
TREND MICRO
Vision One
Endpoint Security

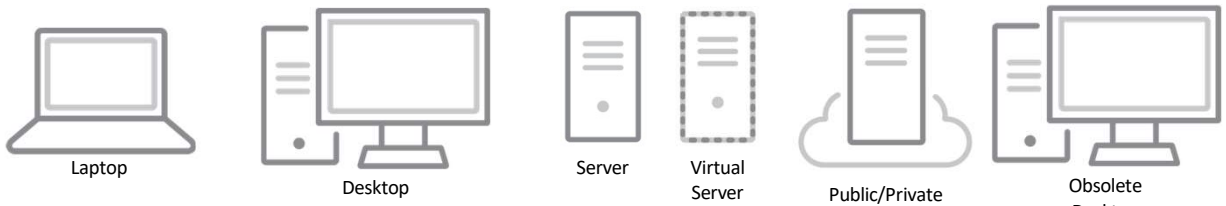
# V1 Endpoint Security - Review

# Server Workloads & User Endpoints Enfrentando Diferentes Amenazas

**Según Gartner1, "Un endpoint de usuario final está expuesto regularmente a amenazas a través de correo electrónico, sitios web, servicios en la nube o unidades USB.**

**Por el contrario, los actores de amenazas se dirigen a las cargas de trabajo de los servidores mediante vulnerabilidades de software y configuración, movimiento lateral y credenciales de empleados robadas.**

**Estas diferencias en la exposición a amenazas crean la necesidad de requisitos de seguridad distintos y estrategias de protección para los puntos finales de los usuarios finales y las cargas de trabajo de los servidores".**




*1. Gartner, Prioritizing Security Controls for Enterprise Servers and End-User Endpoints (Evgeny Mirolyubov, Peter Firstbrook, January 2023)*

# ¿Por qué "Vision One - Endpoint Security"?



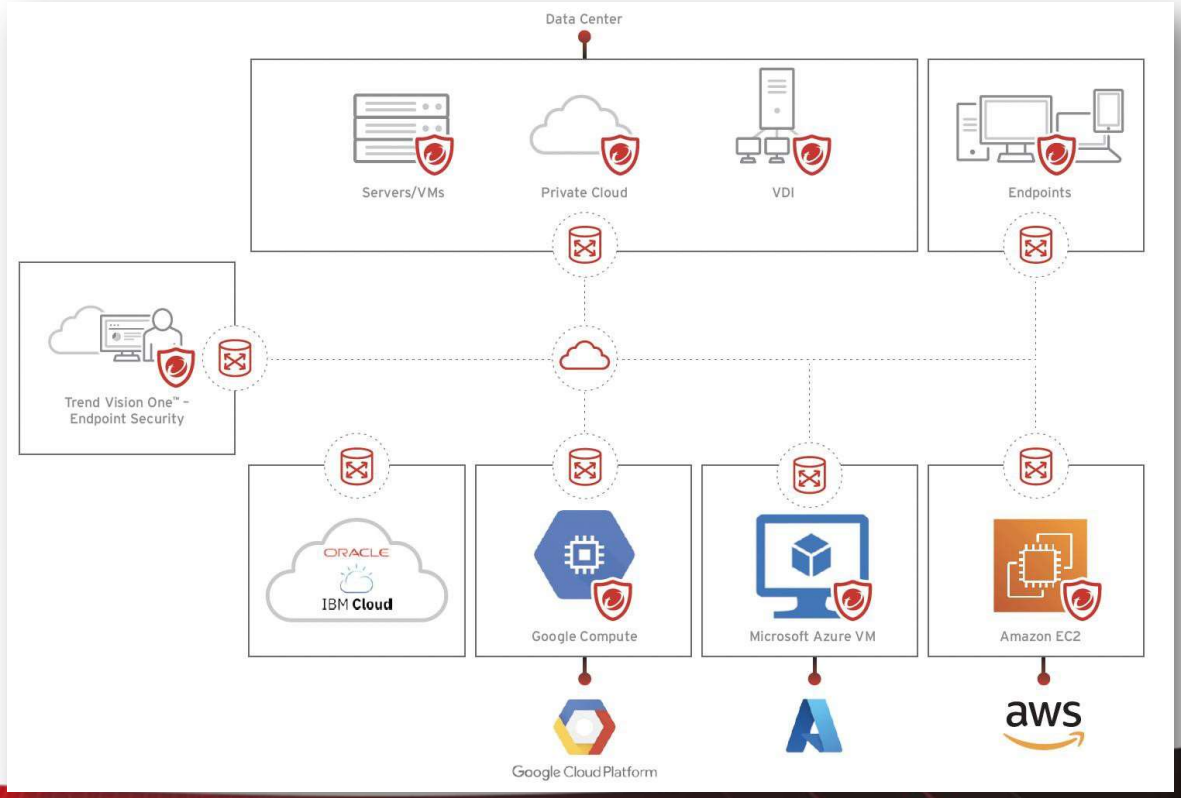

Seguridad especialmente diseñada para endpoints, Workload (servidores)  y en la nube
Centro de datos seguro, nube e híbrido

Consola única para visibilidad y gestión; protección y EDR
Flujo de trabajo conectado de TI/SecOps

Parte de la plataforma Vision One; fácil expansión a otras soluciones de seguridad nativas, XDR y ASRM

# Vision One - Endpoint Security

Obtenga protección oportuna contra una variedad cada vez mayor de amenazas aprovechando los controles de seguridad automatizados y avanzados y la última inteligencia de amenazas líder en la industria. Con una gama completa de capacidades de prevención, detección y respuesta en capas, como la protección moderna contra malware y ransomware, el control de dispositivos, la prevención de intrusiones basada en host, el control de aplicaciones, el aprendizaje automático/IA y más, puede defender sus endpoints, escritorios virtuales, servidores y cargas de trabajo en la nube en tiempo real.



# V1 Endpoint Security – Offering

# Vision One: Endpoint Security Paquetes de suscripción

**Vision One – Endpoint Security**

| | Core | Essentials | Pro | Detection and Response (EDR-XDR Add-on) |
|---|---|---|---|---|
| Primary endpoint type | User endpoints & file server | User endpoints & file server | Critical endpoints including application servers & workloads | |
| Windows, Linux & Mac OS | ✓ | ✓ | ✓ | |
| Antimalware, bahavioral analysis, machine learning, web reputation | ✓ | ✓ | ✓ | |
| Device Control | ✓ | ✓ | ✓ | |
| Data Loss Prevention (DLP) | ✓ | ✓ | | |
| Firewall | ✓ | ✓ | ✓ | |
| Application Control | ✓ | ✓ | ✓ | |
| Intrusion Prevention – IPS (OS) | ✓ | ✓ | ✓ | |
| Virtualization Protection | ✓ | ✓ | ✓ | |
| EDR – XDR | | ✓ | ✓ | ✓ |
| Intrusion Prevention – IPS (Server Applications) | | | ✓ | |
| Integrity Monitoring / Log Inspection | | | ✓ | |

