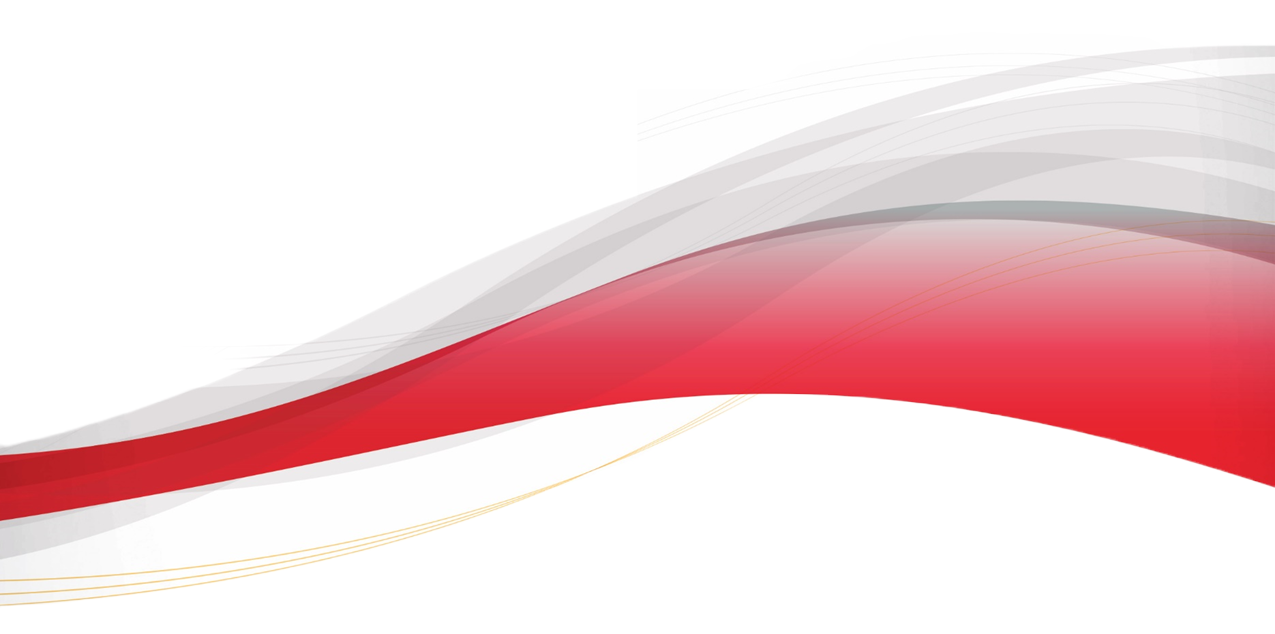
Trend Micro Health Check  
Endpoint Security for



Review of EVENTUS 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** | Review of EVENTUS Apex One 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 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. Trend Micro recommends that EVENTUS 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 may have in place and context as if EVENTUS 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 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 the Windows 7 (Legacy OS) platform.

(input) endpoints are without policy.

Active Directory Sync is configured in Apex Central.

Reports are configured in Apex Central.

Syslog is configured in Apex Central.

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

282 Virus/Malware Detected

25 Spyware/Grayware Detected

836 Web Reputation Detected

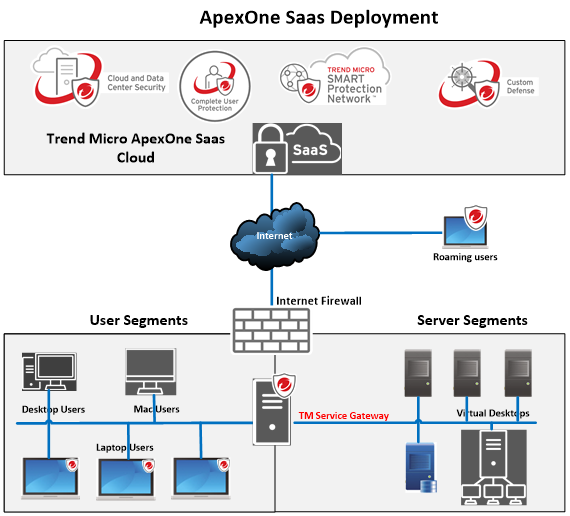
24305 Intrusion Prevention Detected

18477 Device Control Detected

136200 C&C Callback Detected

650 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 Policy Overview: NAME-OF-POLICY Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Policy Configuration - Overview NAME-OF-POLICY Policy** | | | |
| Agent Scan Mode | Smart scan | Smart Scan |  |
| Manual Scan - Policy | Files to Scan > All Scannable files | All Scannable files |  |
| Scan Hidden Folders | Enabled |  |
| 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 | Enabled 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 | | 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 - Malware Behavior Blocking Threats to block Known and potential threats | Disabled Malware Behavior Blocking Known threats |  |
| Ransomware Protection Enable - Protect documents against unauthorized encryption or modification Enable - Automatically backup and restore files changed by suspicious programs | Disabled Protect documents against unauthorized encryption or modification Disabled Automatically back up and restore files changed by suspicious programs |  |
| Enable - Block processes commonly associated with ransomware | Disabled |  |
| Enable program inspection to detect and block compromised executable files | Disabled |  |
| Anti-exploit Protection Enable - Terminate programs that exhibit abnormal behavior associated with exploit attacks | Disabled |  |
| Newly Encountered Programs Enable - Monitor newly encountered programs downloaded through web or email application channels Prompt user | Disabled Monitor newly encountered programs downloaded through web or email application channels Log Only |  |
| Enable - Event Monitoring | Disabled |  |
| Exceptions (specify exception if any) | exceptions added to the Approved Program list |  |
| Predictive Machine Learning | Enable | Disabled |  |
| Action  File: quarantine  Process: Terminate | Action Set  File: Log Only  Process: Log Only |  |
| Exception (specify exception if any) | 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. |  |

## 4.3 Apex Central Configuration Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Configuration Health - Overview** | |  |  |
| License | Within Term | Invalid date |  |
| Version | Build | Build |  |
| Active Directory Sync | Configure | Configured |  |
| Log Retention | Configure | Configured |  |
| Reports | Configure | Scheduled |  |
| Event Notifications | Enable | Enabled |  |
| 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. 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.

**In NAME-OF-POLICY Policy:**

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

In Behaviour Monitoring, Threats to block are selected to Known Threats recommended to select Known and potential threats. It Blocks behavior associated with known threats and acts on behavior that is potentially malicious.

In Behaviour Monitoring, protecting documents against unauthorized encryption or modification is disabled recommended to enable it. It will protect the unauthorized encryption or modification of trusted files.

In Behaviour Monitoring, Block processes commonly associated with ransomware is disabled and recommended to enable it. Ransomware commonly distributes executable files in specific locations on endpoints before attempting to hijack files. Blocking the processes started from these locations can help prevent the ransomware from being able to hijack files.

In Behaviour Monitoring, enabling program inspection to detect and block compromised executable files is disabled and recommended to enable it. Program inspection monitors processes and performs API hooking to determine if a program is behaving in an unexpected manner.

In Behaviour Monitoring, Anti-Exploit protection is disabled and recommended to enable it. Anti-exploit protection works in conjunction with program inspection to monitor the behavior of programs and detect abnormal behavior that may indicate that an attacker has exploited a program vulnerability.

In Behaviour Monitoring, Newly Encountered Program Protection is disabled and recommended to enable it. it works in conjunction with Web Reputation Services and Real-time Scan to verify the prevalence of files downloaded through web channels, email applications, or Microsoft Office macro scripts.

