exploit code in the OLE files. |  |
| Virus/Malware Scan Settings Only > Scan boot area | Enabled - Scan boot area |  |
| CPU Usage > Medium | Medium |  |
| Manual Scan - Actions | Virus/Malware > Use a specific action for each virus/malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine | | Other Malware: Clean & Quarantine | | Virus/Malware > Use Active Action |  |
| Select - Back up files before cleaning. | Disabled - Back up files before cleaning. |  |
| Enable - Damage Cleanup Services with Advanced Clean up | Disabled - Damage Clean up Services with Advanced clean-up |  |
| Enable - Run cleanup when Probable virus/malware is detected | Enabled - Run cleanup when probable virus/malware is detected |  |
| Enable - Spyware/Grayware > Clean: Apex One terminates Processes. | Enabled - Spyware/Grayware > Clean: Apex One terminates processes. |  |
| Real-Time Scan Policy Settings | Enable - Virus/Malware Scan | Enabled |  |
| Enable - Spyware/Grayware scan | Enabled - Spyware/Grayware scan |  |
| User Activity on Files > Scan files being created/modified and retrieved | User Activity on Files > Scan files being created/modified |  |
| Files to Scan > All Scannable files | File types Scanned by IntelliScan |  |
| Enable - Scan the boot sector of the USB storage device after plugging it in. | Enabled - Scan the boot sector of the USB storage device after plugging it in. |  |
| Enable - Scan all files in a removable storage device after plugging in. | Enabled - Scan all files in a removable storage device after plugging in. |  |
| Enable - Quarantine malware variants detected in memory. | Enabled - Quarantine malware variants detected in memory. |  |
| Select - Scan compressed files. > Maximum layers: 2 | Selected - Scan compressed files. > Maximum layers: 2 |  |
| Select - Scan OLE objects. > Maximum layers: 3 | Selected - Scan OLE objects. > Maximum layers: 3 |  |
| Enable - Detect exploit code in the OLE files. | Enabled - Detect exploit code in the OLE files. |  |
| Enable - CVE exploit scanning | Enabled - CVE exploits scanning |  |
| Real-Time Scan-Action Settings | Virus/Malware > Use a specific action for each virus/malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine | | Other Malware: Clean & Quarantine | | Used the same action for all Virus/Malware types.  (If the first action is unsuccessful, Apex One performs the second action.)   |  |  |  | | --- | --- | --- | | Type | 1st Action | 2nd Action | | All types | Quarantine | Quarantine | |  |
| Enable - Back up files before cleaning. | Enabled - Back up files before cleaning. |  |
| Enable - Run cleanup when probable virus/malware is detected | Enabled - Run cleanup when probable virus/malware is detected. |  |
| Enable - Spyware/Grayware > Clean: Apex One terminates processes. | Enabled - Spyware/Grayware > Clean: Apex One terminates processes. |  |
| Schedule Scan Policy Settings | Enable - Virus/Malware Scan | Enabled - Virus/Malware Scan |  |
| Enable - Spyware/Grayware scan | Enabled - Spyware/Grayware scan |  |
| Configure Schedule Scan to run at least once a week. | Weekly Every Monday - Start time: 11:14 |  |
| Files to Scan > All Scannable files | All Scannable files |  |
| Select - Scan compressed files. > Maximum layers: 2 | Selected - Scan compressed files. > Maximum layers: 2 |  |
| Selected - Scan compressed files. > Maximum layers:3 | Selected - Scan OLE objects. > Maximum layers: 3 |  |
| Enable - Detect exploit code in the OLE files. | Disabled - Detect exploit code in the OLE files. |  |
| Virus/Malware Scan Settings Only > Scan boot area | Enabled Scan boot area |  |
| CPU Usage > Medium | Medium |  |
| Schedule Scan-Action Settings | Virus/Malware > Use a specific action for each virus/malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine | | Other Malware: Clean & Quarantine | | Used specific action for each Virus/Malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine & Quarantine | | Select - Other Malware: Clean & Quarantine | |  |
| Select - Back up files before cleaning. | Enabled - Back up files before cleaning. |  |
| Enable - Damage Cleanup Services with Advanced Clean up | Enabled - Damage Clean up Services with Advanced clean-up. |  |
| Enable - Run cleanup when probable virus/malware is detected | Enabled - Run cleanup when probable virus/malware is detected. |  |
| Enable - Spyware/Grayware > Clean: Apex One terminates processes. | Enabled - Spyware/Grayware > Clean: Apex One terminates processes. |  |
| Behavior Monitoring | Enable Malware Behavior Blocking Known and potential threats | Disabled |  |
| Ransomware Protection Protect documents against unauthorized encryption or modification | Disabled |  |
| Protect documents against unauthorized encryption or modification -> Automatically backup and restore files changed by suspicious programs | Enabled |  |
| Enable program inspection to detect and block compromised executable files | Enabled |  |
| Anti-exploit Protection Terminate programs that. exhibit abnormal Behavior. associated with exploit attacks | Enabled |  |
| Newly Encountered Programs Monitor newly encountered programs downloaded through web or email application channels -> Prompt User | Enabled |  |
| Exceptions (specify exception if any) | No exceptions added in the Approved Program list |  |
| Predictive Machine Learning | Enable | Disabled |  |
| Action  File: quarantine  Process: Terminate | Action Set  File: Quarantine  Process: Terminate |  |
| Exception (specify exception if any) | Exceptions added |  |
| Suspicious Connection | Enable with Block option | Disabled with Block option |  |
| Web Reputation | Enable for Internal and External agents with Security Level Medium | Enabled with Security Level Medium |  |
| Vulnerability Protection | Enable | Enabled with Inline Mode |  |
| Device Control | Enable | Disabled |  |
| Application Control | Enable | Disabled |  |
| Firewall | Enable (Optional) | Disabled |  |
| Agent Self-Protection | Enable Self-Protection with a password. | Disabled |  |
| Additional Service | Configure respective services | Enabled Unauthorized Change Prevention Service for Windows desktops and Enabled Windows Server platforms with full mode.  Enabled Firewall Service for Windows desktops and Enabled for Windows Server platforms.  Enabled Suspicious Connection Service for Windows desktops and Enabled Windows Server platforms.  Enabled Data Protection Service for Windows desktops and Enabled Windows Server platforms.  Enabled Advanced Protection Service for Windows desktops and Enabled Windows Server platforms. |  |