TREND MICRO

# Vision One Endpoint Security - XDR

## 1 Endpoint Security

**License Metric**
Devices

**Packages**
Core, Essentials, Pro

**Credit Price**
Core = 45
Essentials = 65
Pro = 300

**Volume Pricing**
*Lowest tier* starting from:
Core = $47.25
Essentials = $63.00
Pro = $315.00

SAP Scanner for Vision One

Apex One Sandbox as a Service

## 1 XDR for Endpoint

**License Metric**
Per Device

**Packages**
Core:
Essentials & Pro: Included

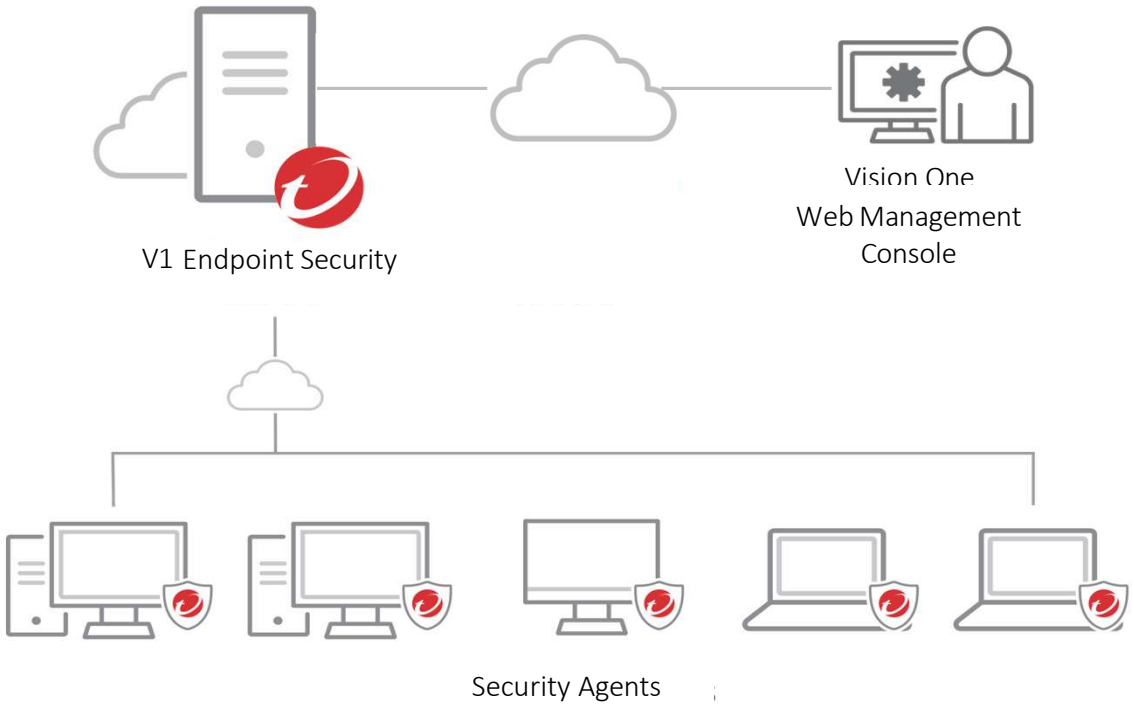
**Credit Price**
20 credits per device

**Volume Pricing**
Yes;
$21 per device

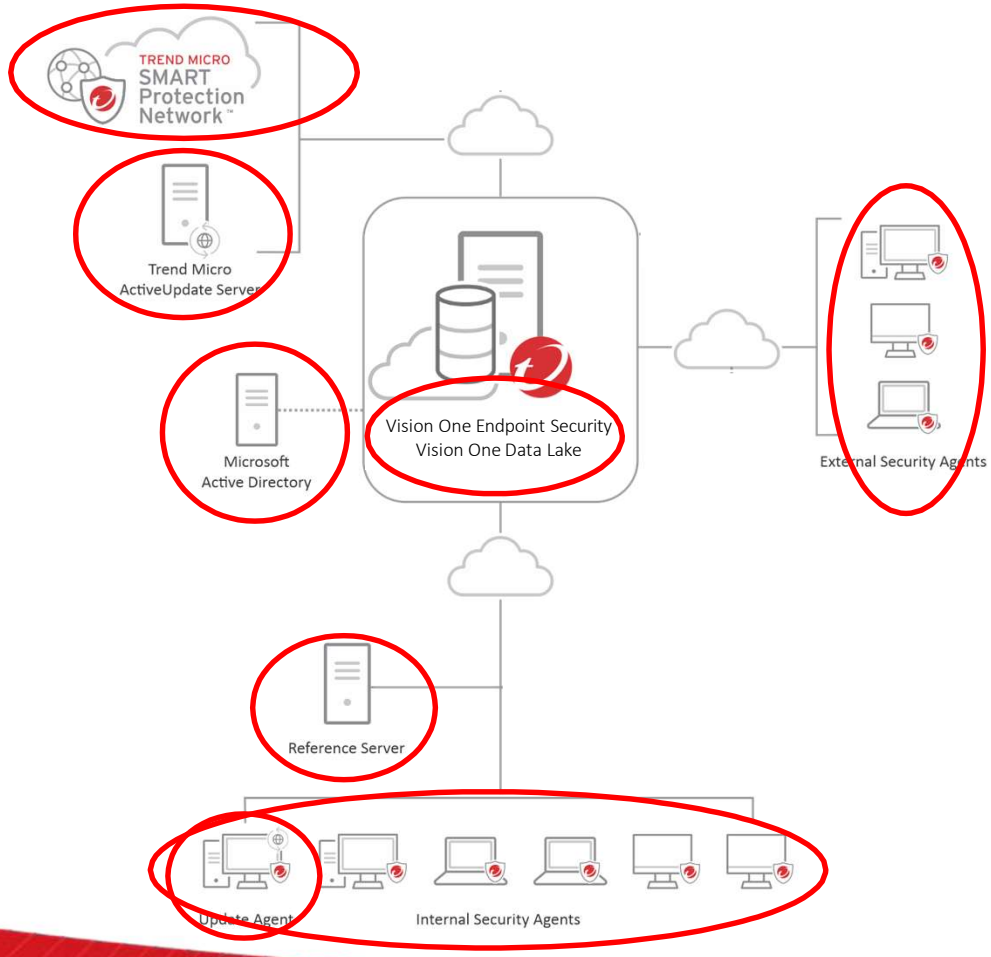
XDR for Endpoints Data Retention

# V1 Endpoint Security - Arquitectura

# High-level arquitectura



# Components




Vision One Endpoint Security: Administra agentes de seguridad en endpoints de Windows, Mac y Linux.

Vision One Data Lake: repositorio basado en la nube para datos de telemetría XDR
Vision One: Amplía las capacidades de XDR
Agentes de seguridad (internos): refuerza la protección en los equipos de punto final Windows, Mac y Linux dentro de la red
Agentes de seguridad (externos): refuerza la protección en Windows, Mac y
Equipos de punto final Linux fuera de la red

Servidor de referencia: Permite a los agentes determinar si son internos o externos a la red

Trend Micro Smart Protection Network: repositorio basado en la nube de
Información y servicios sobre amenazas
Trend Micro ActiveUpdate Server: Fuente de descarga predeterminada para
Archivos de patrones y actualizaciones de programas
Agente de actualización: Agente promocionado que sirve como descarga alternativa
origen de los archivos de patrones y las actualizaciones del agente
Microsoft Active Directory (opcional): proporciona autenticación mejorada para usuarios administrativos, asignación de puntos de conexión y líneas de informes

# V1 Endpoint Security - Requirements

# Requisitos previos de implementación de Security Agent

- Verificar que:
- Los agentes de los endpoints pueden comunicarse con Vision One Endpoint Security
- Los puntos de conexión pueden acceder a *.trendmicro.com
- Si es necesario, configure los ajustes del servidor proxy del agente
- Tener Privilegios de nivel administrativo para instalar software
- No hay claves de registro actualmente en el computador de alguna instalación anterior
- Las aplicaciones antivirus existentes deben ser extraíbles – que se permitan desinstalar. Preferiblemente que previamente se desinstale.



# Excepciones del cortafuegos:Americas - Todas las excepciones

- <Apex One console_DNS>.manage.trendmicro.com
- (refer to license email)
- licenseupdate.trendmicro.com
- asm01-nabu-prod.aot.trendmicro.com
- api-nabu.aot.trendmicro.com
- osce14-p.activeupdate.trendmicro.com
- tmsm35-p.activeupdate.trendmicro.com
- osce14.icrc.trendmicro.com
- osce14-0-en.url.trendmicro.com
- osce140-en.fbs25.trendmicro.com
- osce14-en.gfrbridge.trendmicro.com
- osce14-en-census.trendmicro.com
- osce140-en-f.trx.trendmicro.com
- mcs.trendmicro.com
- oscecmp140-en-f.trx.trendmicro.com
- osce140-en-b.trx.trendmicro.com
- osce14bak-en-census.trendmicro.com
- www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/

**Important:**
If you enable endpoint sensor detection and response, you must also add the **Endpoint Sensor Agents** exceptions.

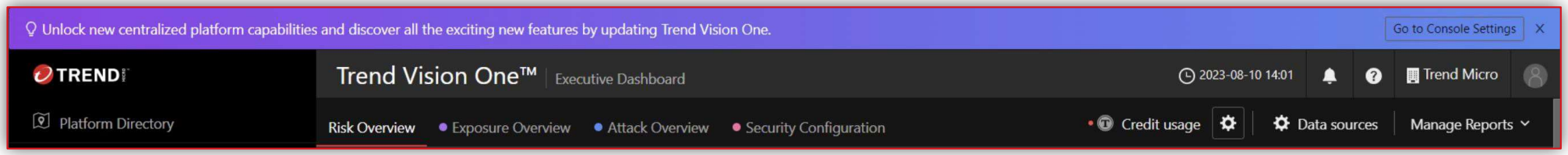
- assessment-us1.mgcp.trendmicro.com
- release-us1.mgcp.trendmicro.com
- cti-us1.mgcp.trendmicro.com
- api-us1.xbc.trendmicro.com
- wsc-us1.xbc.trendmicro.com
- tgw-us1.mgcp.trendmicro.com
- support-connector-api.manage.trendmicro.com
- supportconnectorpacks.manage.trendmicro.com
- rpcollectedthings.manage.trendmicro.com
- cloudendpoint-us1.mgcp.trendmicro.com
- er-ws-ue1.xdr.trendmicro.com
- era-ue1.xdr.trendmicro.com
- endpointpolicy-cdn-us1.xbc.trendmicro.com
- files.trendmicro.com
- xlogr-ue1.xdr.trendmicro.com
- api.xdr.trendmicro.com
- api-cert.xdr.trendmicro.com
- upload.xdr.trendmicro.com