In Behaviour Monitoring, Event Monitoring is disabled and recommended to enable it. Event Monitoring provides a more generic approach to protecting against unauthorized software and malware attacks. It monitors system areas for certain events, allowing administrators to regulate programs that trigger such events.

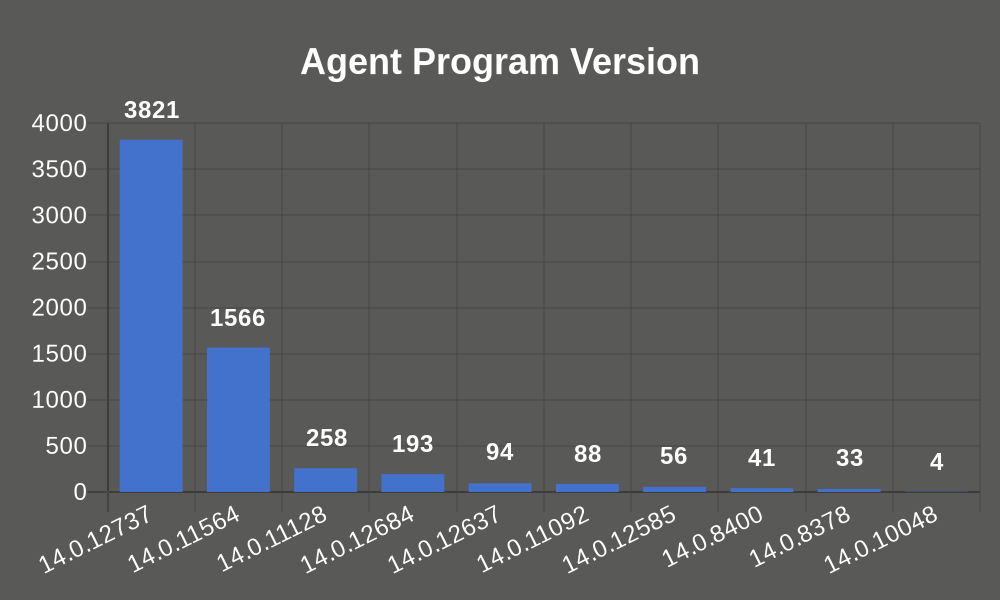
The predictive Machine Learning module is disabled, recommended to enable it. It uses advanced machine learning technology to correlate threat information and perform in-depth file analysis or behavioral process and script analysis to detect emerging unknown security risks.

In Predictive Machine Learning module is enabled with log-only mode, recommended to set the action Terminate/Quarantine to prevent unknown threats.

# 5 Apex One Product Efficacy

## 5.1 Agent Distribution

|  |  |
| --- | --- |
| **Agent Platform** | **Count** |
| Windows 10 10.0.19045 | 3134 |
| Windows 10 10.0.14393 | 906 |
| Windows 11 10.0.22621 | 634 |
| Windows 10 10.0.18363 | 336 |
| Windows 7 6.1.7601 | 314 |
| Windows 10 10.0.19044 | 214 |
| Windows 10 10.0.17763 | 208 |
| Windows 10 10.0.19043 | 94 |
| Windows 11 10.0.22000 | 90 |
| Windows 10 10.0.19042 | 77 |
| Windows 10 10.0.17134 | 51 |
| Windows 10 10.0.18362 | 30 |
| Windows 10 10.0.19041 | 25 |
| Windows 8.1 6.3.9600 | 24 |
| Windows 10 10.0.16299 | 23 |
| Windows 7 Embedded 6.1.7601 | 22 |
| Windows 10 10.0.10240 | 18 |
| Windows 10 10.0.15063 | 8 |
| Windows Server 2019 10.0.18363 | 7 |
| Windows Server 2016 10.0.14393 | 6 |
| Windows 7 6.1.7600 | 6 |
| Windows 10 10.0.10586 | 6 |
| Windows Server 2019 10.0.17763 | 5 |
| Windows 10 10.0.21996 | 1 |
| Windows Server 2012 R2 6.3.9600 | 1 |
| Windows Server 2008 6.1.7600 | 1 |
| **Total** | **6241** |



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

(INPUT) endpoints (NAMES-OF-ENDPOINTS) are required restart for cleanup.

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

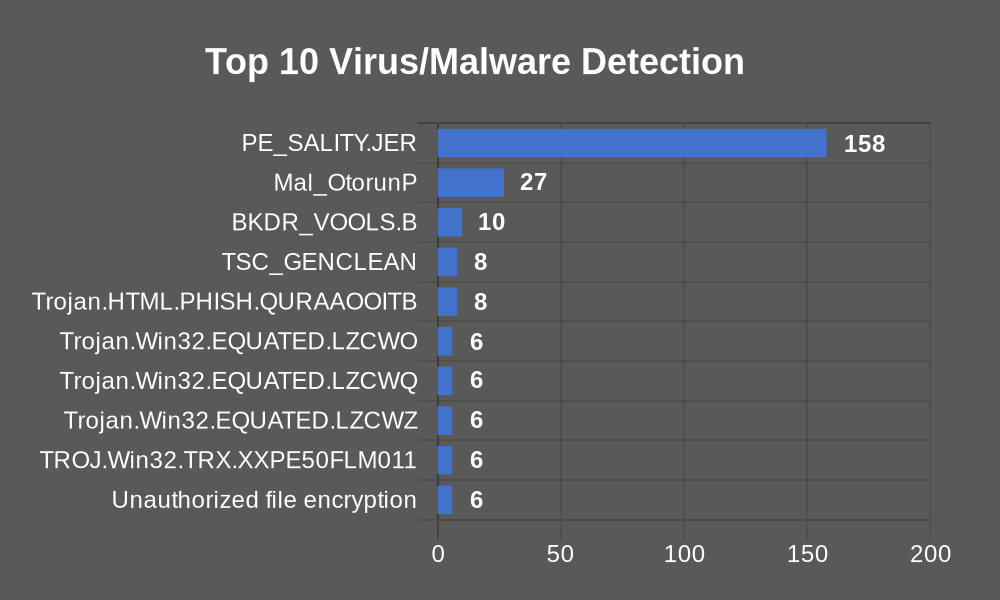
(INPUT) agents have outdated patterns older than 7 days out of (INPUT) agents.

(INPUT) agents (NAMES-OF-AGENTS) are using the Windows servers platform.

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

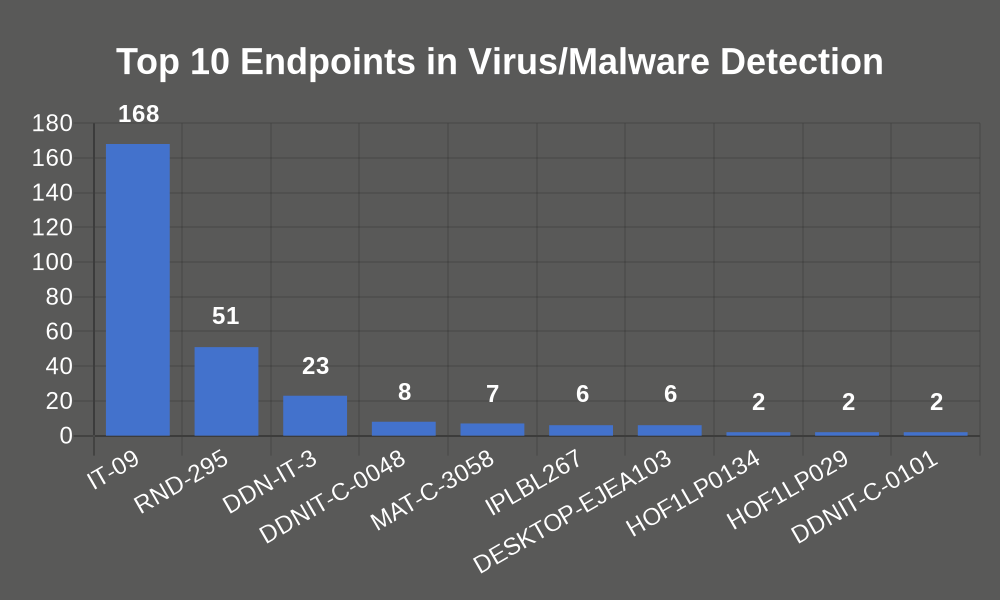
## 5.2 Virus/Malware

We generated a Virus/Malware Event of the last 30 Days on 10th Oct 2023 from Apex Central/Apex One. There was a total of 282 detections.