## 4.3 Apex Central Configuration Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Configuration Health - Overview** | |  |  |
| License | Within Term | 03/10/2023 |  |
| Version | Build 123 | Build 24 |  |
| Active Directory Sync | Configure | Not Configured |  |
| Log Retention | Configure | not configured |  |
| Reports | Configure | Not Scheduled |  |
| Event Notifications | Enable | Disabled |  |
| Syslog | Configure | Configured |  |
| Report Maintenance | Configure | Configured |  |
| Product Registration | Register all Trend Micro products with Apex Central | Apex One Server is Registered |  |

## 4.4 Identified Gaps and Recommendations

(input) Agents have outdated Program versions out of (input) agents keep all agent program versions updated.
Minimum OS Version requirement for the latest Apex One SaaS agent version: <https://success.trendmicro.com/dcx/s/solution/000291904?language=en_US>

(input) endpoints are required to restart for the update. Apex One Agents may need to reboot for engine updates. Recommended to restarting those endpoints.

(input) endpoints (input) are required restart for cleanup.

(input) agents are installed on Windows 7 (Legacy OS) platform, recommended to upgrade it to the latest OS.
For the Windows 7 & 8.1 machines End-of-Support <https://success.trendmicro.com/dcx/s/solution/000291687?language=en_US&sfdcIFrameOrigin=null>

(input) agents (input) are using the Windows servers platform. recommended to use Cloud One Workload Security for better protection of the server.

(input) Endpoints are without policy, recommended to apply policy to all endpoint on priority for better protection.

Memory Allocated to the Apex One server is not as per the Trend Micro Requirement, recommended to refer to the sizing document for details. https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne\_2019\_req.pdf.

Apex One is running on an older build version recommended to upgrade it to the Latest version 1132.

Please contact your Trend Micro Account Manager to renew the license to protect your endpoints.

Apex One seat count is 12 and is managing 23 endpoints recommended to increase the seat count.

Certified Safe Software Service is disabled, recommend to enable it.

It is recommended to register the Apex one with Apex Central to manage the policies.

33 Agents have smart scan pattern version older than 7 days out of 123, recommended to keep all patterns up to date.

Notification is disabled, recommended to enable it.

Apex central is running on an older build version recommended to upgrade it to the Latest version 123. Download link: https://www.trendmicro.com/en\_us/business/products/downloads.html.

Your Trend Micro Apex central license will expire soon. Please get in touch with the Trend Micro account manager to start the renewal process.

