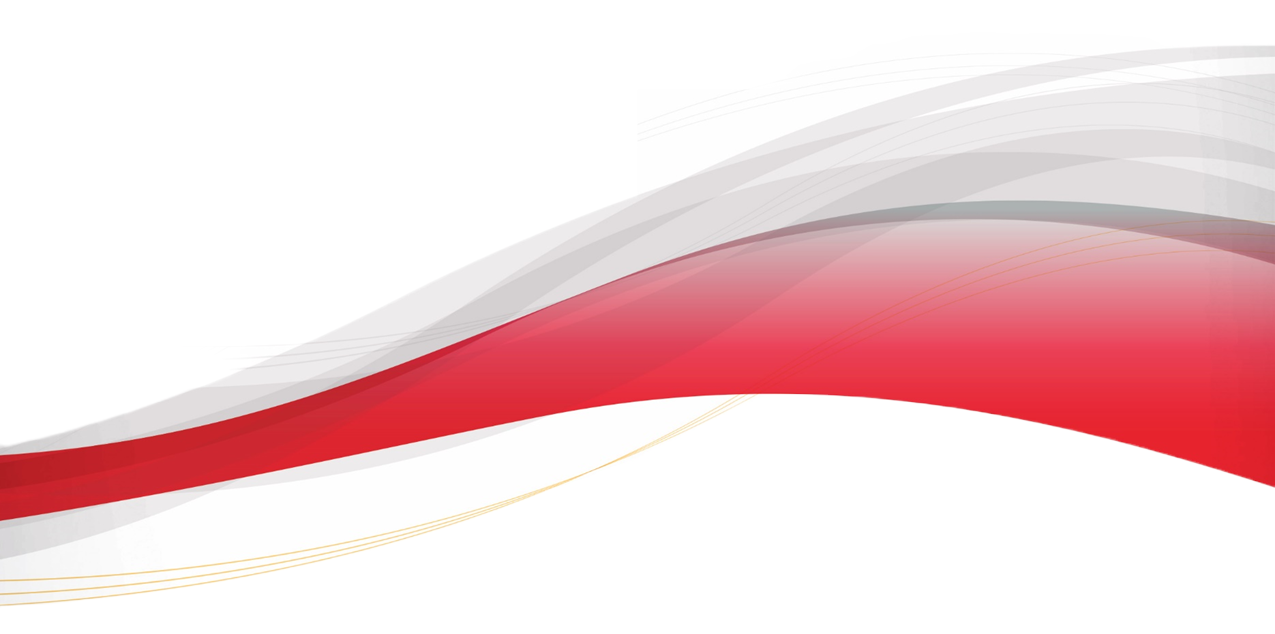
Trend Micro Health Check  
Endpoint Security for



Review of Eventus Security Apex One On-Premises Implementation



Document Version: V1.0  
  
Version Release Date: 03/10/2023  
  
Prepared By: Pramit P  
  
Approved By:   
  
Trend Micro India Pvt Ltd

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Version** | 1.0 | **Version Date** | 03/10/2023 |
| **Title** | Review of Eventus Security Apex One SaaS/On-Premises Implementation | | |

**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 Eventus Security 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 Eventus Security. Trend Micro recommends that Eventus Security 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 Eventus Security may have in place and context as if Eventus Security 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 Eventus Security 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 2023-09-27 for Eventus Security 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 the Windows 7 (Legacy OS) platform.

(input) endpoints are without policy.

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

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.

In Apex Central syslog is not configured.

Your Trend Micro Apex central license has expired.

In Apex Central Log Retention is not configured.

In Apex Central Event Notifications are not Enabled.

In Apex Central Report Maintenance is not configured.

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

14 Virus/Malware Detected

3 Spyware/Grayware Detected

799 Web Reputation Detected

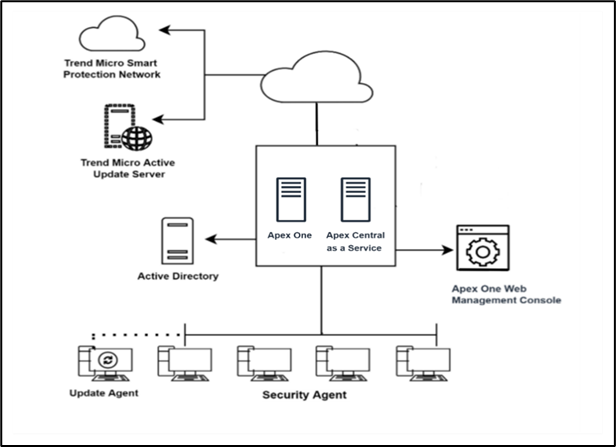
12017 Intrusion Prevention Detected

276 Device Control Detected

429568 C&C Callback Detected

1109 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) | 8 |  |
| Operating System | Supported OS | Windows Server 2019 |  |
| CPU | 0 cores | 0 cores |  |
| Hostname / IP |  | 00.00.00.00 |  |
| Apex One Build Version | 1234 | 1234 |  |
| Agent Management tree | AD / Custom / NetBIOS grouping | AD |  |
| License | Within Term | Invalid date |  |
| Deployed Agents | Total Purchased Licensed Seat is 0 | 0 |  |
| Certified Safe Software Service | Enable Certified Safe Software Service | Enabled |  |
| Patterns Update Status | Up to Date | Up to Date- 0 Outdated- 0 |  |
| Apex Central Integration | Register Apex One to Apex Central | Yes |  |
| 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 | Enabled- Daily |  |
| Smart Protection Server | Integrated/Standalone SPS Server/Global SPS | Integrated SPS |  |
| Notification | Enabled | Enabled |  |

## 4.2.1 Policy Overview: 01 TEST Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Policy Configuration - Overview TEST Policy** | | | |
| Agent Scan Mode | Smart scan | Conventional Scan |  |
| Manual Scan - Policy | Files to Scan > All Scannable files | File types Scanned by IntelliScan |  |
| Scan Hidden Folders | Disabled |  |
| Select - Scan compressed files. > Maximum layers: 2 | Select- Scan compressed files. > Maximum layers: 2 |  |
| 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 | Disabled - Scan boot area |  |
| CPU Usage > Medium | High |  |
| 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 | | 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. | Disabled - 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. |  |
| 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 and retrieved |  |
| Files to Scan > All Scannable files | All Scannable files |  |
| 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 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 | |  |
| 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: 00:00 |  |
| 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. | Enabled - 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 | Enabled |  |
| Ransomware Protection Protect documents against unauthorized encryption or modification | Enabled |  |
| 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 | Enabled |  |
| Action  File: quarantine  Process: Terminate | Action Set  File: Quarantine  Process: Terminate |  |
| Exception (specify exception if any) | No Exceptions added |  |
| Suspicious Connection | Enable with Block option | Enabled 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 | Enabled |  |
| Application Control | Enable | Enabled |  |
| Firewall | Enable (Optional) | Enabled |  |
| Agent Self-Protection | Enable Self-Protection with a password. | Enabled |  |
| 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. |  |

## 4.2.2 Policy Overview: 02 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 | File types Scanned by IntelliScan |  |
| Scan Hidden Folders | Disabled |  |
| Select - Scan compressed files. > Maximum layers: 2 | Select- Scan compressed files. > Maximum layers: 2 |  |
| 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 | Disabled - Scan boot area |  |
| CPU Usage > Medium | High |  |
| 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 | | 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. |  |
| 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 and retrieved |  |
| Files to Scan > All Scannable files | All Scannable files |  |
| 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 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 | |  |
| 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: 00:00 |  |
| 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. | Enabled - 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 with Ransomware Protection & Anti-exploit protection | Enabled with Ransomware Protection & Anti-exploit protection |  |
| Predictive Machine Learning | Enable | Enabled |  |
| Suspicious Connection | Enable with Block option | Enabled with Block option |  |
| Vulnerability Protection | Enable | Enabled with Inline Mode |  |
| Device Control | Enable | Enabled |  |
| Web Reputation | Enable for Internal and External agents with Security Level Medium | Enabled with Medium Security Level |  |
| Application Control | Enable | Enabled |  |
| Firewall | Enable (Optional) | Disabled |  |
| Agent Self-Protection | Enable Self-Protection with a password | Enabled |  |
| 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** | |  |  |
|  | Within Term | 28/09/2023 |  |
|  | Build | Build |  |
|  | Configure | Not Configured |  |
|  | Configure | not configured |  |
|  | Configure | Not Scheduled |  |
|  | Enable | Disabled |  |
|  | Configure | Not Configured |  |
|  | Configure | Not Configured |  |
|  | Register all Trend Micro products with Apex Central | Apex One Server is not 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. Recommend restarting those endpoints.