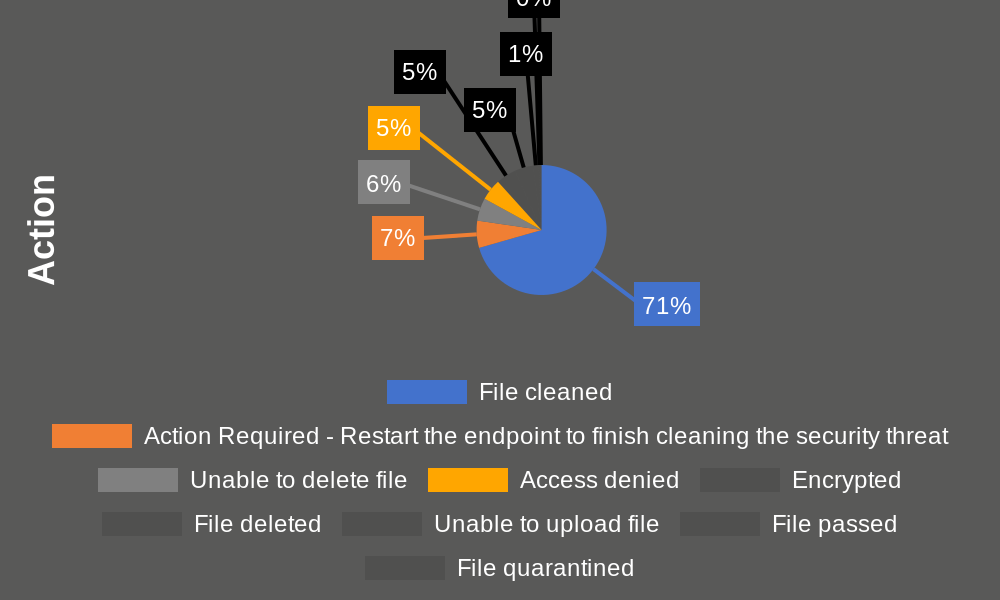
PE\_SALITY.JER Virus/Malware was detected 158 times on the IT-09 endpoint, and the files were successfully cleaned, unable to delete files, Encrypted, access denied, and Action Required - Restart the endpoint to finish cleaning the security threat by Apex One.

Mal\_OtorunP Virus/Malware was detected 27 times on DDN-IT-3, DDNIT-C-0048, and DDNIT-C-0101 endpoints, and the files were successfully cleaned, access denied, deleted, and Action Required - Restart the endpoint to finish cleaning the security threat by Apex One.



168 times Virus/Malware was detected on the IT-09 endpoint, and the files were successfully cleaned, Encrypted, unable to delete files, deleted, and Action Required - Restart the endpoint to finish cleaning the security threat by Apex One.

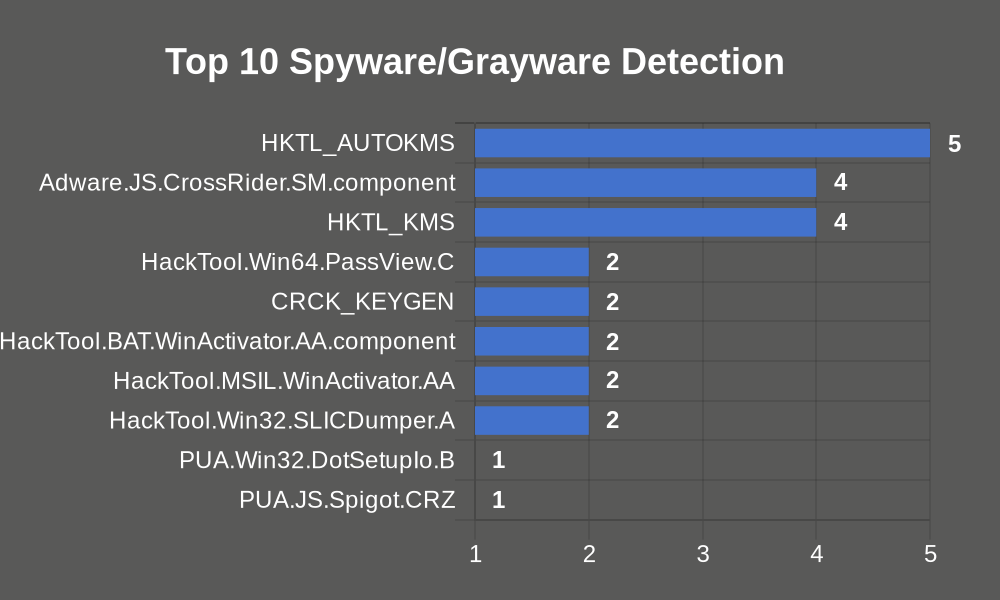
51 times Virus/Malware was detected on the RND-295 endpoint, and the files were successfully cleaned, deleted, unable to delete files, access denied, and Action Required - Restart the endpoint to finish cleaning the security threat by Apex One.



Files were cleaned, Action Required - Restart the endpoint to finish cleaning the security threat, unable to delete files, access denied, Encrypted, deleted, unable to upload files, passed, and quarantined by Apex One.

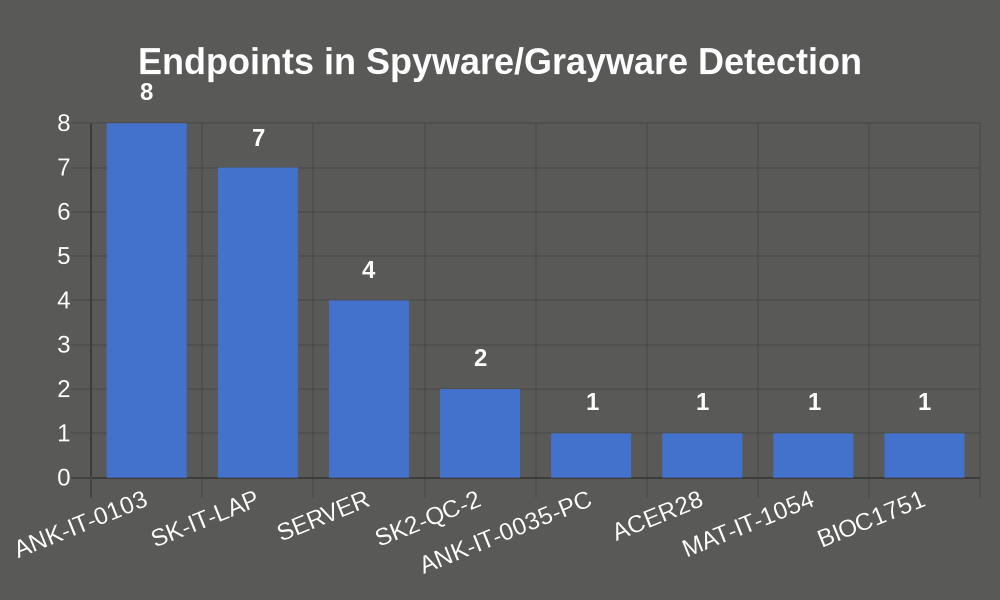
## 5.3 Spyware/ Grayware

We generated a Spyware/Grayware Event of the last 30 Days on 10th Oct 2023 from Apex Central/Apex One. There was a total of 25 detections.