Configure Active Directory Sync to allow administrators to create user accounts for web console access based on Active Directory users or groups.
For more information [Active Directory Integration](https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/getting-started/active-directory-and_001/active-directory-int/configuring-active-d.aspx.)

In Apex Central Log Retention is not configure recommended to configure it.

In Apex Central Schedule Reports are not configured, recommended to configure it for better visibility in the console for all types of events.

In Apex Central Event Notifications are disabled, recommended to enable it.

**In PUBLIC Policy:**

All the agents are using the Conventional Scan method recommended to use Smart scan Method. Smart Scan leverages threat signatures that are stored in the cloud.

In Manual Scan and policy settings, Scan Hidden Folders is disabled, recommended to enable it.

In Manual and Schedule Scan and policy settings, Detect exploit code in OLE is disabled, recommended to enable it.

In Manual Scan Action Settings, active Action is selected, recommended to select Use a specific action for each virus/malware type.

In Manual Scan Action Settings, back up files before cleaning is disabled, recommended to enable it.

In Manual Scan Action Settings, damage Clean up Services with Standard clean up, recommended to enable it with Advanced clean up as The Security Agent uses advanced cleanup rules to proactively detect and stop applications that exhibit Fake AV and rootkit behavior.

In Real-Time Scan Policy Settings, user Activity on Files > Scan files being created/modified and retrieved not selected recommend to configure this to all files.

In Real-Time Scan & policy settings, Files to scan are set as File types scanned By IntelliScan, recommended to set it as All Scannable files as Only scan files known to potentially harbor malicious code, including files disguised by a harmless extension name are Scan in IntelliScan.

In Real-Time Scan Action Settings, same action for all malware-Virus types is selected, recommended to select Use a specific action for each virus/malware type.

Behavior Monitoring protection modules are disabled and recommended to enable it for better protection from ransomware.

Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis or behavioral process and script analysis to detect emerging unknown security risks.

Suspicious Connection is enabled with Log only action, recommended to enable with block action to protect agents against C&C server callbacks.

Device Control is disabled, recommended to enable it as it regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss and leakage, combined with file scanning, helps guard against security risks.

Application Control is disabled, recommended to enable as it provides the ability to control which users have access to specific applications on certain endpoints.

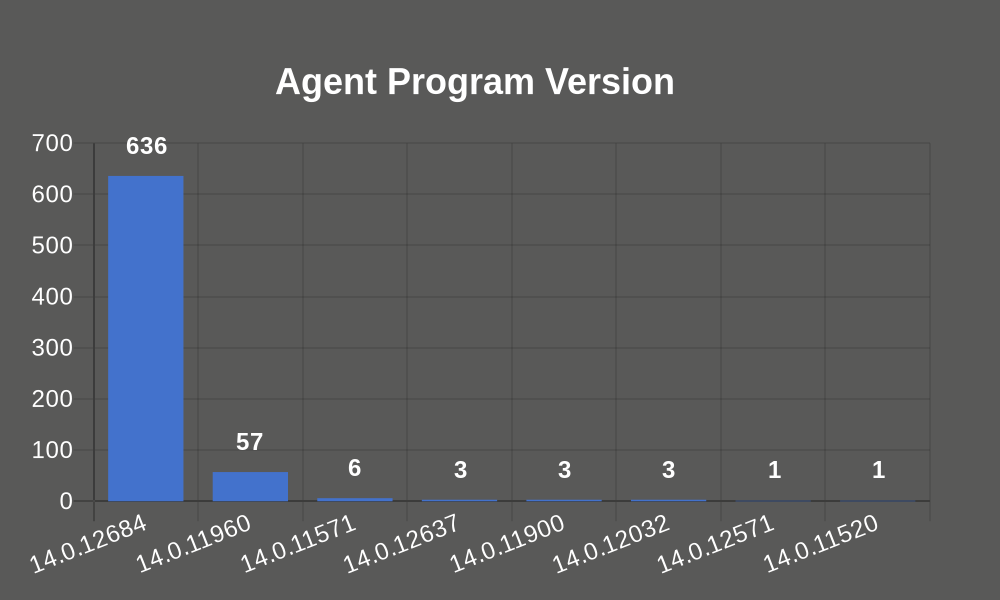
The firewall is disabled, recommended to enable it (Optional). Firewall policies allow you to block or allow certain types of network traffic not specified in a policy exception. A policy also defines which Apex One Firewall features are enabled or disabled. Assign the policy to one or multiple Firewall profiles.

Agent Self-Protection is Disabled, recommended to enable it to prevent unauthorized agent Uninstallation and Unloading.