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

(input) agents are installed on the 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 endpoints on priority for better protection.

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

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 configured 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 Apex Central syslog is not configured, recommended to configure them to forward logs to the syslog server (For compliance purposes). For more information [Configuring Syslog Forwarding](https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/detections/logs_001/syslog-forwarding.aspx)

In Apex Central Report Maintenance is not configured, recommended to configure it.

**In Both Policy:**

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

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

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

In Manual Scan and policy settings, the scan boot area is disabled, recommended to enable it.

In Manual Scan and policy settings, CPU usage is set as High recommended to set as Medium for optimal performance.

**In TEST Policy:**

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

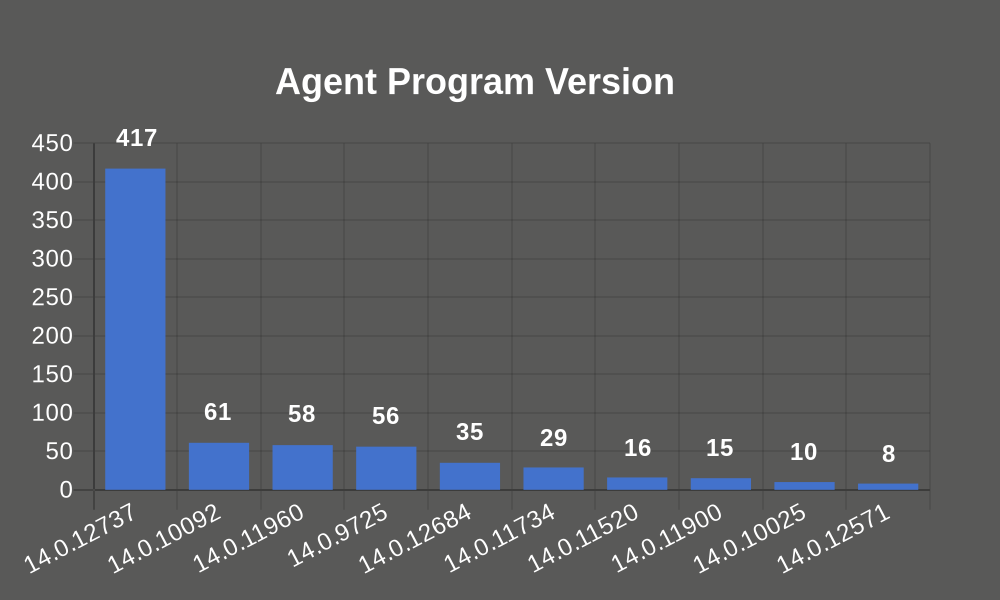
**In PUBLIC Policy:**

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.

# 5 Apex One Product Efficacy

## 5.1 Agent Distribution

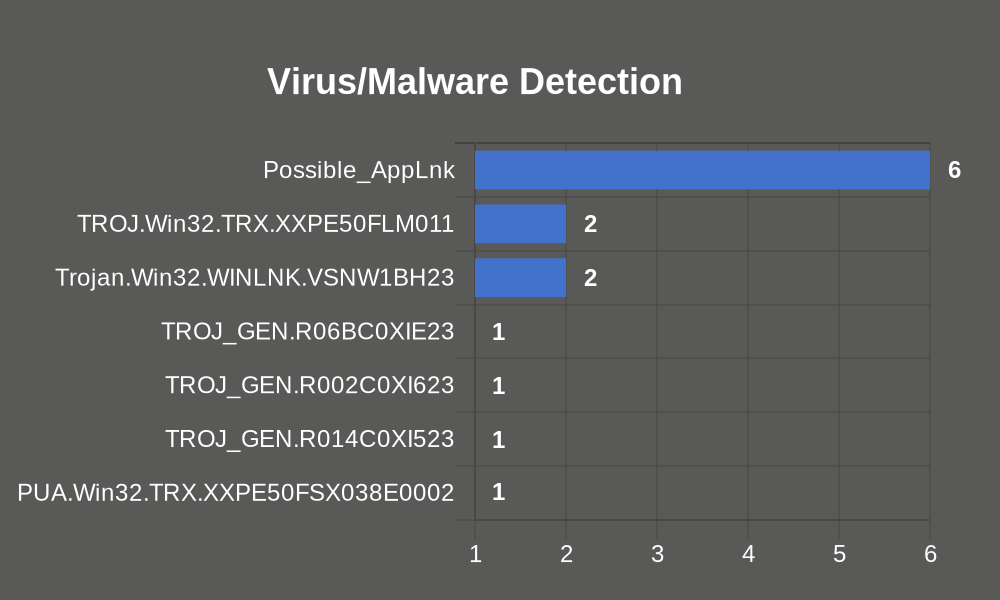
|  |  |
| --- | --- |
| **Agent Platform** | **Count** |
| Windows 11 10.0.22621 | 213 |
| Windows Server 2016 10.0.14393 | 15 |
| Windows 10 10.0.19044 | 6 |
| Windows 11 10.0.22000 | 5 |
| Windows Server 2012 6.2.9200 | 4 |
| Windows Server 2012 R2 6.3.9600 | 4 |
| Windows Server 2019 10.0.17763 | 2 |
| Windows Server 2022 10.0.20348 | 1 |
| **Total** | **250** |



14.0.12737 is the latest agent Program version recommended to upgrade all the older agents to the latest version.

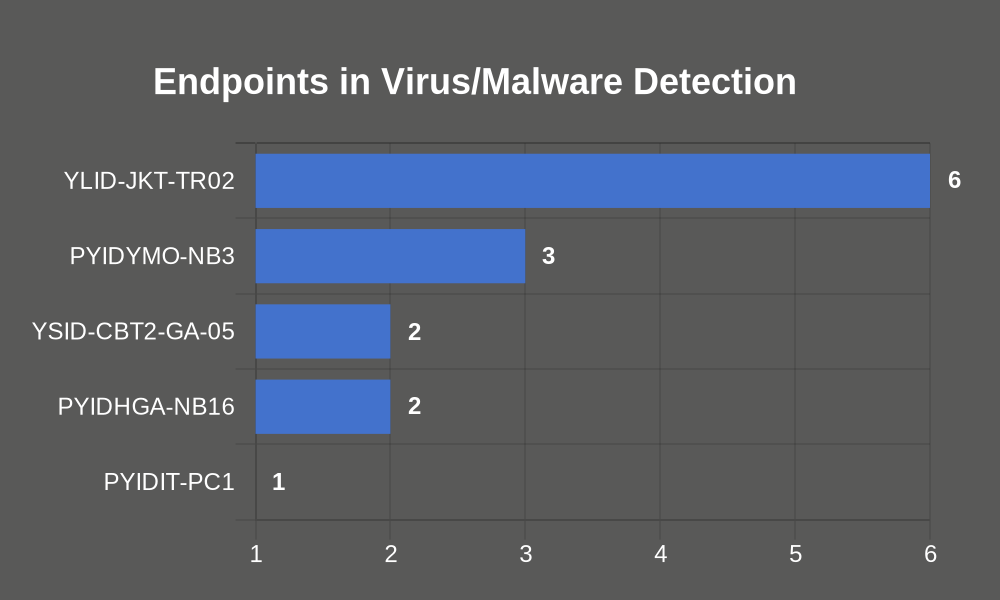
## 5.2 Virus/Malware

We generated a Virus/Malware Event of the last 30 Days on 26th Sep 2023 from Apex Central/Apex One. There was a total of 14 detections.