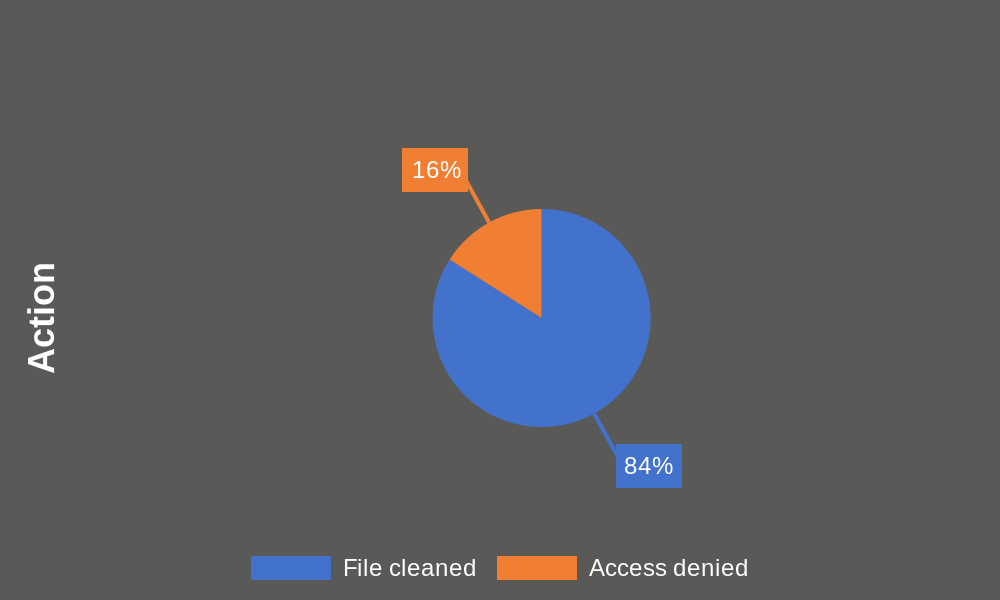
HKTL\_AUTOKMS Spyware/Grayware was detected 5 times on the SK-IT-LAP endpoint, and the files were successfully cleaned by Apex One.

Adware.JS.CrossRider.SM.component Spyware/Grayware was detected 4 times on the SERVER endpoint, and the files were successfully access denied by Apex One.



8 times Spyware/Grayware was detected on the ANK-IT-0103 endpoint, and the files were successfully cleaned by Apex One.

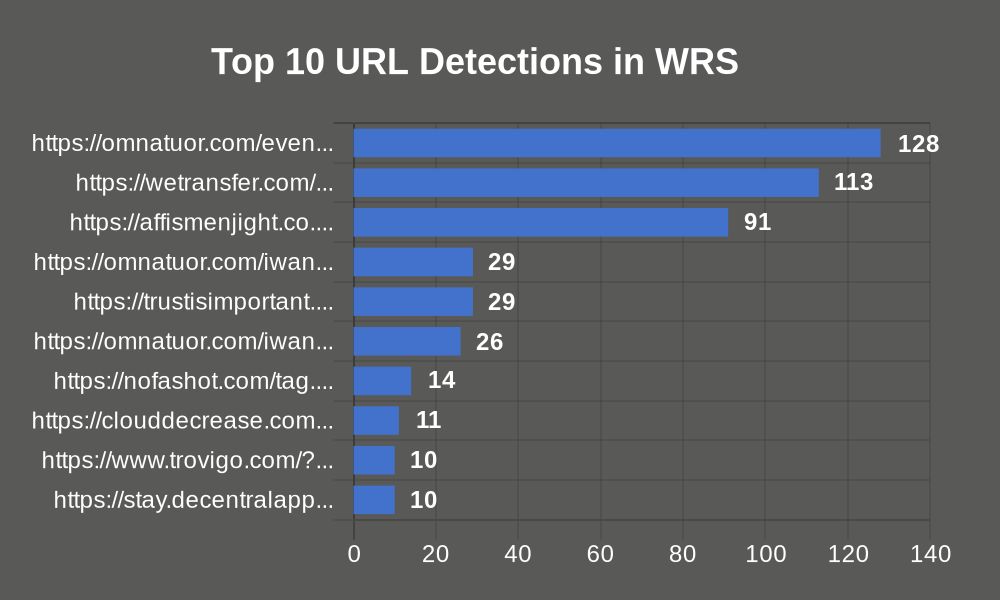
7 times Spyware/Grayware was detected on the SK-IT-LAP endpoint, and the files were successfully cleaned by Apex One.



Files were cleaned, and access denied by Apex One.

## 5.4 Web Reputation

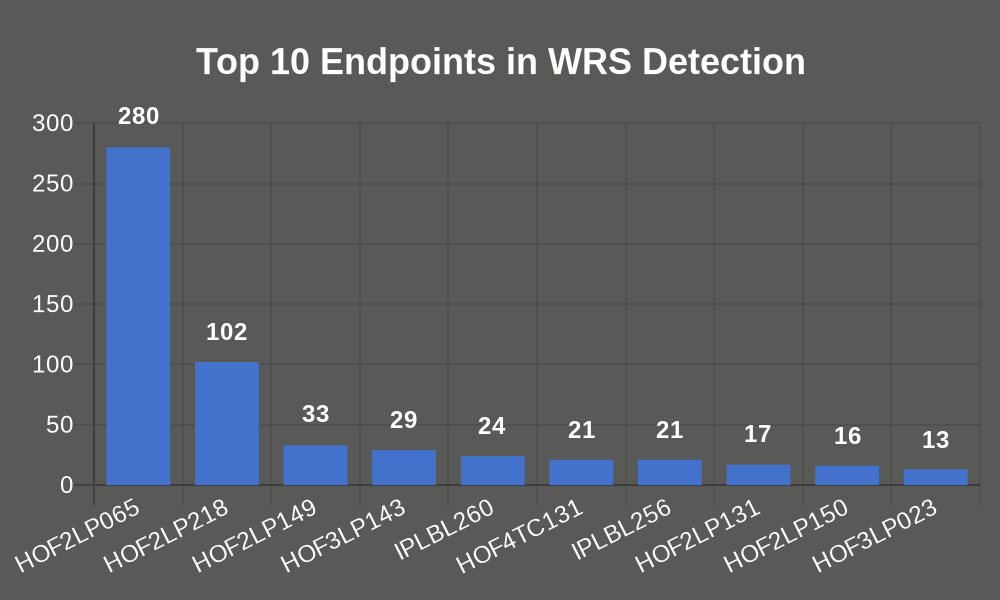
We generated a Web Reputation Detections Event of the last 30 Days on 10th Oct 2023 from Apex Central/Apex One. There was a total of 836 detections.