# 5 Apex One Product Efficacy

## 6.1 Agent Distribution

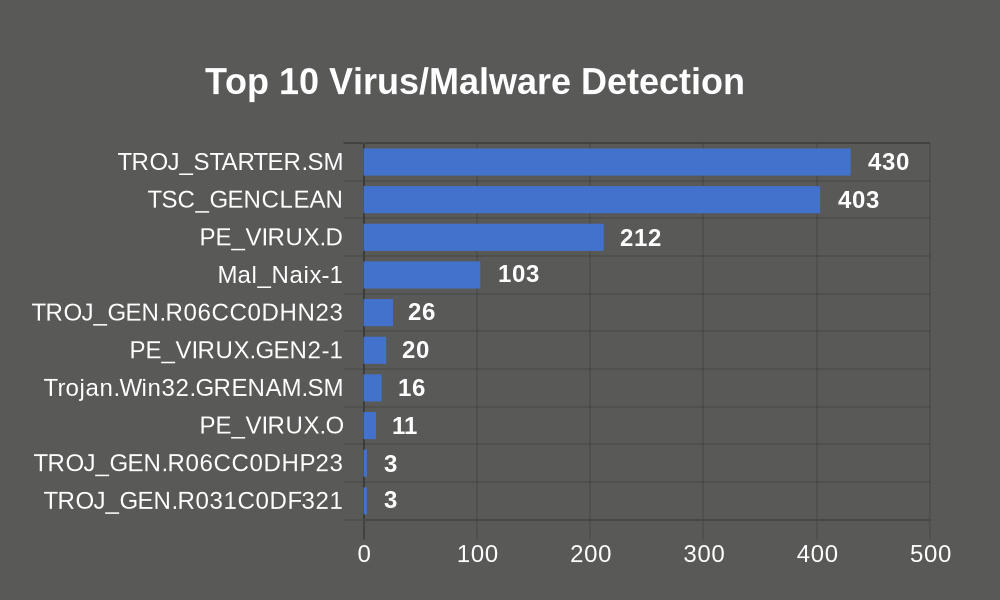
|  |  |
| --- | --- |
| **Agent Platform** | **Count** |
| Windows 10 10.0.19045 | 384 |
| Windows Server 2016 10.0.14393 | 182 |
| Windows 11 10.0.22621 | 47 |
| Windows 10 10.0.18363 | 26 |
| Windows 10 10.0.19044 | 18 |
| Windows 10 10.0.19041 | 10 |
| Windows Server 2008 6.1.7601 | 7 |
| Windows 10 10.0.16299 | 7 |
| Windows 7 6.1.7601 | 6 |
| Windows 10 10.0.19043 | 6 |
| Windows 11 10.0.22000 | 5 |
| Windows Server 2012 R2 6.3.9600 | 5 |
| Windows 10 10.0.19042 | 3 |
| Windows 10 10.0.18362 | 1 |
| Windows 10 10.0.17134 | 1 |
| Windows Server 2022 10.0.20348 | 1 |
| Windows 10 10.0.15063 | 1 |



14.0.12684 is the latest agent Program version recommended to upgrade all the older agents to the latest version.

## 6.2 Virus/Malware

We generated a Virus/Malware Event of the last 30 Days on 4th Mar 2024 from Apex central/Apex One. There was a total of 1237 detections.