*Fuente: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-firewallexceptionsam_001#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-ia3nqu*

# V1 Endpoint Security - Despliegue

# Aprovisionamiento de instancias: clientes existentes

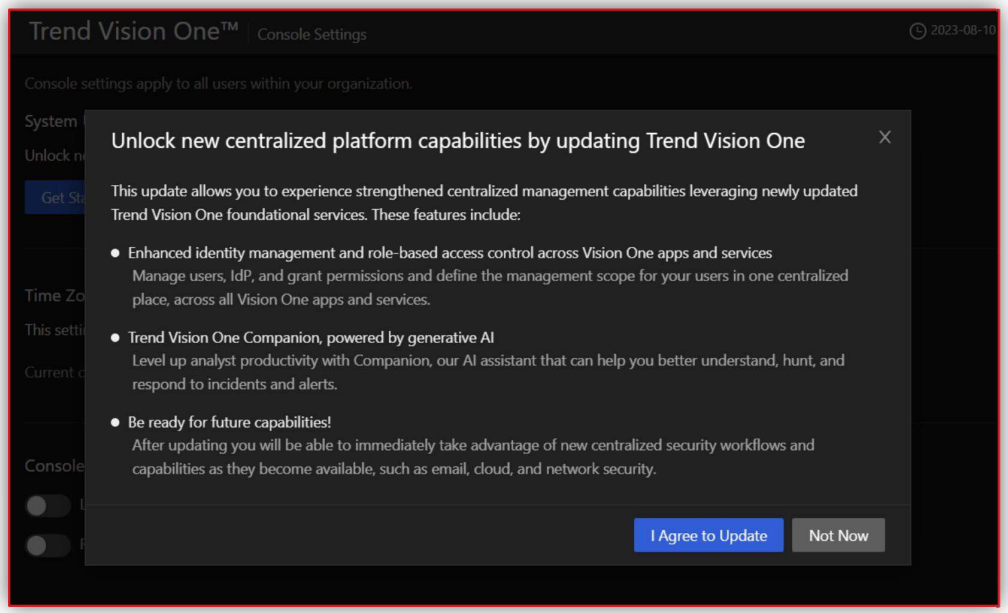
Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.



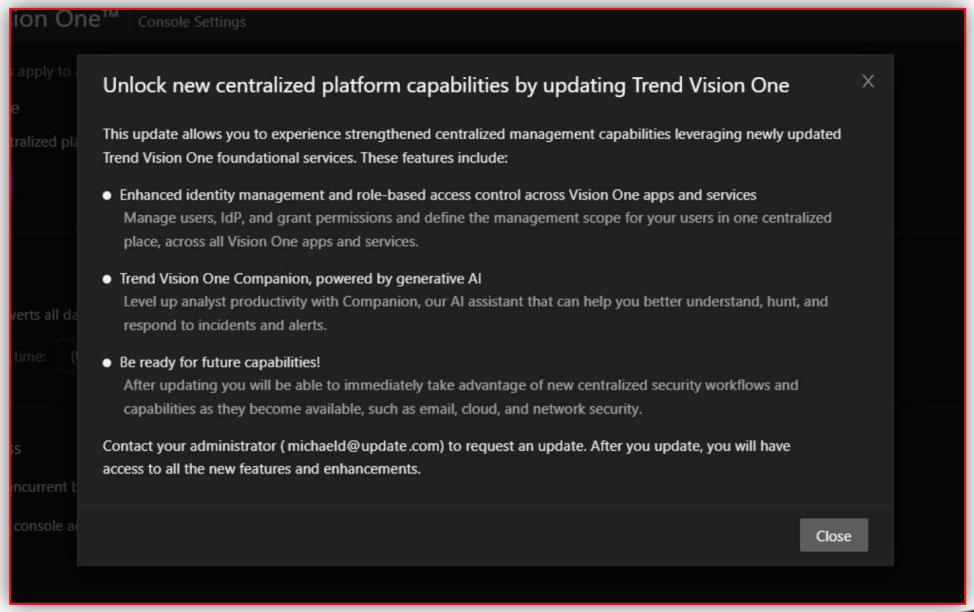
# Instance Provisioning – Existing customers

Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.

Only the **root user has the ability** to initiate the update to Trend Vision One.



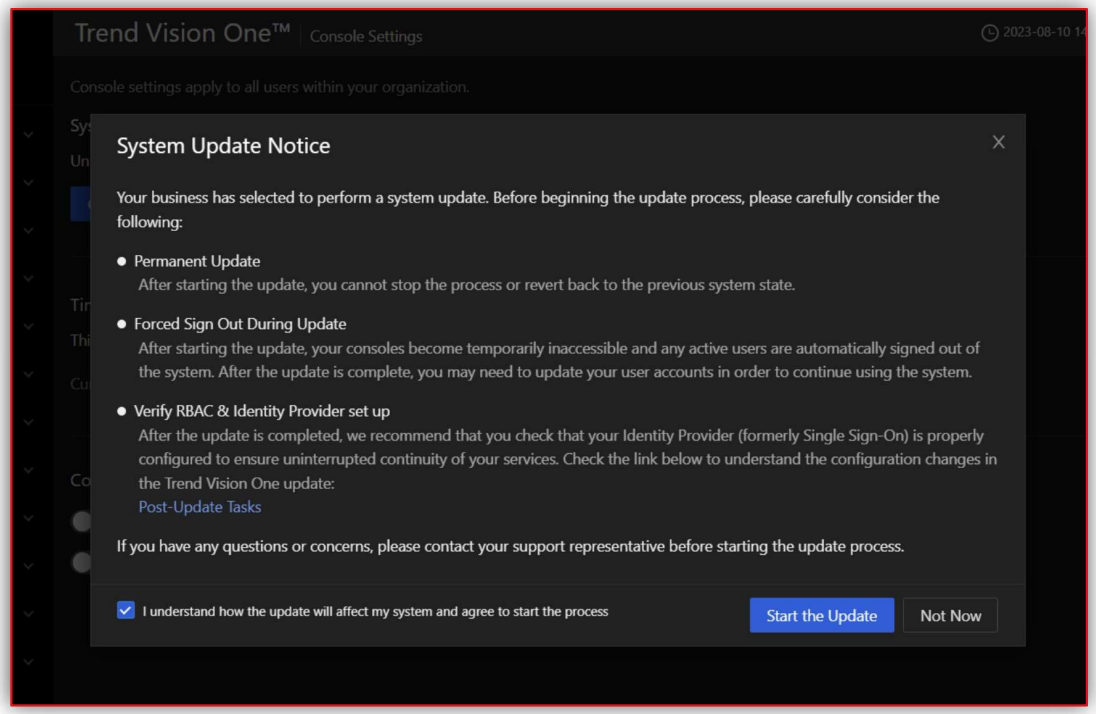

All other **non-root Master Administrators** are presented with a similar information window, but theirs contains a message to contact the root user to initiate the update.



# Instance Provisioning – Existing customers

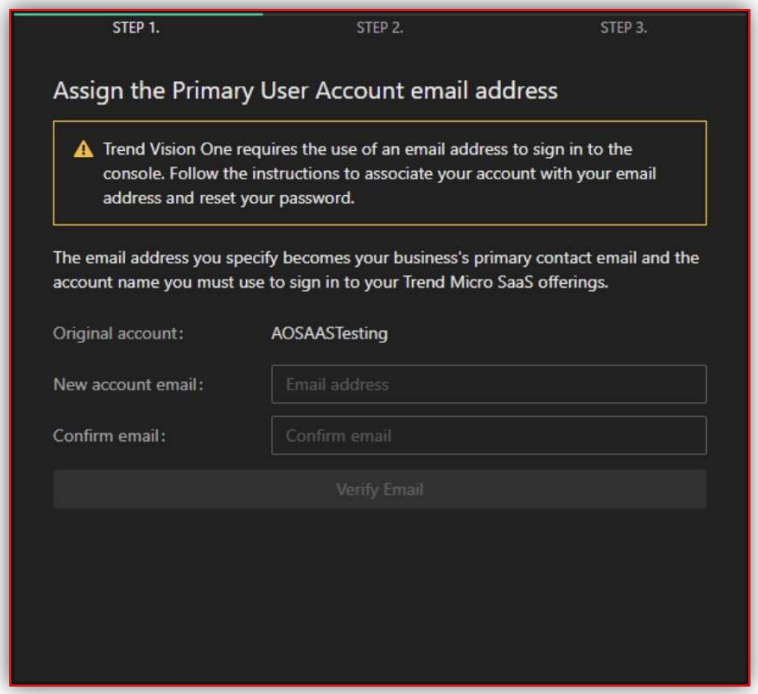
Customers who already have Trend Micro endpoint security products, such as Apex One as a Service, **already connected to Trend Vision One** will require an update to take advantage of the new feature in Trend Vision One, **including Endpoint Security. No changes or updates to installed security agents are required.**

A **System Update Notice** is displayed for the root user with some considerations regarding the update.