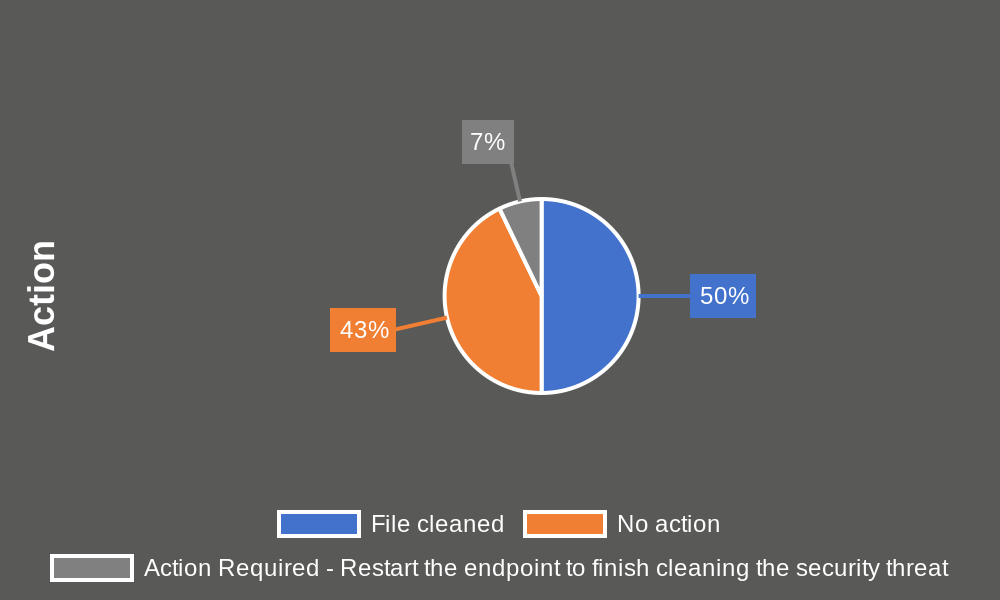
Possible\_AppLnk Virus/Malware was detected 6 times on the YLID-JKT-TR02 endpoint, and the files were successfully No action by Apex One.

TROJ.Win32.TRX.XXPE50FLM011 Virus/Malware was detected 2 times on the YSID-CBT2-GA-05 endpoint, and the files were successfully cleaned by Apex One.



6 times Virus/Malware was detected on the YLID-JKT-TR02 endpoint, and the files were successfully No action by Apex One.

3 times Virus/Malware was detected on the PYIDYMO-NB3 endpoint, and the files were successfully cleaned by Apex One.

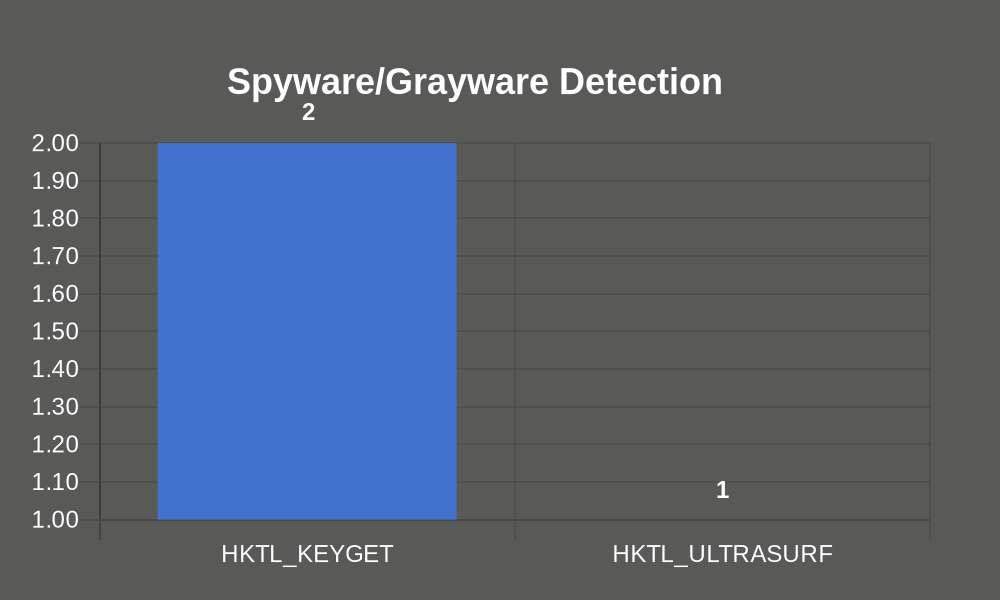


Files were cleaned, No action, and Action Required - Restart the endpoint to finish cleaning the security threat by Apex One.

Run cleanup when probable virus/malware is detected is disabled, recommended to enable in all Scan Modules.

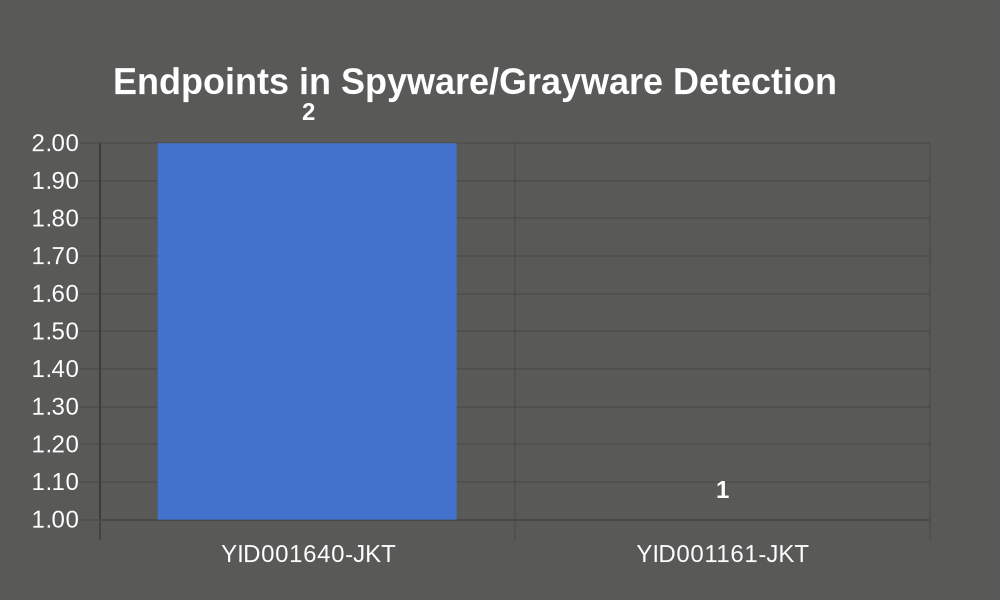
## 5.3 Spyware/ Grayware

We generated a Spyware/Grayware Event of the last 30 Days on 26th Sep 2023 from Apex Central/Apex One. There was a total of 3 detections.