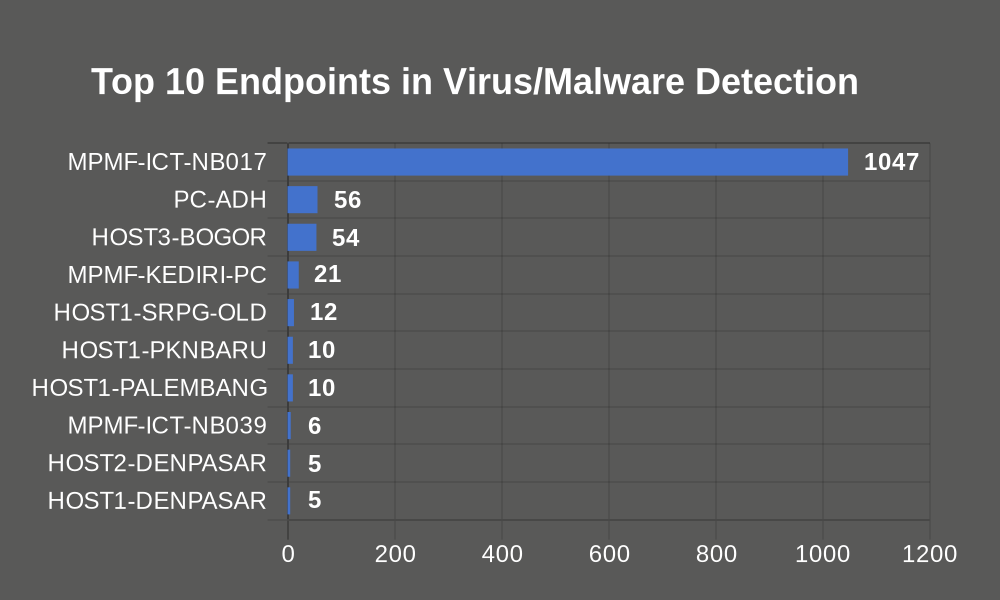


TROJ\_STARTER.SM Virus/Malware was detected 430 times on the MPMF-ICT-NB017 endpoint, and the files were successfully cleaned by Apex One.

* + dfd
  + dfd

TSC\_GENCLEAN Virus/Malware was detected 403 times on MPMF-ICT-NB017, PC-ADH and MPMF-KEDIRI-PC endpoints, and the files were successfully cleaned by Apex One.

* + dfd
  + dfd

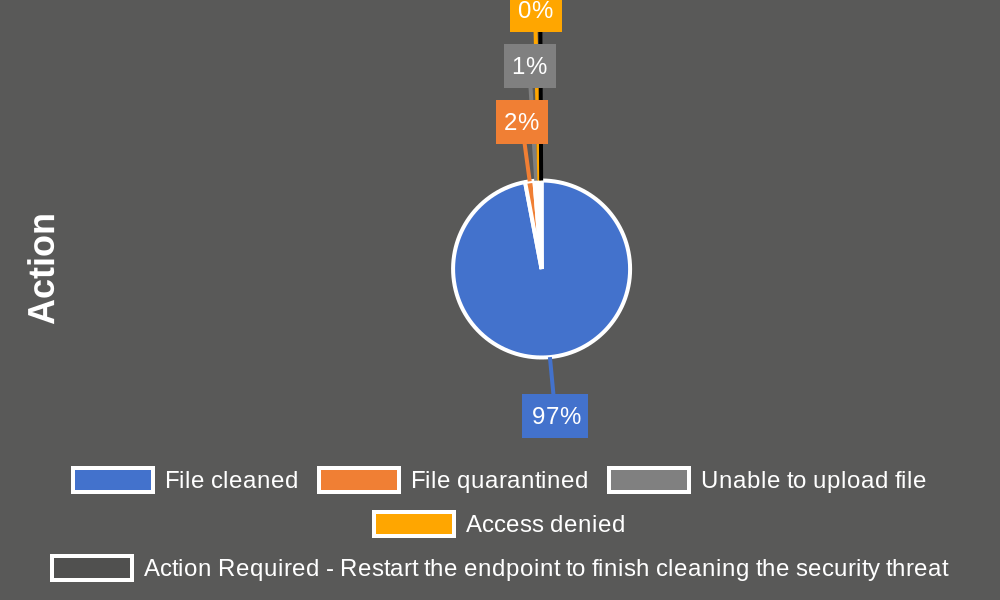


1047 times Virus/Malware was detected on the MPMF-ICT-NB017 endpoint, and the files were successfully cleaned by Apex One.