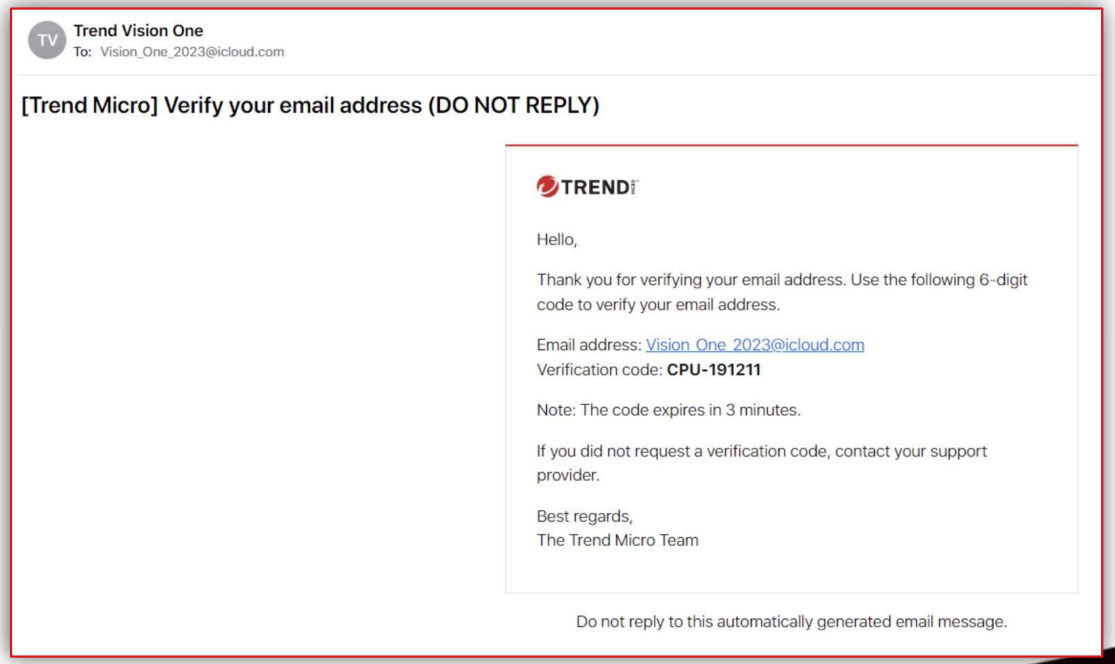


# Instance Provisioning – Existing customers

Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.



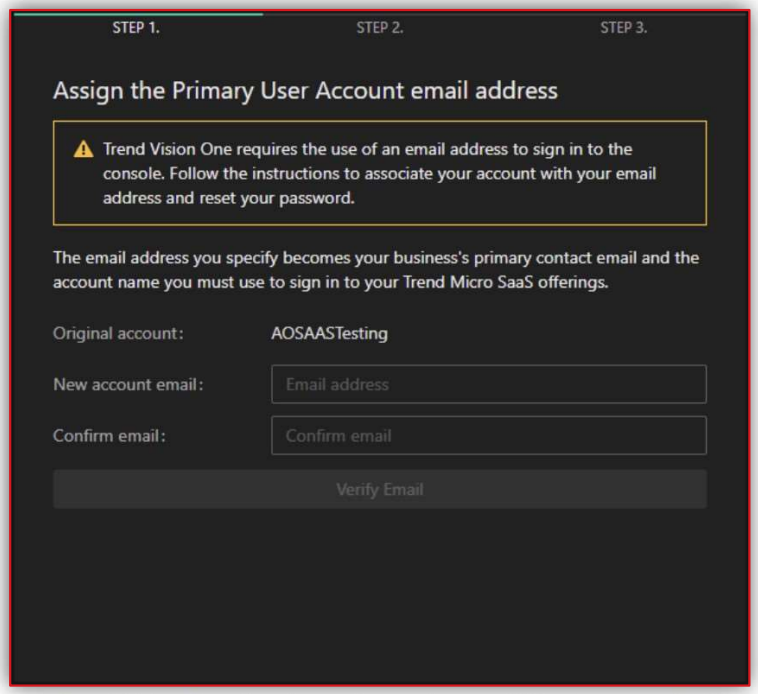


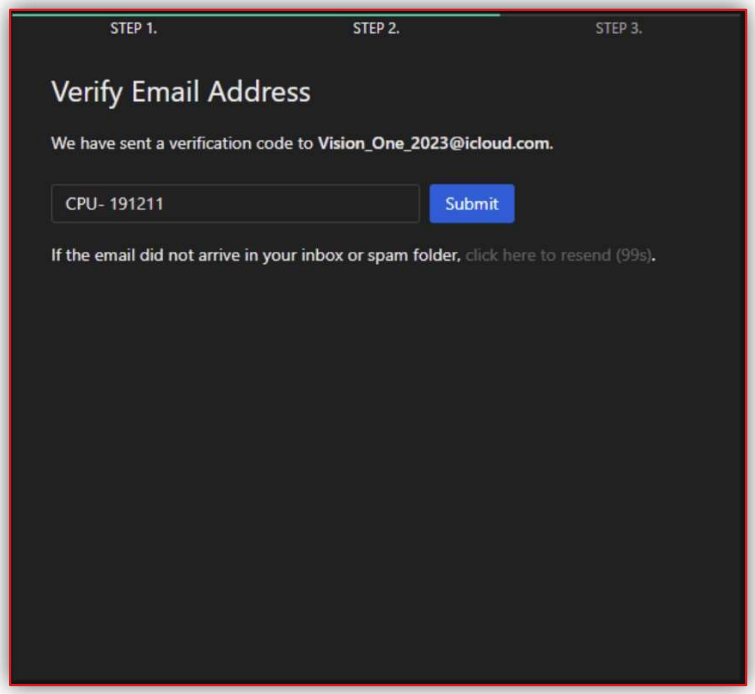

Identities in Trend Vision One after the update to the new IAM rely on email addresses instead of usernames. As part of the update, the user is prompted to enter an email address for the primary user account.

# Instance Provisioning – Existing customers

Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.



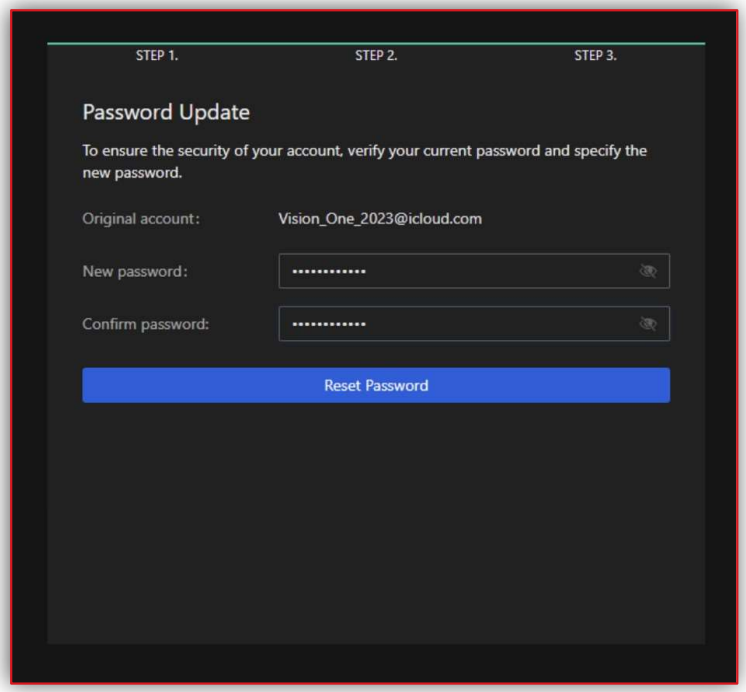

Identities in Trend Vision One after the update to the new IAM rely on email addresses instead of usernames. As part of the update, the user is prompted to enter an email address for the primary user account.