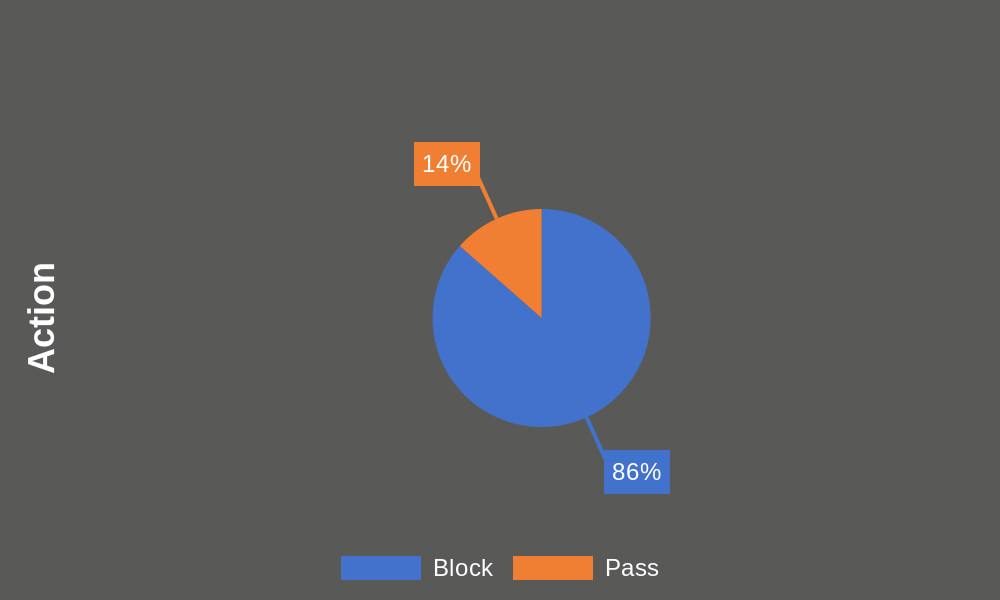
65 times HTTP sites are detected in WRS detection, and the files were successfully blocked by Apex One. Check whether it's secure or not if it's secure then add it to the approved list otherwise block it.

https://omnatuor.com/event This site is detected 128 times on the HOF2LP065 endpoint, and the files were successfully blocked by Apex One.

https://wetransfer.com/ This site is detected 113 times on HOF2LP281, HOF2LP125, HOF2LP259, HOF4TC131, and HOF2LP128 endpoints, and the files were successfully Pass by Apex One.

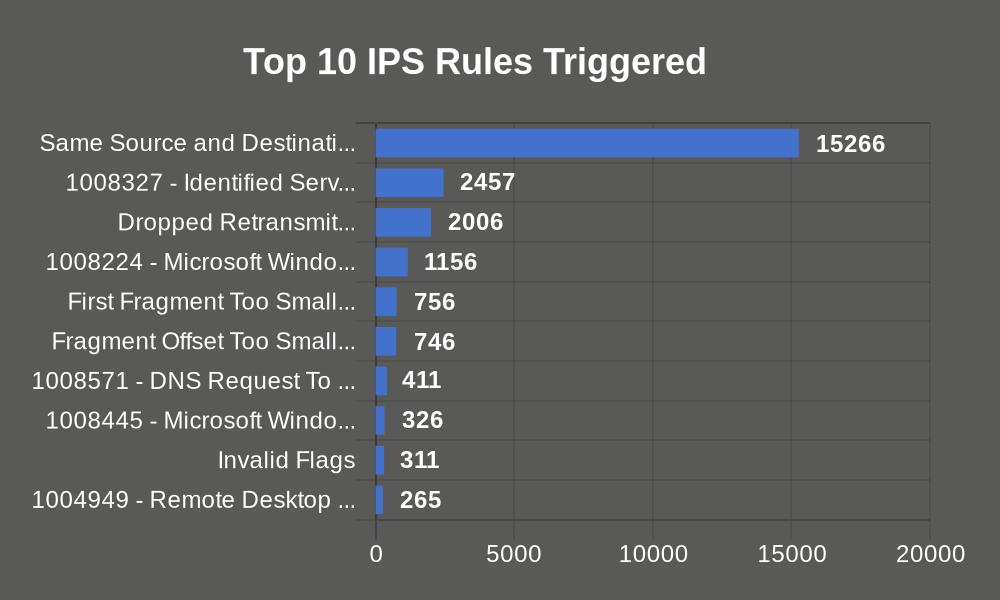


All the web violation events were successfully blocked by Apex One.



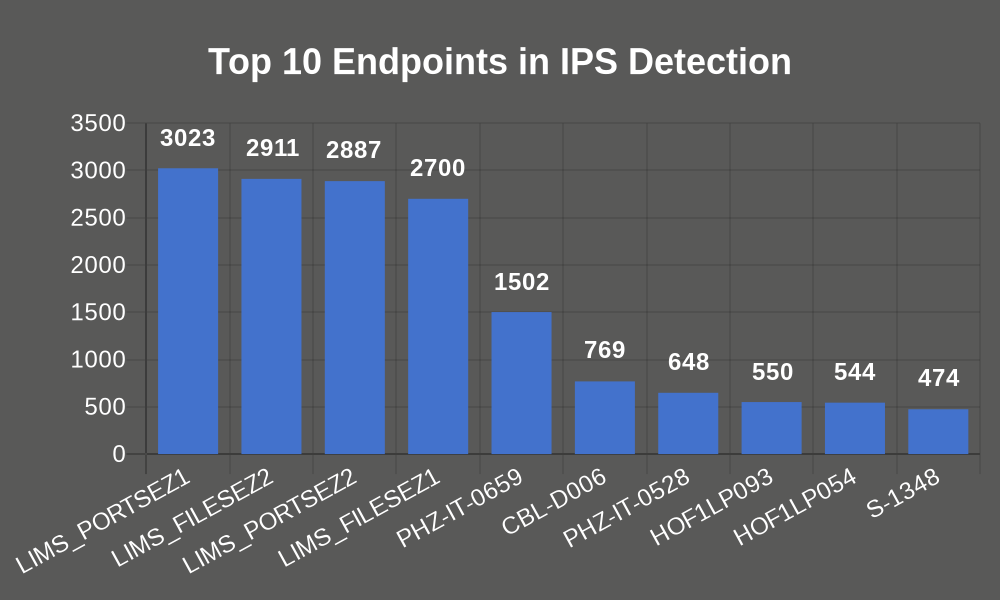
## 5.5 Intrusion Prevention

We generated an Intrusion Prevention Event of the last 30 Days on 10th Oct 2023 from Apex Central/Apex One. There was a total of 24305 detections.



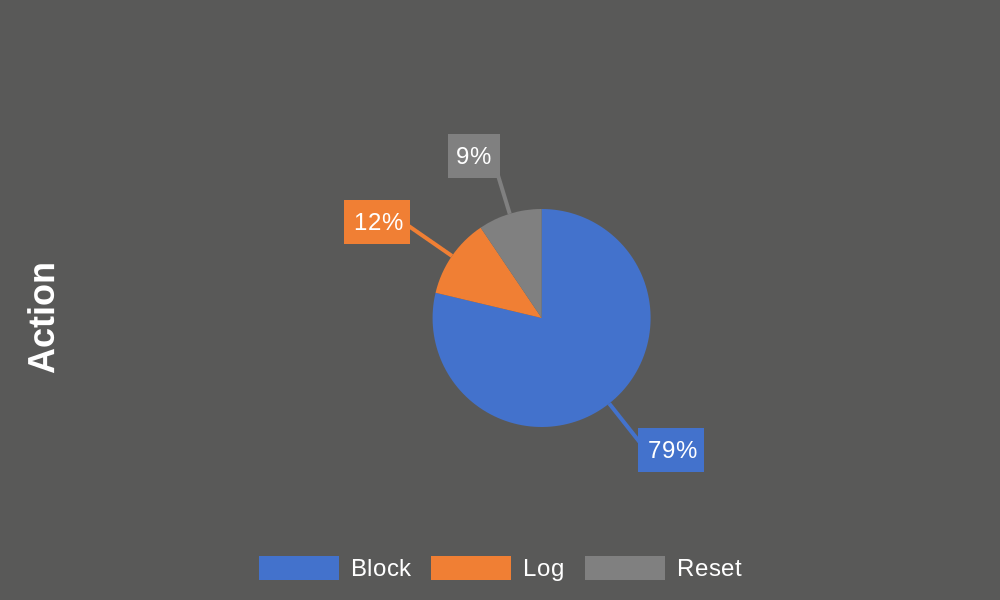
Same Source and Destination IP triggered 15266 times with Critical severity, and it is in Prevent mode and the files were successfully blocked by Apex One.