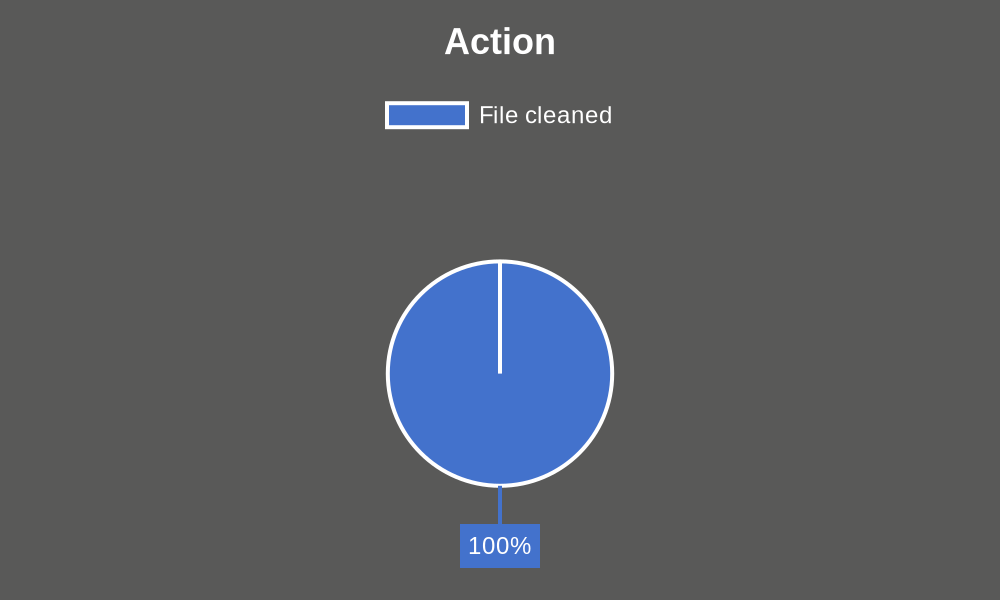
HKTL\_KEYGET Spyware/Grayware was detected 2 times on the YID001640-JKT endpoint, and the files were successfully cleaned by Apex One.

HKTL\_ULTRASURF Spyware/Grayware was detected 1 time on the YID001161-JKT endpoint, and the files were successfully cleaned by Apex One.



2 times Spyware/Grayware was detected on the YID001640-JKT endpoint, and the files were successfully cleaned by Apex One.

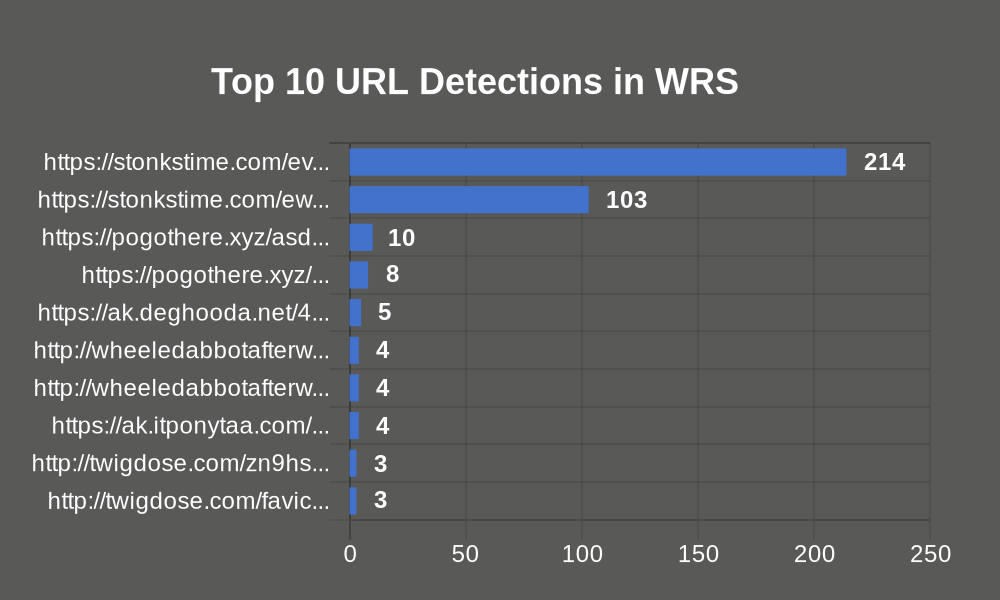
1 time Spyware/Grayware was detected on the YID001161-JKT endpoint, and the files were successfully cleaned by Apex One.



Files were cleaned by Apex One.

## 5.4 Web Reputation

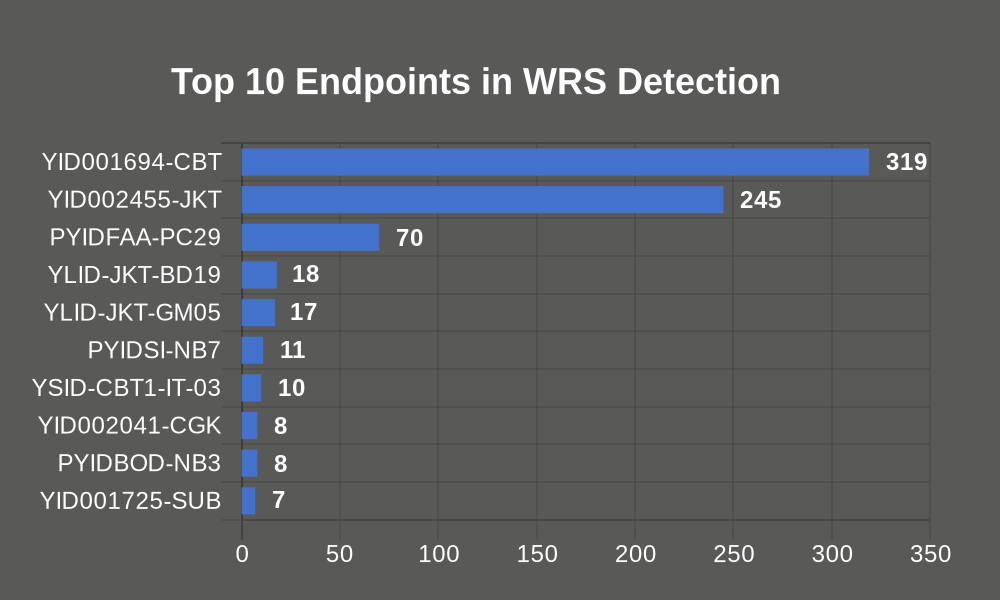
We generated a Web Reputation Detections Event of the last 30 Days on 4th Mar 2024 from Apex Central/Apex One. There was a total of 799 detections.