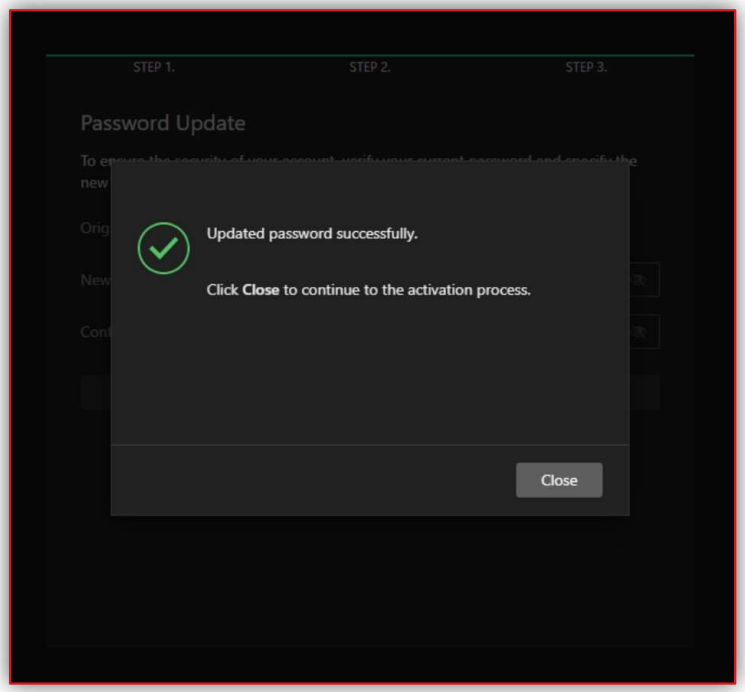



On the Verify Email Address tab, type the code listed in the email and click Submit

# Instance Provisioning – Existing customers

Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.

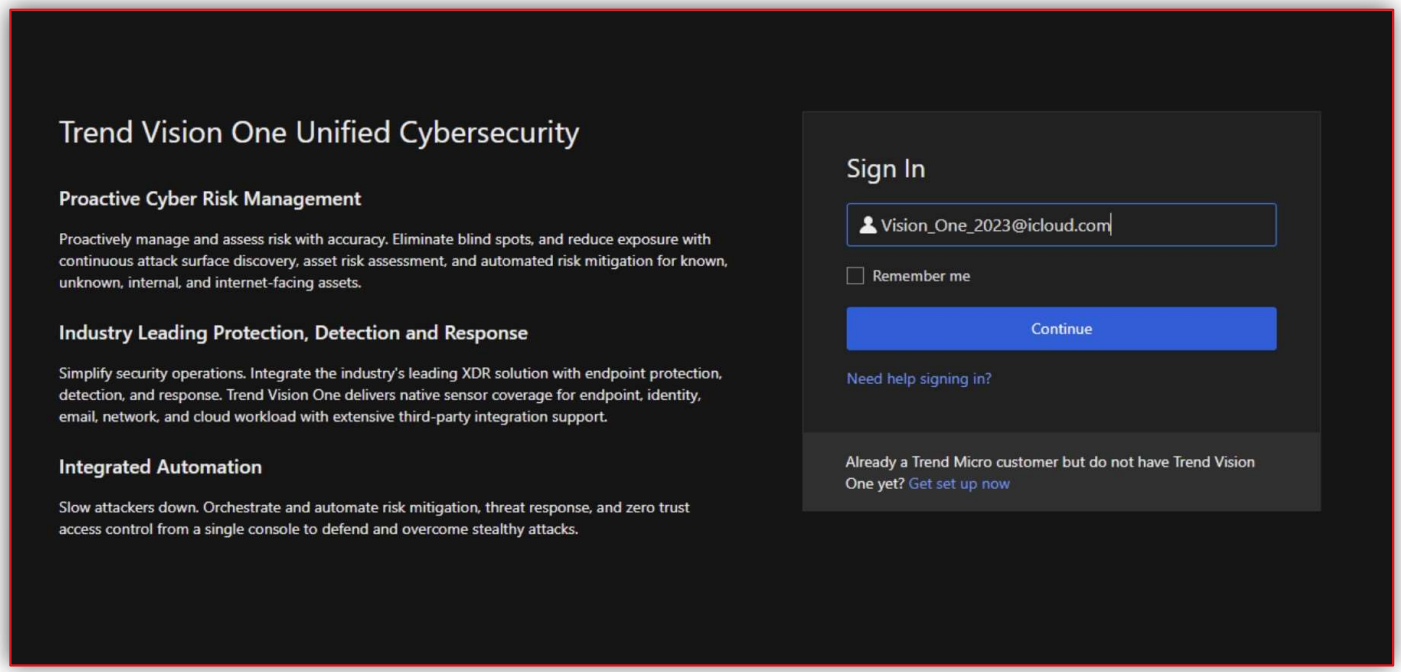



A new password for the account must be provided. Enter and confirm a new password and click **Reset Password**

# Instance Provisioning – Existing customers

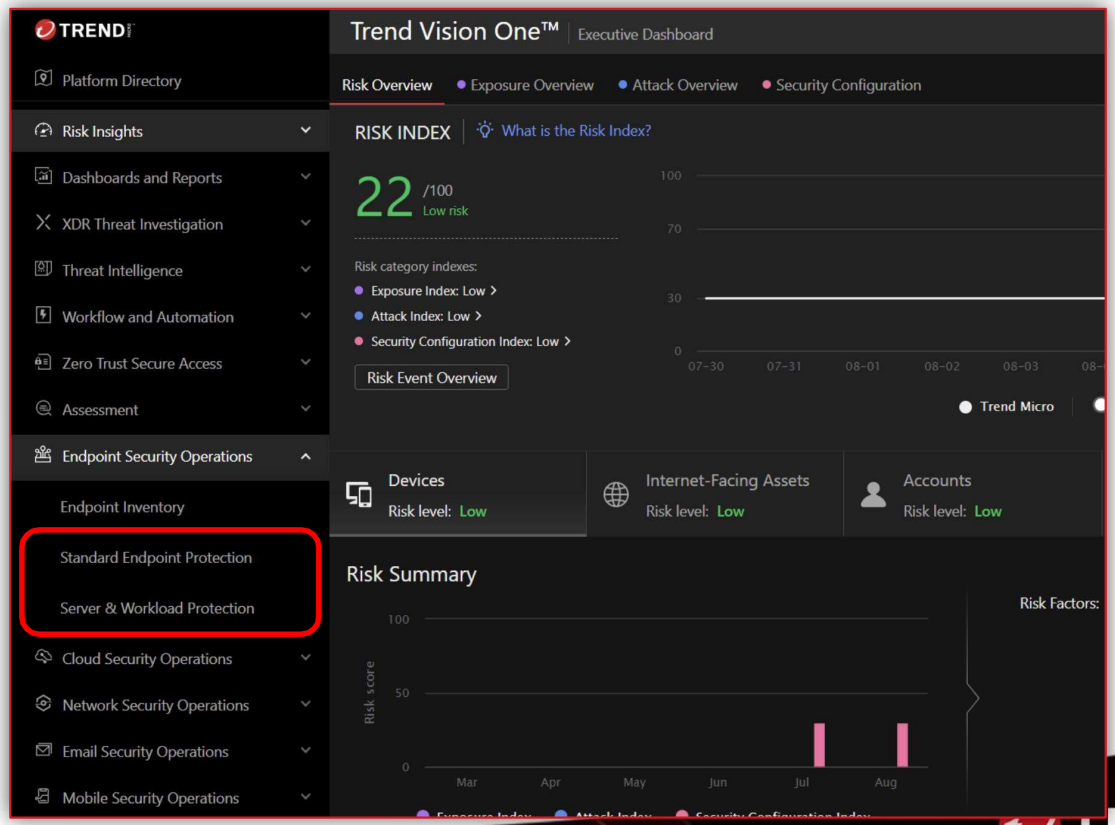
Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.



# Instance Provisioning – Existing customers

Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.