* + dfd
  + fdsf

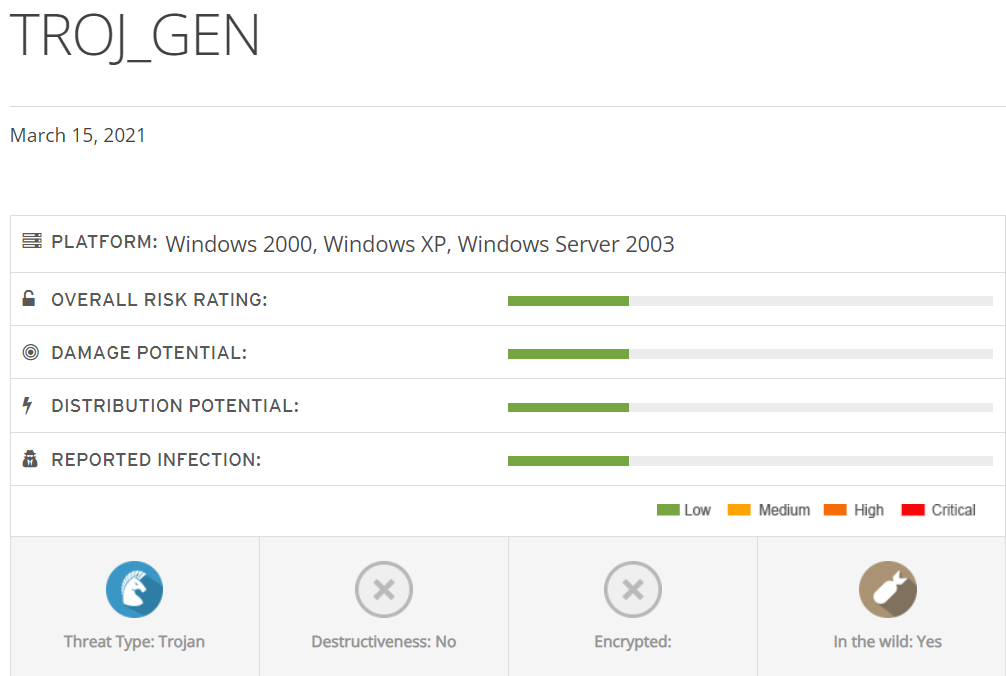
56 times Virus/Malware was detected on the PC-ADH endpoint, and the files were successfully cleaned, quarantined, unable to upload files and access denied by Apex One.

* + sdf
  + dfd



Files were cleaned, quarantined, unable to upload files, access denied, and unable to clean files by Apex One.

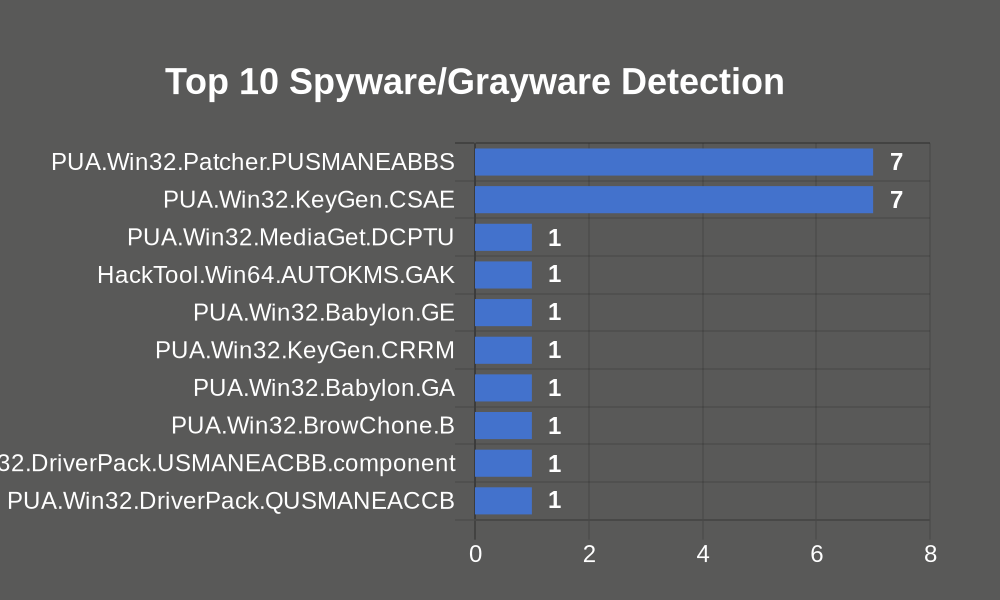
https://global.sitesafety.trendmicro.com/result.php



Add Description and action to take if any
Add the url of that detection
Add Description and action to take if any
Add the url of that detection
Add Description and action to take if any
Add the url of that detection