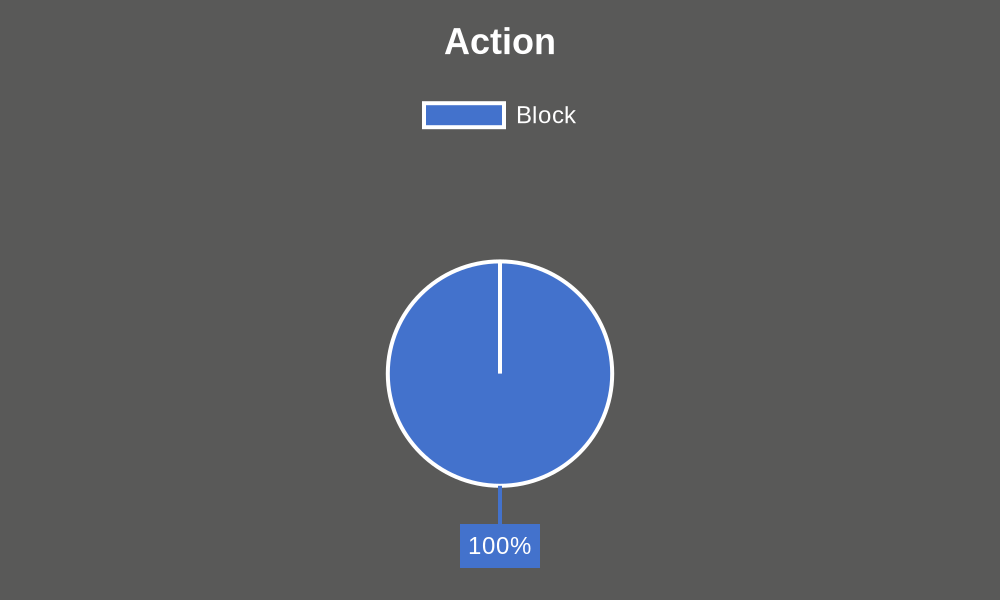
194 times HTTP sites are detected in WRS detection, and the files were successfully blocked by apex one. Check whether it's secure or not if it's secure then add it to the approved list otherwise block it.

https://stonkstime.com/event This site is detected 214 times on the YID001694-CBT endpoint, and the files were successfully blocked by apex one.

https://stonkstime.com/ewant This site is detected 103 times on the YID001694-CBT endpoint, and the files were successfully blocked by apex one.

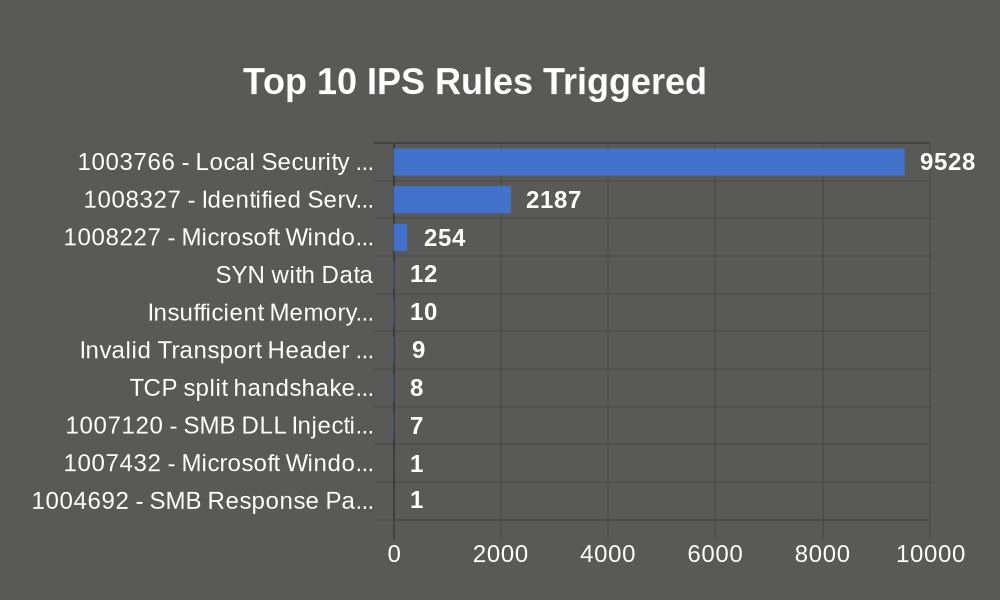


All the web violation events were successfully blocked by Apex One.



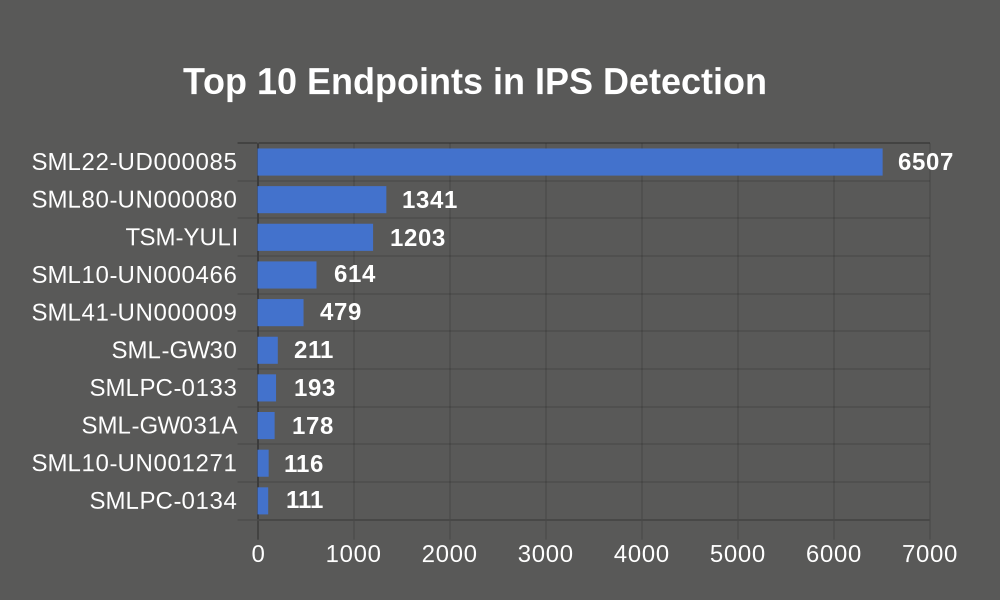
## 5.5 Intrusion Prevention

We generated an Intrusion Prevention Event of the last 30 Days on 26th Sep 2023 from Apex Central/Apex One. There was a total of 12017 detections.



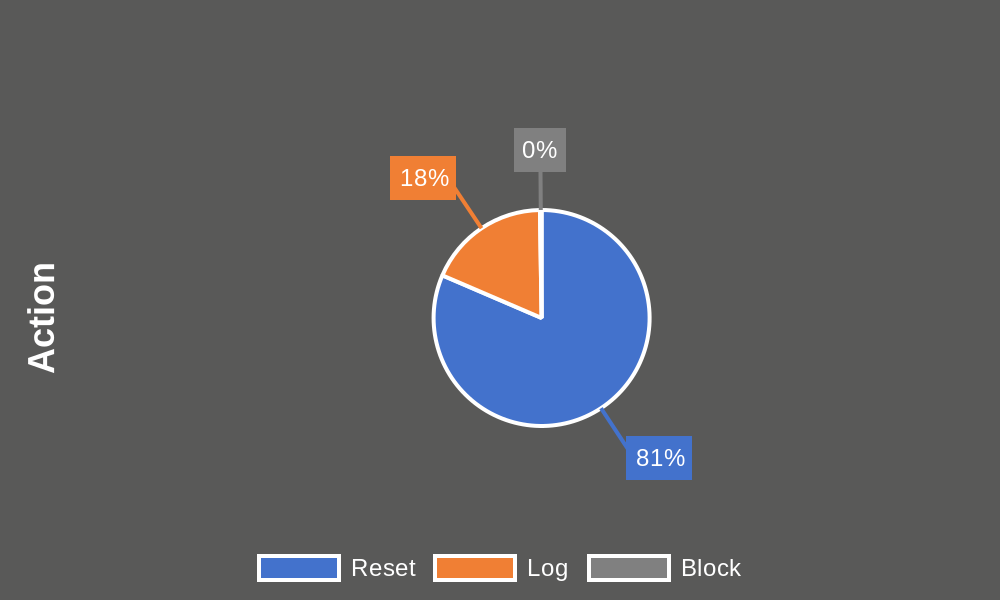
1003766 - Local Security Authority Subsystem Service Integer Overflow Vulnerability triggered 9528 times with High severity, and it is in Prevent mode and the files were successfully reset by Apex One.