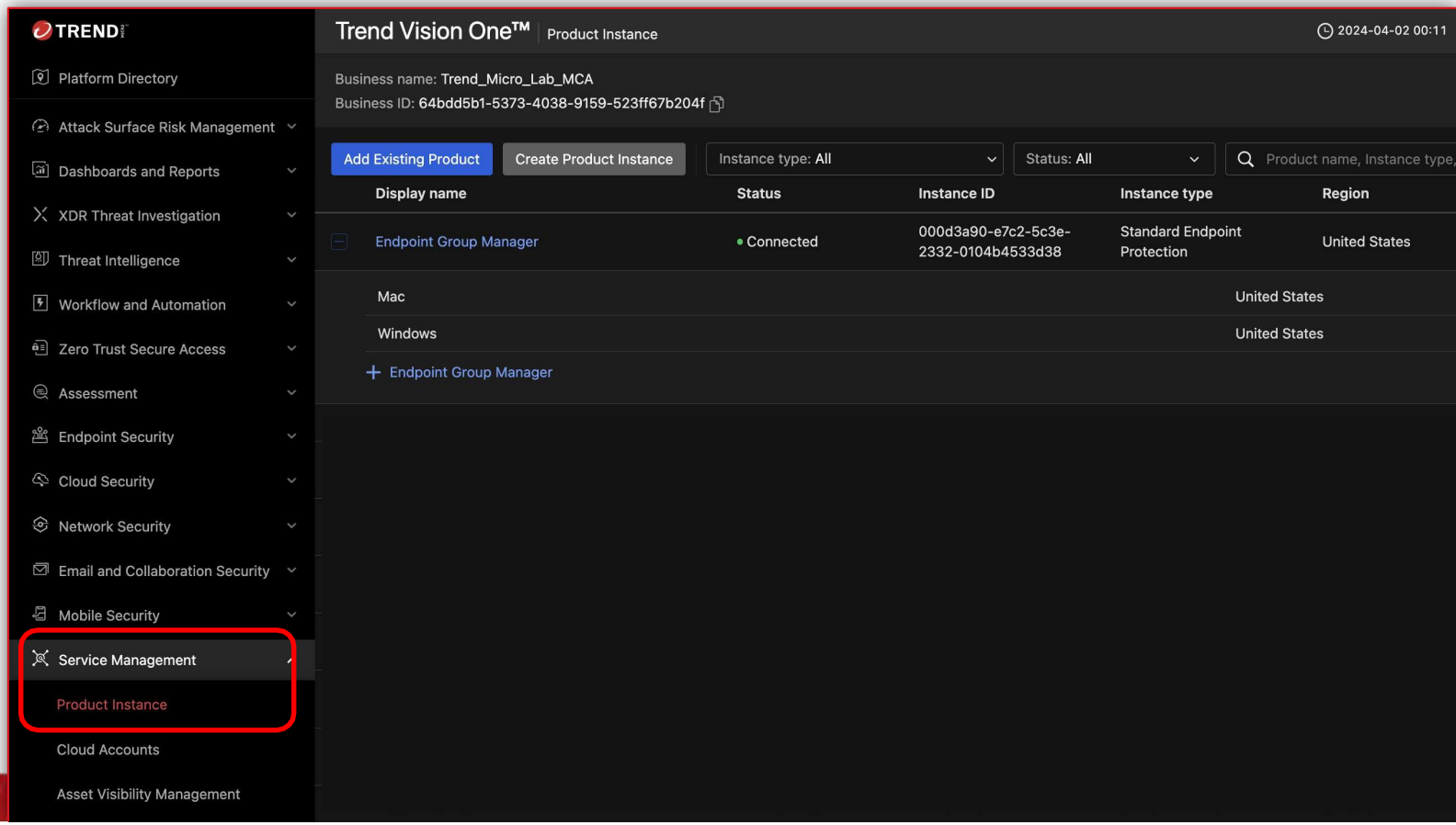
Observará las nuevas aplicaciones Standard Endpoint Protection y Server & Workload Protection en el menú Operaciones de Endpoint Security.



# Instance Provisioning – Existing customers

Los clientes que ya tienen productos de seguridad para endpoints de Trend Micro, como Apex One as a Service, ya conectados a Trend Vision One necesitarán una actualización para aprovechar la nueva función de Trend Vision One, incluida Endpoint Security. No se requieren cambios ni actualizaciones en los agentes de seguridad instalados.

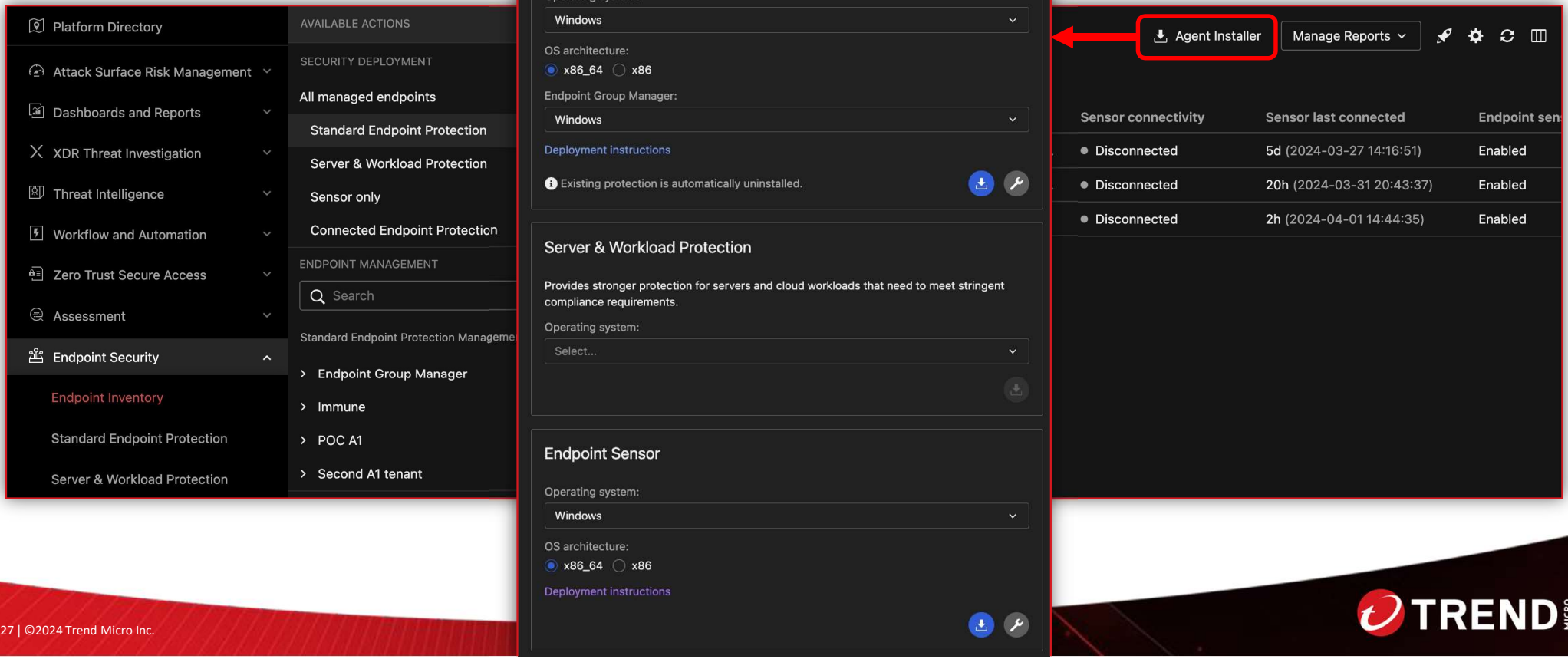
Expanda la categoría Gestión de servicios y haga clic en el botón Producto Aplicación de instancia. Verá la instancia de Apex One as a Service que está conectada a Trend Vision One.



# Agent Deployment

Se puede descargar un paquete de instalación de a d Endpoint Protection, Servidores y Carga de trabajo

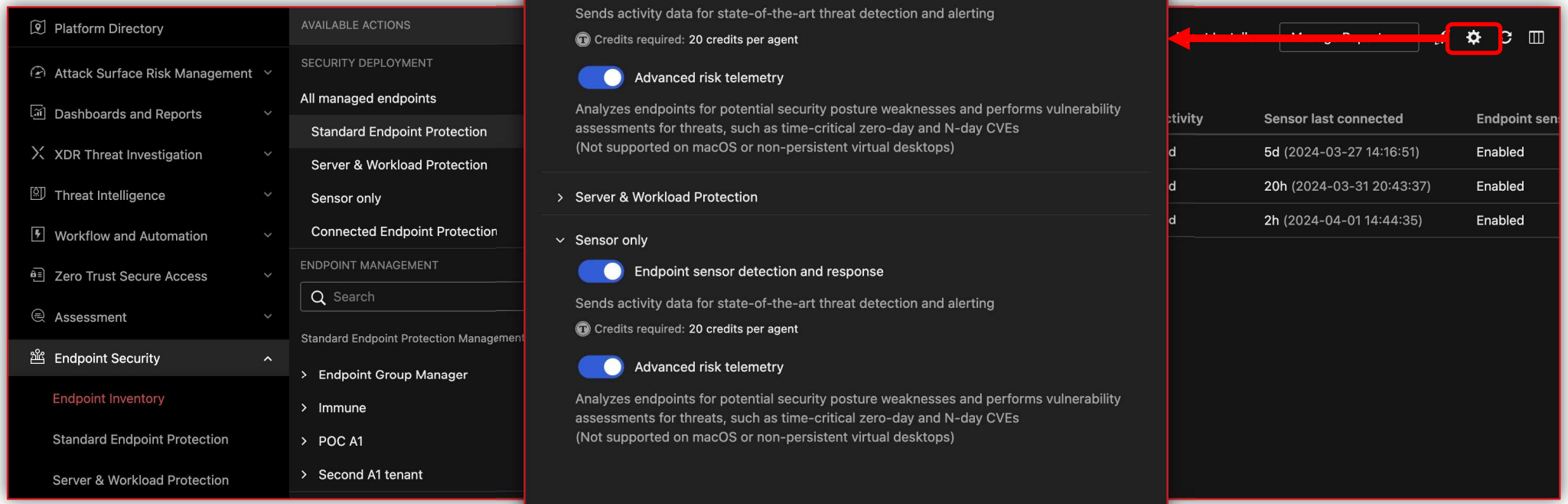
Protección, o solo un sensor de punto final. Se desc do y ejecute el archivo EndpointBasecamp.exe.