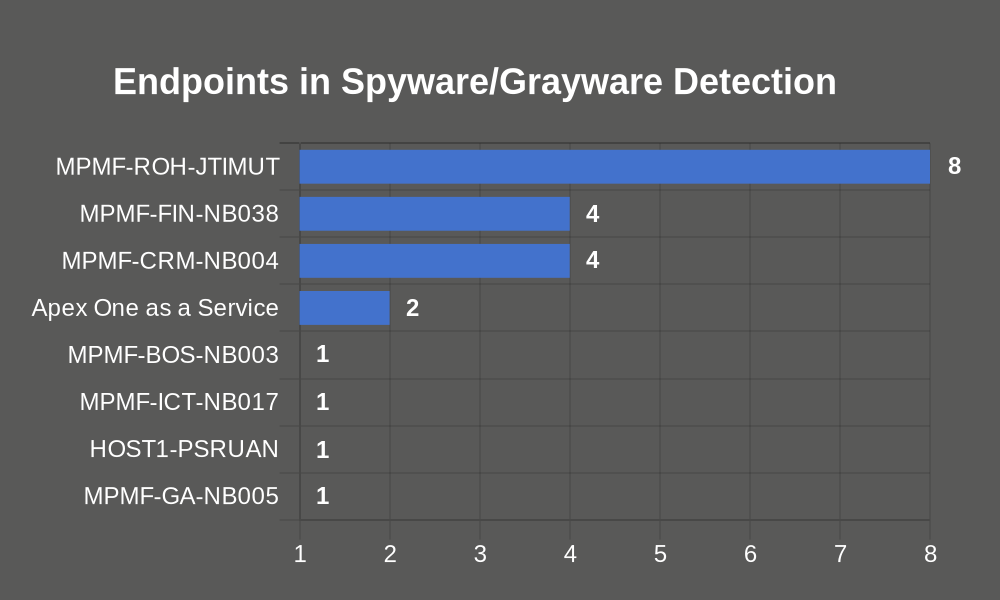
## 6.3 Spyware/ Grayware

We generated a Spyware/Grayware Event of the last 30 Days on 18th Sep 2023 from Apex central/Apex One. There was a total of 22 detections.



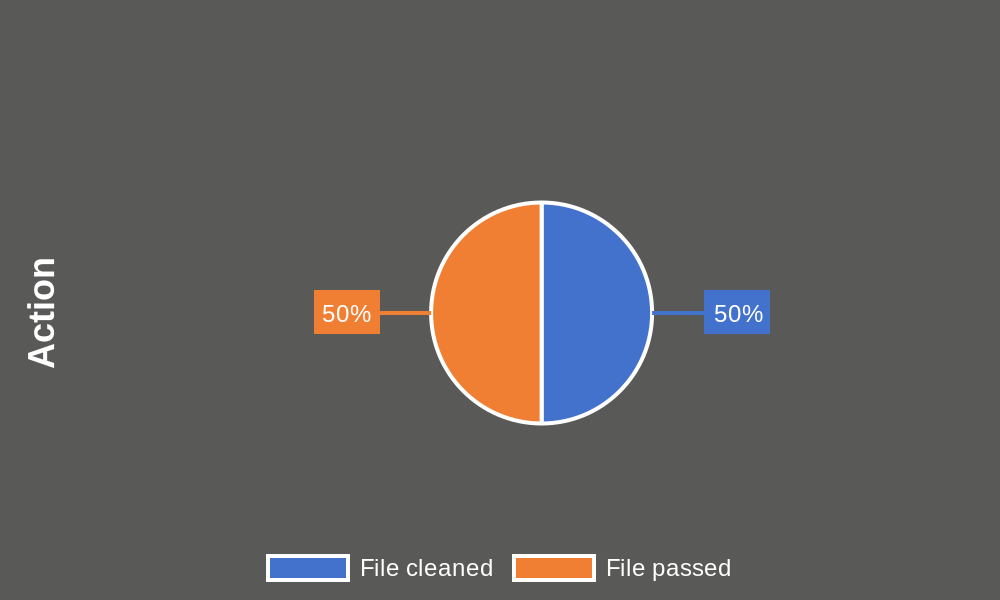
PUA.Win32.Patcher.PUSMANEABBS Spyware/Grayware was detected 7 times on MPMF-ROH-JTIMUT, Apex One as a Service and MPMF-CRM-NB004 endpoints, and the files were successfully passed and cleaned by Apex One.

PUA.Win32.KeyGen.CSAE Spyware/Grayware was detected 7 times on MPMF-ROH-JTIMUT, Apex One as a Service and MPMF-CRM-NB004 endpoints, and the files were successfully passed and cleaned by Apex One.



8 times Spyware/Grayware was detected on the MPMF-ROH-JTIMUT endpoint, and the files were successfully passed and cleaned by Apex One.