1008327 - Identified Server Suspicious SMB Session triggered 2187 times with Critical severity, and it is in Prevent mode and the files were successfully logged by Apex One.



Intrusion Prevention was detected 6507 times on the SML22-UD000085 endpoint, and the files were successfully reset by Apex One.

Intrusion Prevention was detected 1341 times on the SML80-UN000080 endpoint, and the files were successfully reset by Apex One.

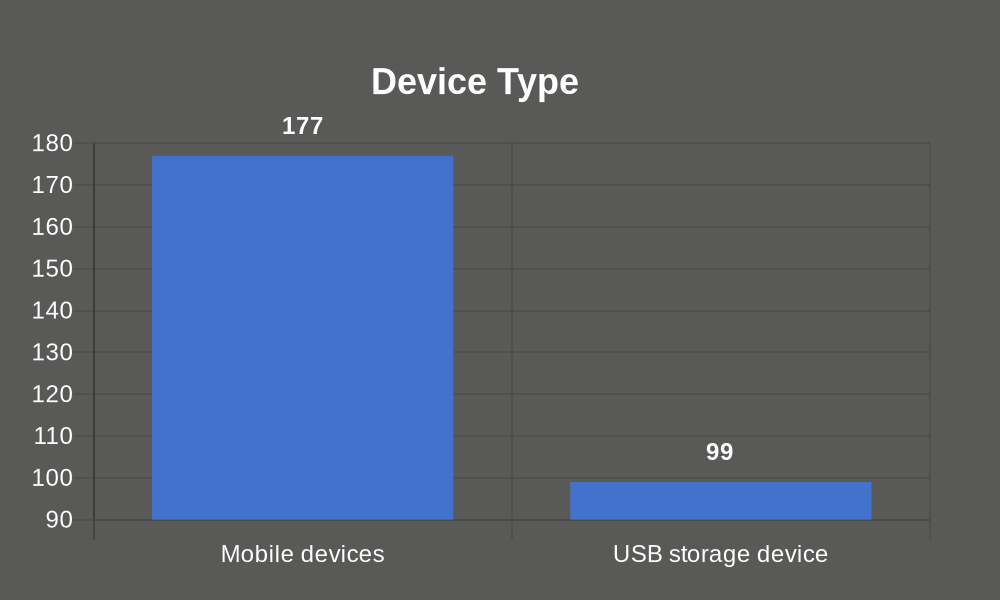


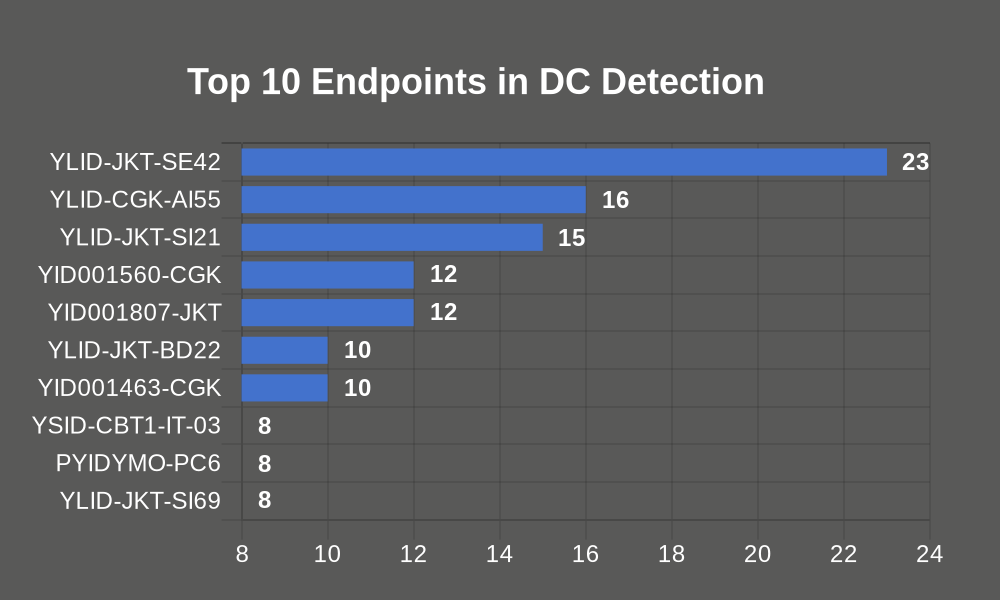
All the events that were triggered have been reset, logged, and Blocked successfully.

|  |  |  |  |
| --- | --- | --- | --- |
| **IPS DETECTION & SEVERITY** | **ACTION** | | |
| **Log** | **Reset** | **Block** |
| **1008327 - Identified Server Suspicious SMB Session** | **2187** |  |  |
| Critical |  |  |  |
| **1008227 - Microsoft Windows SMB Information Disclosure Vulnerability (CVE-2017-0147)** |  | **254** |  |
| Critical |  |  |  |
| **1003766 - Local Security Authority Subsystem Service Integer Overflow Vulnerability** |  | **9528** |  |
| High |  |  |  |
| **TCP split handshake** |  |  | **8** |
| Critical |  |  |  |
| **SYN with Data** |  |  | **12** |
| Critical |  |  |  |
| **Insufficient Memory** | **5** | **5** |  |
| Critical |  |  |  |
| **Invalid Transport Header Length** |  |  | **9** |
| Critical |  |  |  |
| **1007120 - SMB DLL Injection Exploit Detected (ATT&CK T1055.001)** | **7** |  |  |
| Low |  |  |  |
| **1007432 - Microsoft Windows Server Message Block Memory Corruption Vulnerability (CVE-2015-2474)** |  | **1** |  |
| Critical |  |  |  |
| **1004692 - SMB Response Parsing Vulnerability (CVE-2011-1268)** |  | **1** |  |
| Critical |  |  |  |
| **Total** | **2199** | **9789** | **29** |

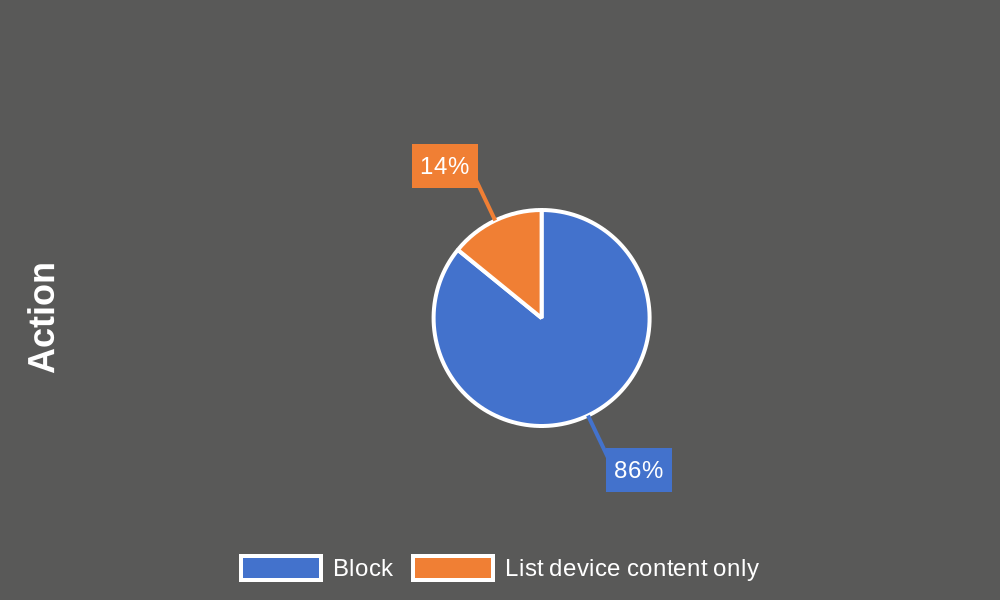
## 5.6 Device Control Detection

We generated a Device control Detection Event of the last 30 Days on 26th Sep 2023 from Apex Central/Apex One. There was a total of 276 detections.