1008327 - Identified Server Suspicious SMB Session triggered 2457 times with Critical severity, and it is in Prevent mode and the files were successfully logged by Apex One.



Intrusion Prevention was detected 3023 times on the LIMS\_PORTSEZ1 endpoint, and the files were successfully blocked by Apex One.

Intrusion Prevention was detected 2911 times on the LIMS\_FILESEZ2 endpoint, and the files were successfully blocked by Apex One.

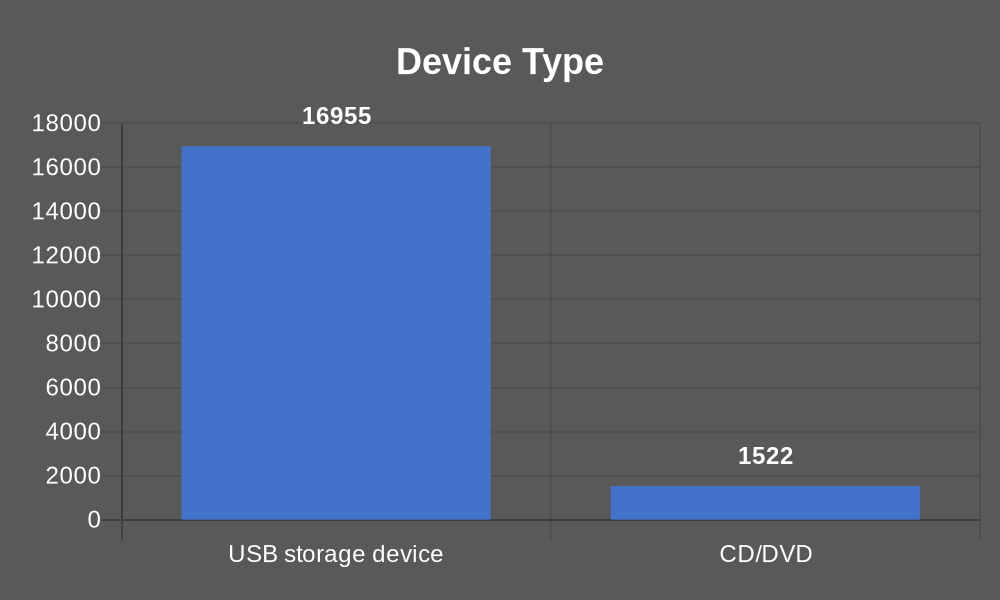


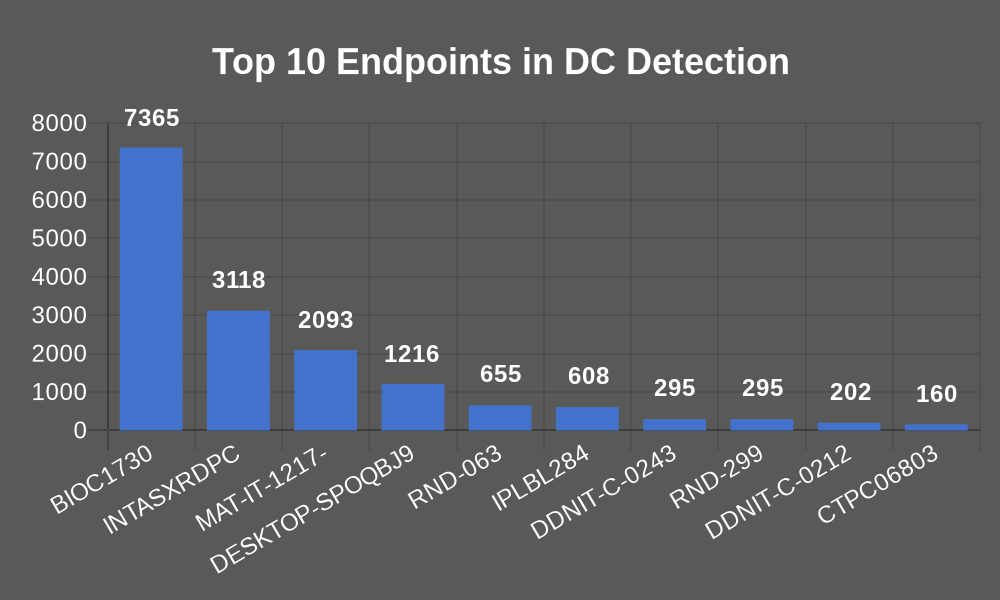
All the events that were triggered have been blocked, logged, and reset successfully.

|  |  |  |  |
| --- | --- | --- | --- |
| **IPS DETECTION & SEVERITY** | **ACTION** | | |
| **Reset** | **Block** | **Log** |
| **1004949 - Remote Desktop Protocol Vulnerability (CVE-2012-0002)** | **265** |  |  |
| Critical |  |  |  |
| **Dropped Retransmit** |  | **2006** |  |
| Critical |  |  |  |
| **1008571 - DNS Request To ShadowPad Domain Detection** |  |  | **411** |
| High |  |  |  |
| **Same Source and Destination IP** |  | **15266** |  |
| Critical |  |  |  |
| **1008224 - Microsoft Windows SMB Remote Code Execution Vulnerabilities (CVE-2017-0144 and CVE-2017-0146)** | **1156** |  |  |
| Critical |  |  |  |
| **1008327 - Identified Server Suspicious SMB Session** |  |  | **2457** |
| Critical |  |  |  |
| **1008227 - Microsoft Windows SMB Information Disclosure Vulnerability (CVE-2017-0147)** | **264** |  |  |
| Critical |  |  |  |
| **1007561 - Identified Windows DCERPC AUTH LEVEL CONNECT Password Validate Request** | **96** |  |  |
| Medium |  |  |  |
| **Invalid TCP Header Length** |  | **18** |  |
| Critical |  |  |  |
| **1008445 - Microsoft Windows Search Remote Code Execution Vulnerability (CVE-2017-8543)** | **326** |  |  |
| Critical |  |  |  |
| **1003766 - Local Security Authority Subsystem Service Integer Overflow Vulnerability** | **178** |  |  |
| High |  |  |  |
| **Insufficient Memory** | **9** |  | **9** |
| Critical |  |  |  |
| **First Fragment Too Small** |  | **756** |  |
| Critical |  |  |  |
| **SYN with Data** |  | **11** |  |
| Critical |  |  |  |
| **Invalid Flags** |  | **311** |  |
| Critical |  |  |  |
| **Fragment Offset Too Small** |  | **746** |  |
| Critical |  |  |  |
| **TCP split handshake** |  | **7** |  |
| Critical |  |  |  |
| **Packet on Closed Connection** |  | **11** |  |
| Critical |  |  |  |
| **1007432 - Microsoft Windows Server Message Block Memory Corruption Vulnerability (CVE-2015-2474)** | **2** |  |  |
| Critical |  |  |  |
| **Total** | **2296** | **19132** | **2877** |