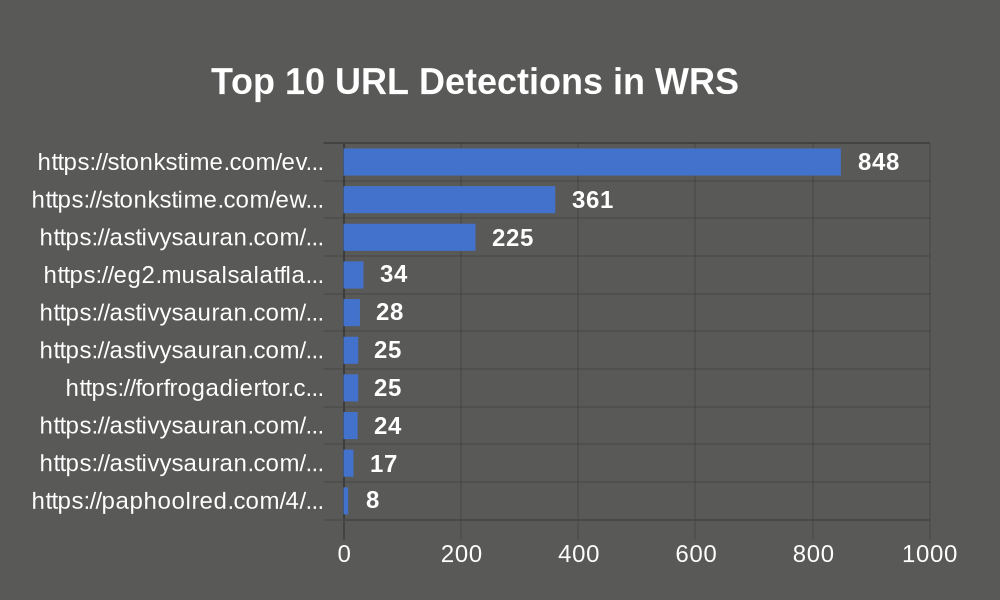
4 times Spyware/Grayware was detected on the MPMF-FIN-NB038 endpoint, and the files were successfully cleaned by Apex One.



Files were cleaned, and passed by Apex One.

## 6.4 Web Reputation

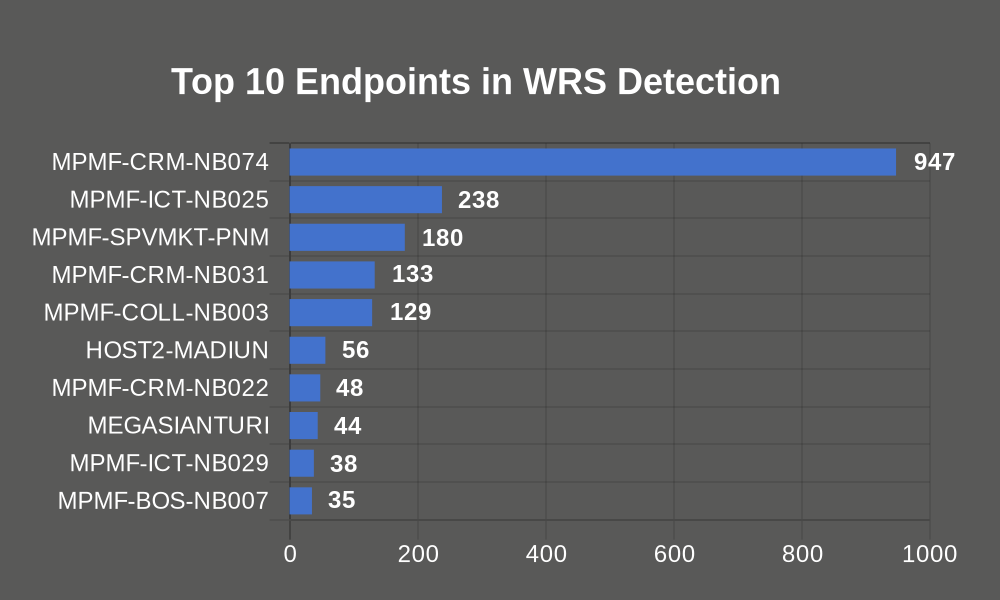
We generated a Web Reputation Detections Event of the last 30 Days on 18th Sep 2023 from Apex central/Apex One. There was a total of 2024 detections.



33 times HTTP sites are detected in WRS detection, and the files were successfully Blocked by apex one. Check whether it's secure or not if it's secure then add it to the approved list otherwise block it.

https://stonkstime.com/event This site is detected 848 times on MPMF-CRM-NB074, MEGASIANTURI, MPMF-CRM-NB022 and MPMF-SPVMKT-PNM endpoints, and the files were successfully Blocked by apex one.

https://stonkstime.com/ewant This site is detected 361 times on MPMF-CRM-NB074, MEGASIANTURI, MPMF-CRM-NB022 and MPMF-SPVMKT-PNM endpoints, and the files were successfully Blocked by apex one.



All the web violation events were successfully blocked by apex one.