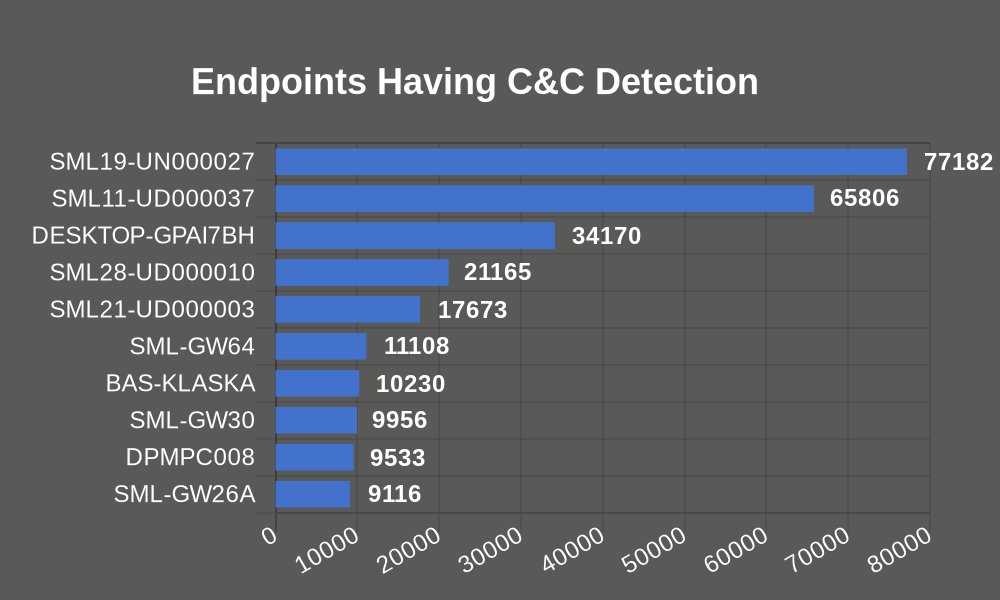


YLID-JKT-SE42 was the endpoint that was triggered the most having Device control detection and was blocked successfully.



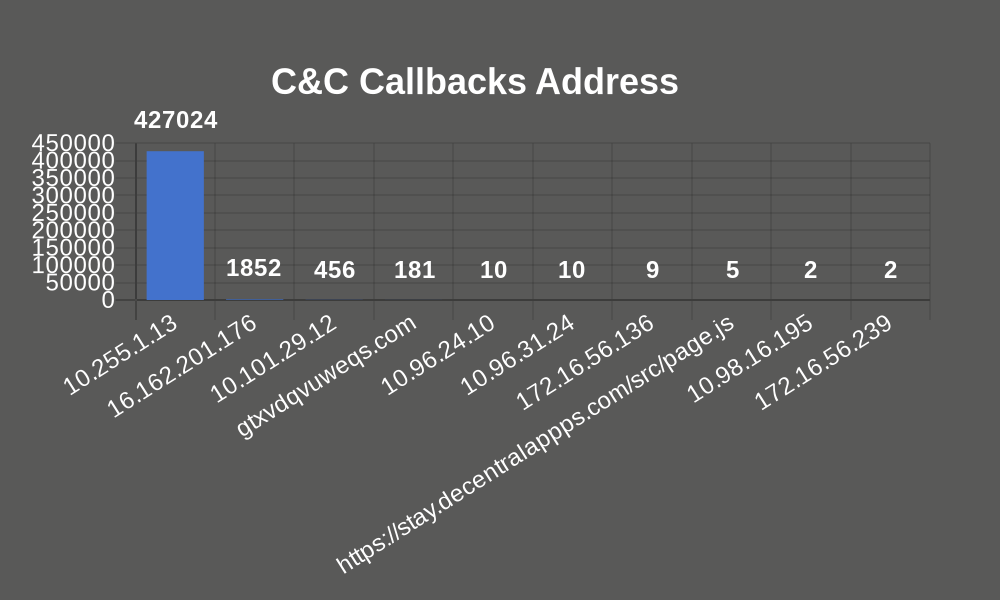
## 5.7 C&C Callback

We generated a C&C Callbacks Event of the last 7 Days on 26th Sep 2023 from Apex Central/Apex One. There was a total of 429568 detections.



77182 times C&C Callbacks were detected on the SML19-UN000027 endpoint.

65806 times C&C Callbacks were detected on the SML11-UD000037 endpoint.



10.255.1.13 callback address detected 427024 times, check this IP Address to if it's a secure connection then add it to the suspicious approve list otherwise block this IP address.

16.162.201.176 callback address detected 1852 times, check this IP Address to if it's a secure connection then add it to the suspicious approve list otherwise block this IP address.

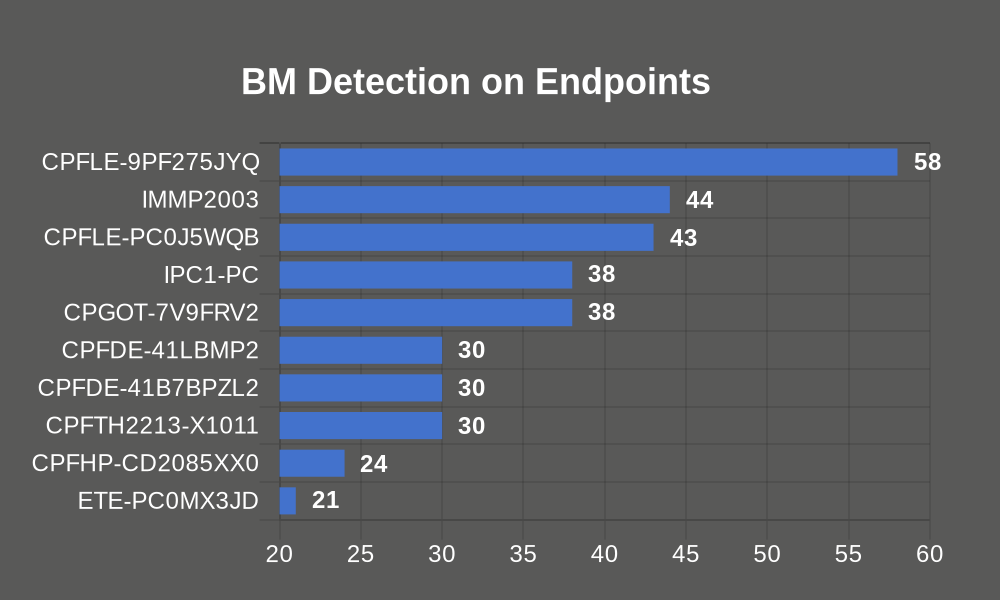
Check below KB in case of Command and Control (C&C) callback detection.

* + <https://success.trendmicro.com/solution/1121033>
  + <https://global.sitesafety.trendmicro.com/result.ph>

Recommended to check the Callback address that is triggered and whitelist the internal IP.