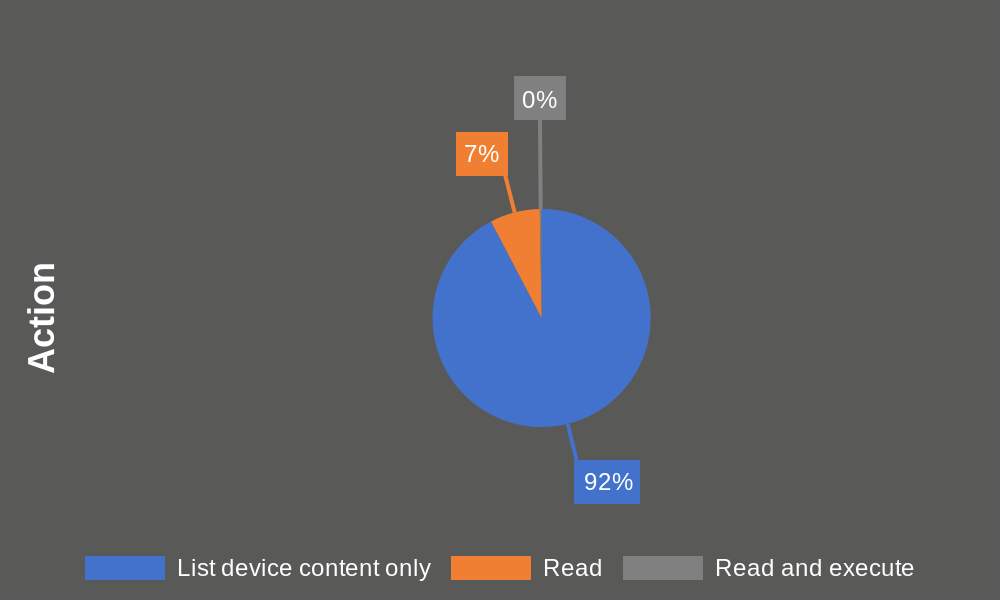
## 5.6 Device Control Detection

We generated a Device control Detection Event of the last 30 Days on 10th Oct 2023 from Apex Central/Apex One. There was a total of 18477 detections.



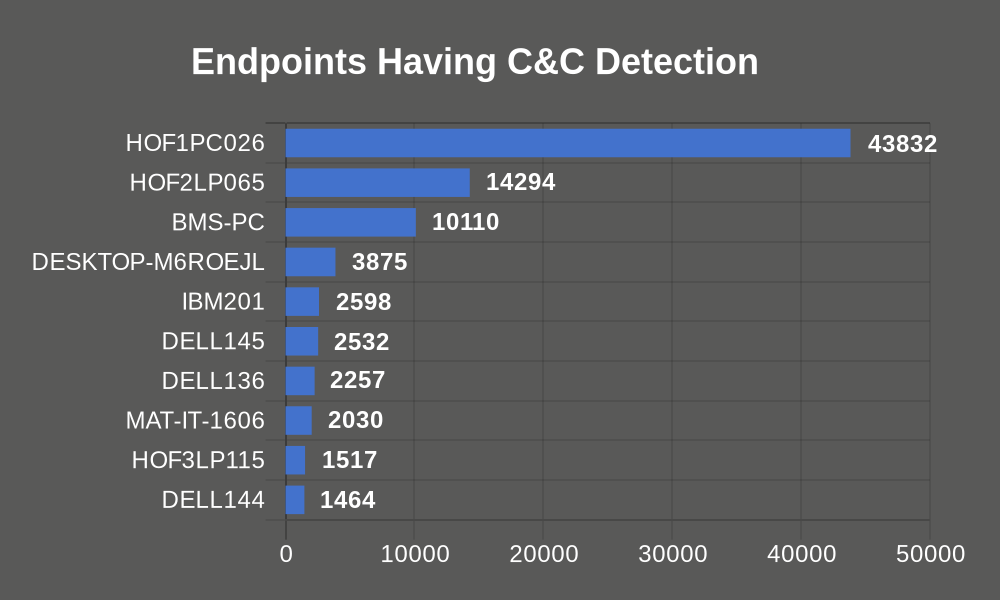


BIOC1730 was the endpoint that was triggered the most having Device control detection and was list device content only successfully.



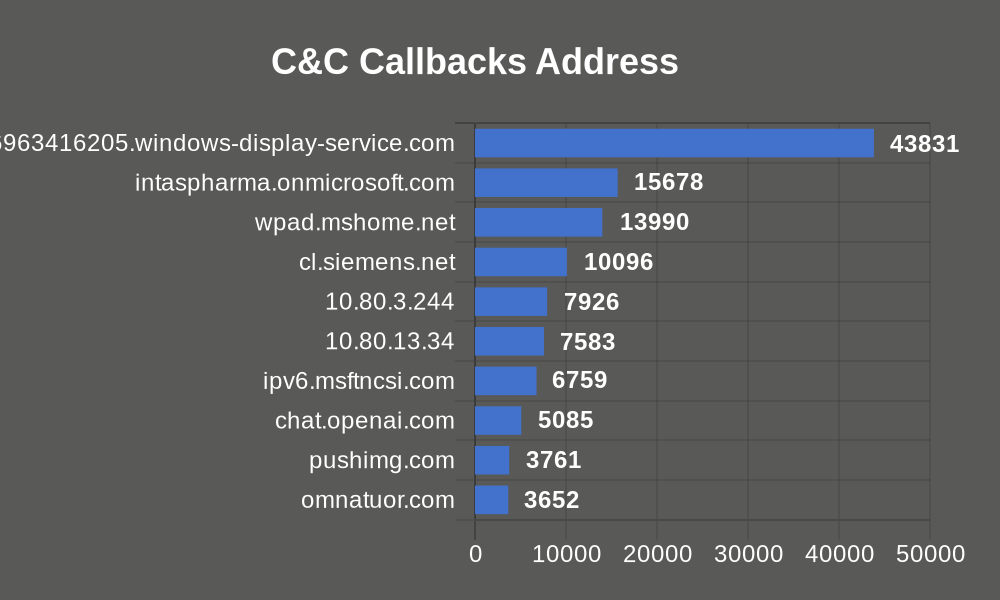
## 5.7 C&C Callback

We generated a C&C Callbacks Event of the last 30 Days on 10th Oct 2023 from Apex Central/Apex One. There was a total of 136200 detections.



43832 times C&C Callbacks were detected on the HOF1PC026 endpoint.

14294 times C&C Callbacks were detected on the HOF2LP065 endpoint.



www.google.com.205196963416205.windows-display-service.com callback address detected 43831 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.

intaspharma.onmicrosoft.com callback address detected 15678 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.