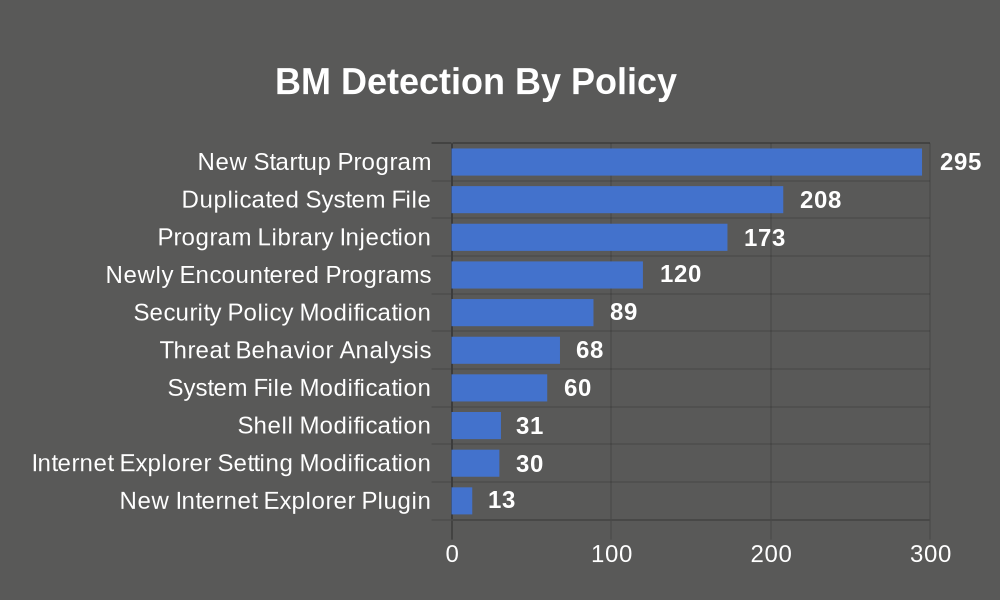
## 5.8 Behavior Monitoring

We generated a Behavior Monitoring Event of the last 30 Days on 4th Mar 2024 from Apex Central/Apex One. There was a total of 1109 detections.



On the endpoint, CPFLE-9PF275JYQ Behavior Monitoring was triggered 58 times with Low and High Severity. Processes were assessed by Apex One.

On the endpoint, IMMP2003 Behavior Monitoring was triggered 44 times with Low Severity. Processes were assessed by Apex One.



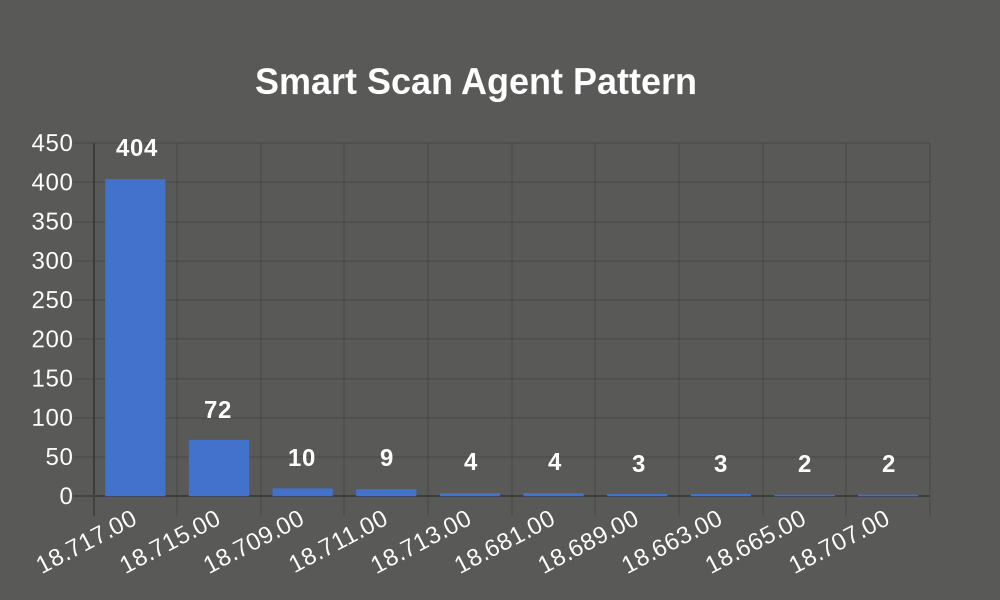
295 times New Startup Program was triggered on CPFLE-635600600, CPGOT-7V9FRV2, CPFLE-9PF275JYQ, CPF1214-AANL110, and CPFTH2301-X2066 endpoints and it was assessed by Apex One.

208 times Duplicated System File was triggered on CPFHP-CG8120WM7, ETE-PC0MX3JD, CPFTH2301-X1358, CPF1313-X1099, and CPFHP-CG0127NW5 endpoints and it was assessed by Apex One.

|  |  |  |  |
| --- | --- | --- | --- |
| **BM BY POLICY & RISK LEVEL** | **ACTION** | | |
| **Assess** | **Deny** | **Terminate** |
| **New Startup Program** | **295** |  |  |
| Low |  |  |  |
| **Duplicated System File** | **208** |  |  |
| Low |  |  |  |
| **Program Library Injection** | **172** | **1** |  |
| Low |  |  |  |
| **Newly Encountered Programs** | **95** | **25** |  |
| Low |  |  |  |
| **Security Policy Modification** | **89** |  |  |
| High |  |  |  |
| Low |  |  |  |
| **Threat Behavior Analysis** |  | **4** | **64** |
| High |  |  |  |
| **System File Modification** | **60** |  |  |
| High |  |  |  |
| **Shell Modification** | **31** |  |  |
| Low |  |  |  |
| **Internet Explorer Setting Modification** | **30** |  |  |
| High |  |  |  |
| **New Internet Explorer Plugin** | **13** |  |  |
| Low |  |  |  |
| **Total** | **993** | **30** | **64** |

## 5.9 Smart Scan Agent Pattern Coverage Details

|  |  |
| --- | --- |
| Last 7 days Pattern updated agents | 502 |
| Older than 7 Days Pattern updated agents | 320 |
| Total Agents | 822 |



# 6 Apex One & Apex Central Further Information

[Apex One Administrator Guide](https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p3_ag.pdf)

[Apex One Installation and Upgrade Guide](https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_iug.pdf)

# 7 End of Life for Trend Micro Products information

<https://success.trendmicro.com/solution/1105726>

# 8 Other documentation

[Apex One Best Practice Guide](https://powerbox-na-file.trend.org/SFDC/DownloadFile_iv.php?jsonInfo=%7B%22Query%22%3A%22E6%2FaBX7NRLgNhlFV9prpuOiZ%2BfBD3GRI5g3EWcXN2wO0yrcs72AtOr%2Bd7jbTo0Fnj%2F%2F%2F76wXivkV6IVgYXc%2BQzbD%2B%2FKfkbOyItLyPfpSIJoT0HV%2B3GhPZU02OB6BmcIuhU7IZ3Ki%2B2ZNf3oZi%2FxcX%2BaDQ3AXLm1NlrYHrKAmBWl808Gv8mFeN0MeOaCoZ5%2FOZJhpJ4W6NboPVDxDNrHY%2BZWIfRvXkGVzX0vnfp%2B%2Fc34HfH%2B4SyIIL7cbRn1vJCEsxqanrr7sqZePi1K2jesmdb4l7KQ5HiOampFamEGT698%3D%22%2C%22iv%22%3A%224ce282318ea4758451af77c290c71f25%22%7D)