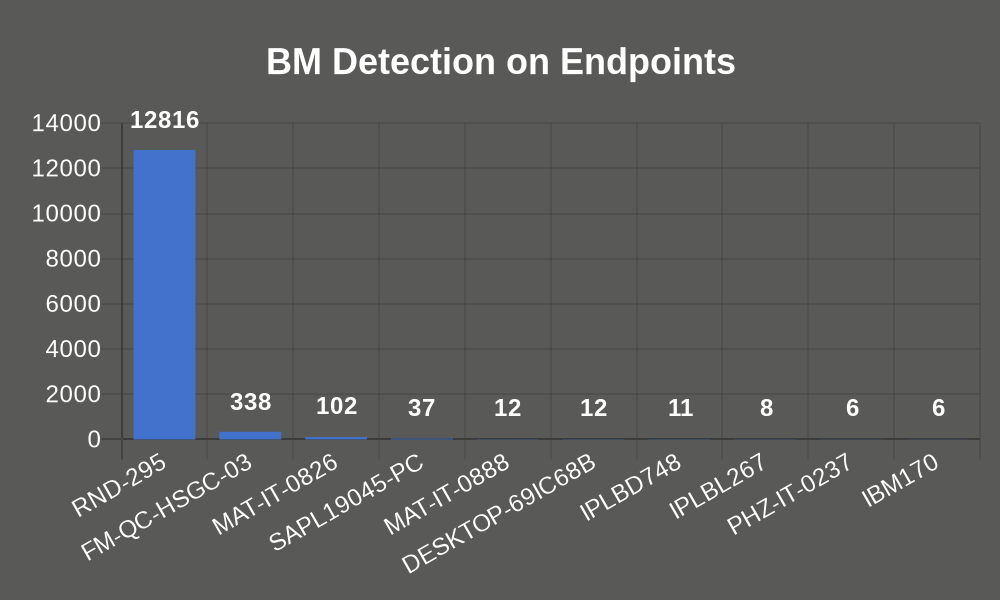
Check below KB in case of Command and Control (C&C) callback detection.

* + <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.

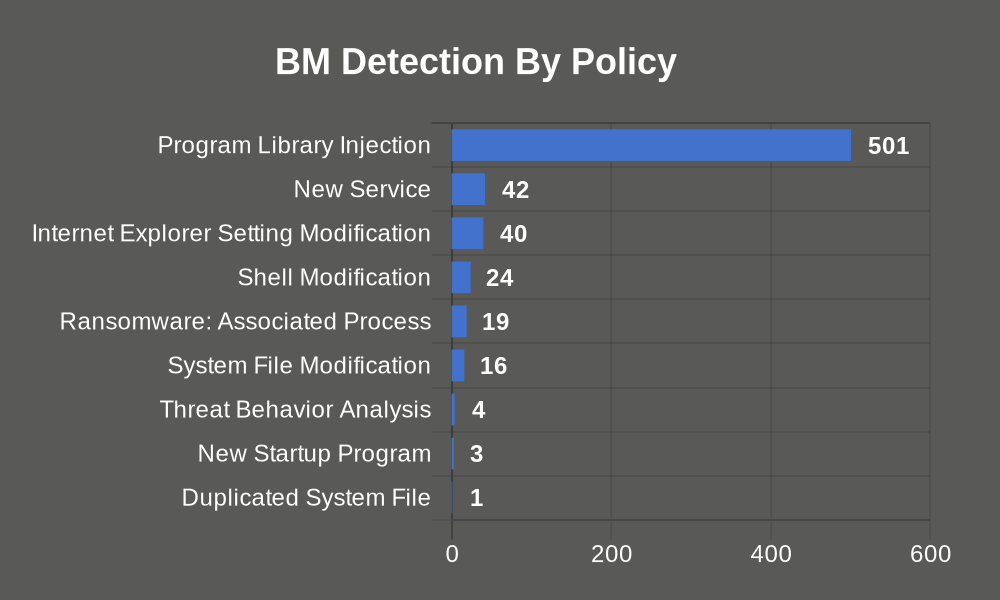
## 5.8 Behavior Monitoring

We generated a Behavior Monitoring Event of the last 30 Days on 10th Oct 2023 from Apex Central/Apex One. There was a total of 13463 detections.



On the endpoint, RND-295 Behavior Monitoring was triggered 12816 times with Low Severity. Processes were denied by Apex One.

On the endpoint, FM-QC-HSGC-03 Behavior Monitoring was triggered 338 times with Low Severity. Processes were denied by Apex One.



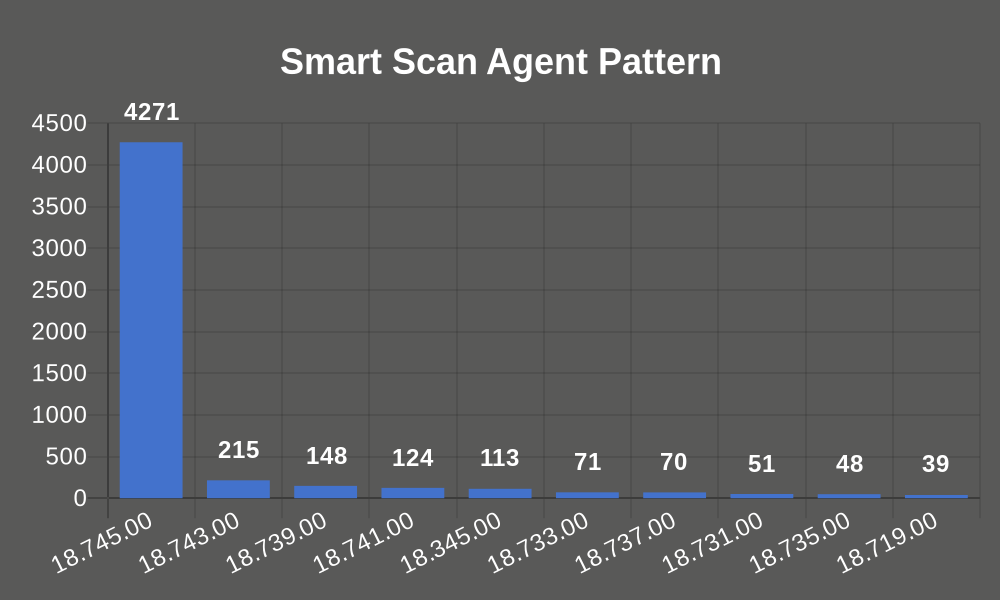
501 times Program Library Injection was triggered on MAT-IT-0219, FM-QC-HSGC-03, RND-295, DELL096, and MAT-IT-0826 endpoints, and it was denied by Apex One.

42 times New Service was triggered on MAT-IT-1608, MAT-IT-1614, MAT-IT-0888, MAT-IT-1355, and MAT-IT-1624 endpoints, and it was assessed by Apex One.

|  |  |  |  |
| --- | --- | --- | --- |
| **BM BY POLICY & RISK LEVEL** | **ACTION** | | |
| **Deny** | **Assess** | **Terminate** |
| **Program Library Injection** | **501** |  |  |
| Low |  |  |  |
| **New Service** |  | **42** |  |
| Low |  |  |  |
| **Internet Explorer Setting Modification** | **40** |  |  |
| High |  |  |  |
| **Shell Modification** | **24** |  |  |
| Low |  |  |  |
| **Ransomware: Associated Process** | **19** |  |  |
| High |  |  |  |
| **System File Modification** | **16** |  |  |
| High |  |  |  |
| **Threat Behavior Analysis** |  |  | **4** |
| High |  |  |  |
| **New Startup Program** | **1** | **2** |  |
| Low |  |  |  |
| **Duplicated System File** |  | **1** |  |
| Low |  |  |  |
| **Total** | **601** | **45** | **4** |

## 5.9 Smart Scan Agent Pattern Coverage Details

|  |  |
| --- | --- |
| Last 7 days Pattern updated agents | 4947 |
| Older than 7 Days Pattern updated agents | 1000 |
| Total Agents | 5947 |



# 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)