# Agent Deployment -

Se pueden definir configuraciones de políticas de senso ndar o solo para un sensor. Los puntos finales con un sensor instalado

heredan automáticamente la configuración definida aq



# Deploying Agents with a Software Management System

Use un sistema de administración de software, como Microsoft Intune, para implementar el instalador del agente en los puntos de conexión administrados.

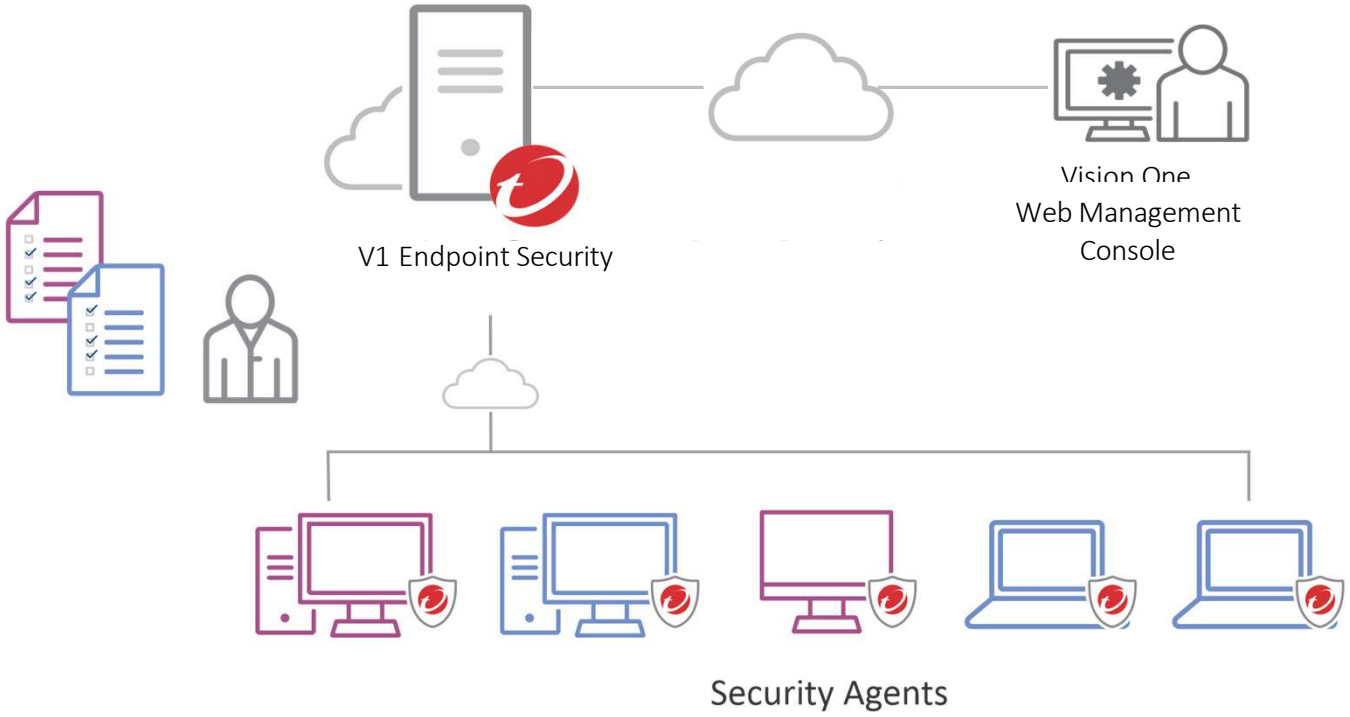
Puede utilizar un sistema de administración de software para implementar el instalador del agente en todo su entorno, lo que facilita aún más la implementación y la instalación. La implementación de agentes de Trend Vision One Endpoint Security está probada y es compatible con los siguientes métodos de implementación:

**Microsoft Intune**

**Microsoft Endpoint Configuration Manager (anteriormente System Center Configuration Manager)**

**Objeto de directiva de grupo (GPO) de Microsoft Active Directory**

# Implementación de políticas



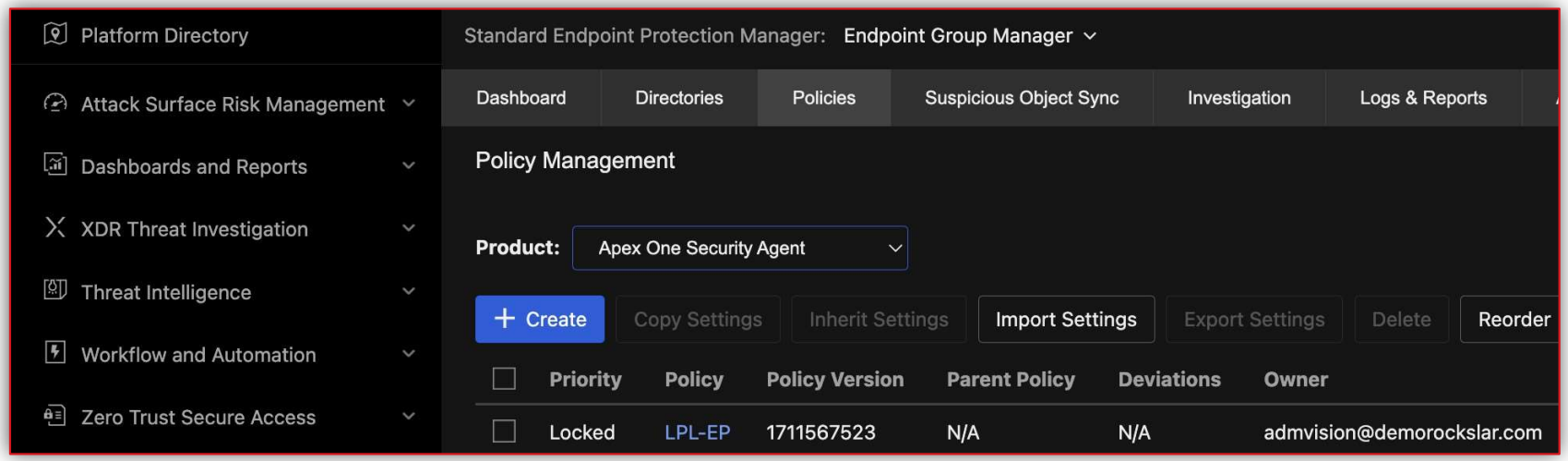
# Policy Management

Select product

Select targets

Define settings

Deploy



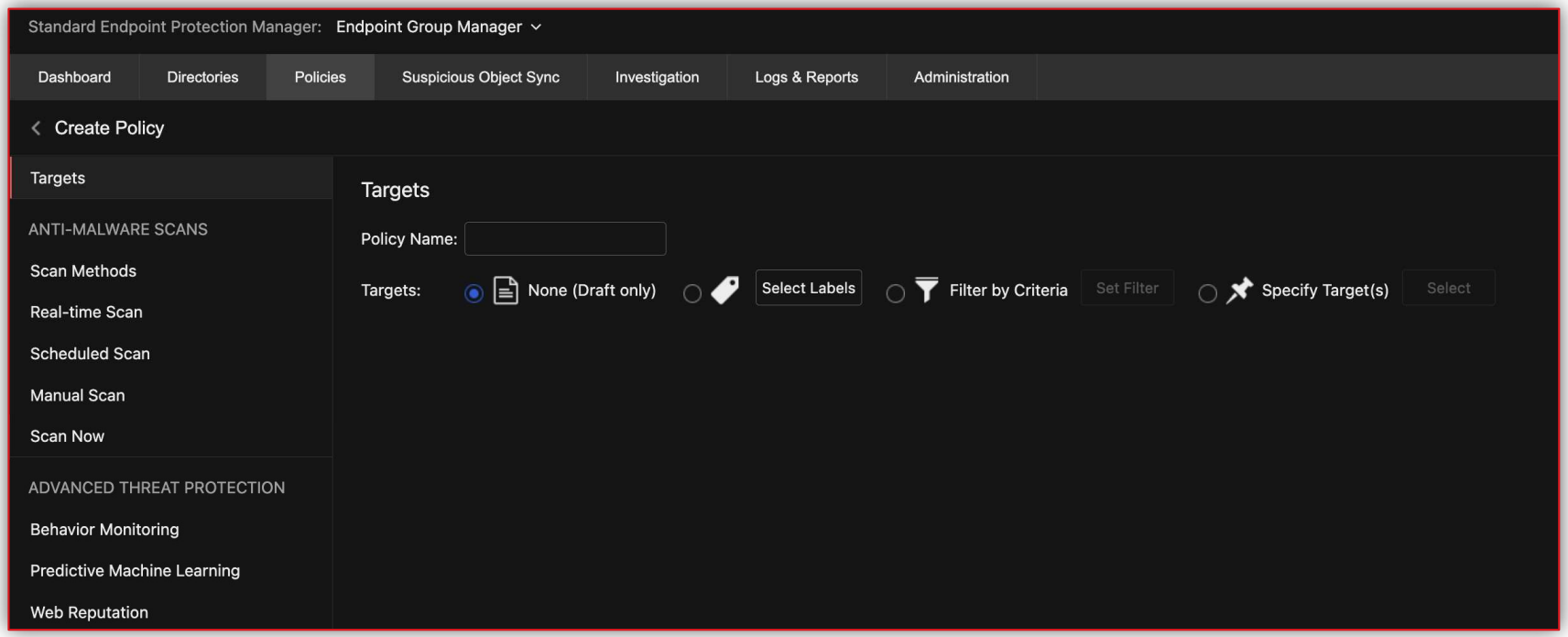
# Policy Management

Select product

Select targets

Define settings

Deploy



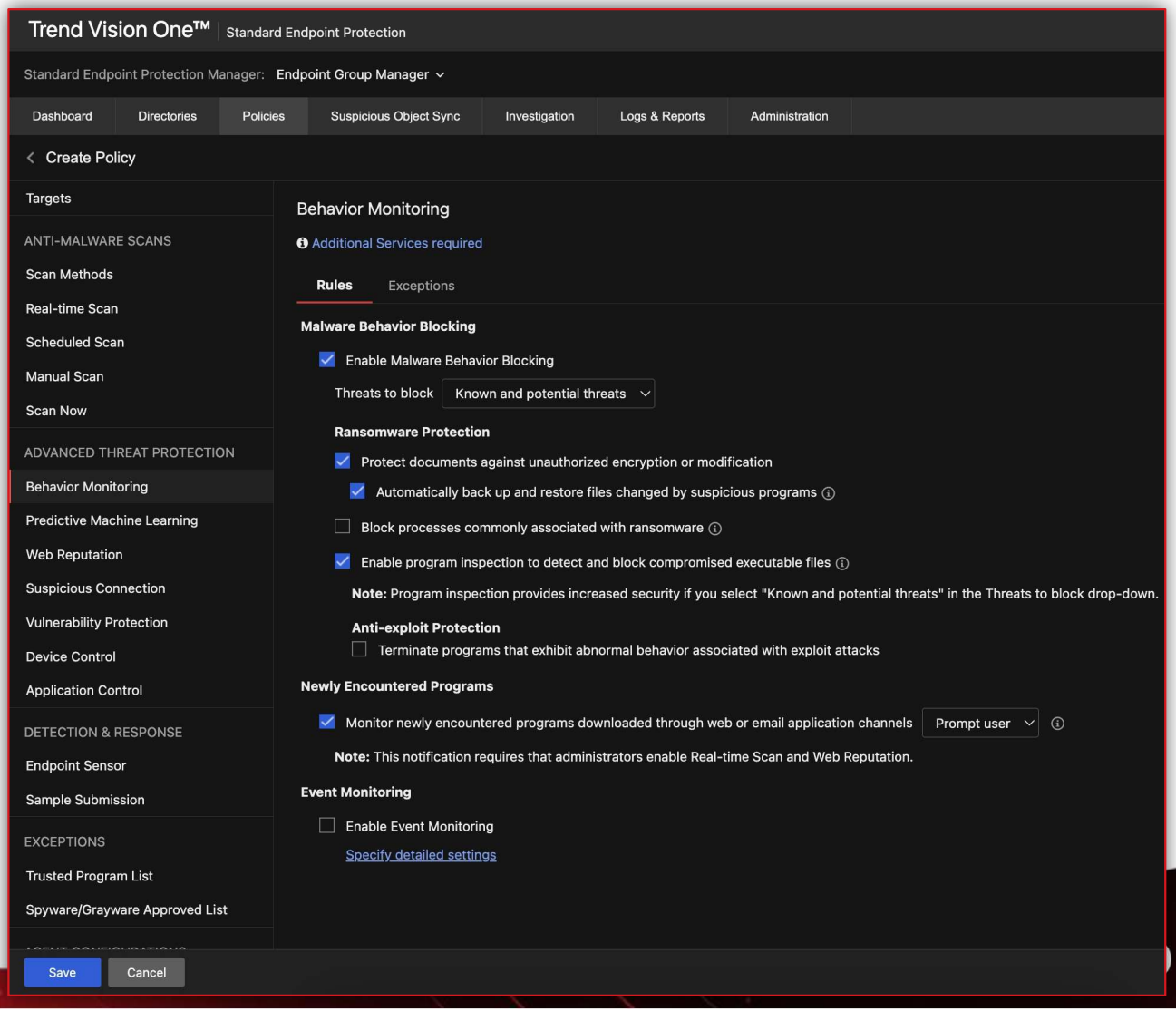
# Policy Management

Select product

Select targets

Define settings

Deploy



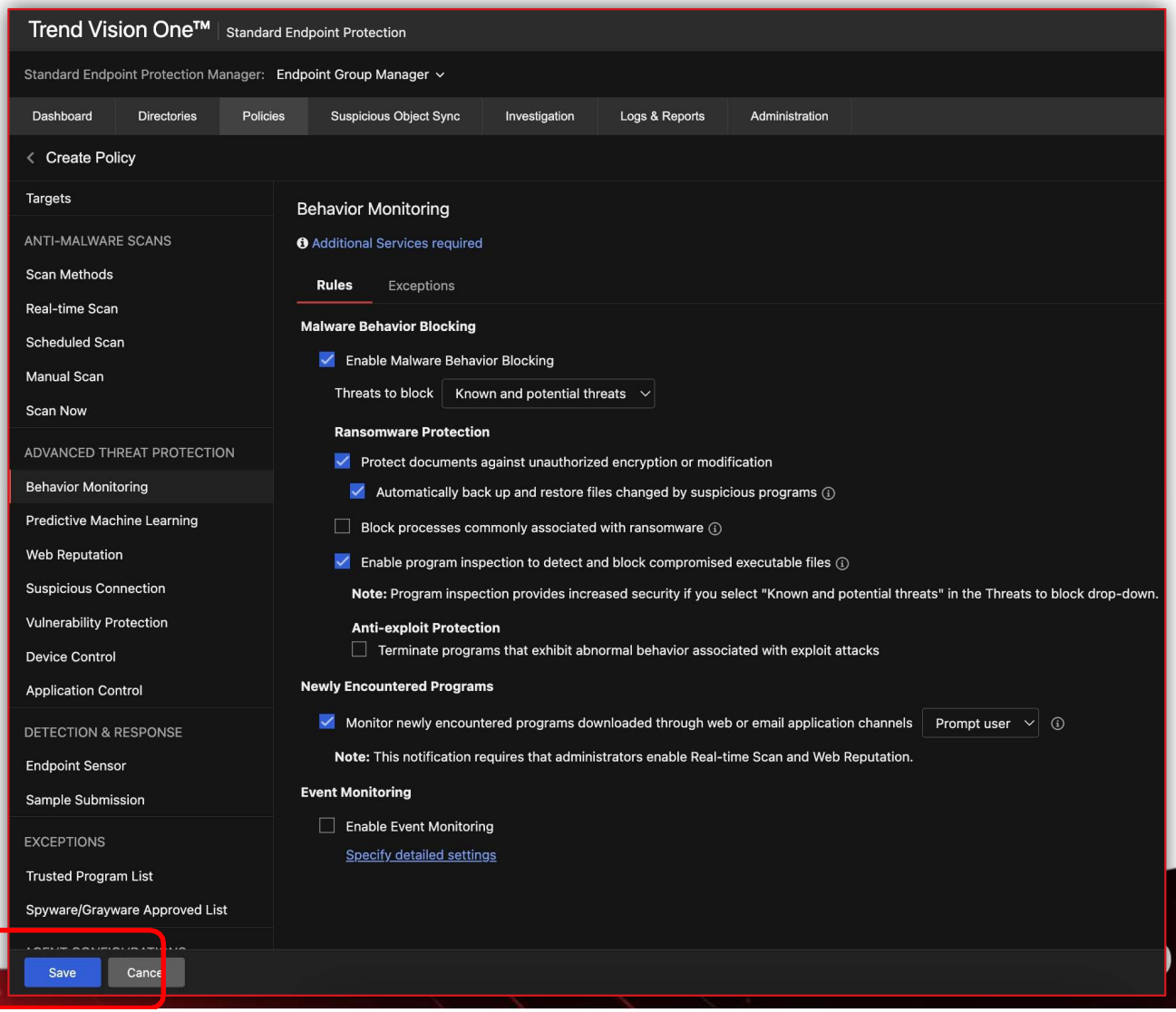
# Policy Management

Select product

Select targets

Define settings

Deploy



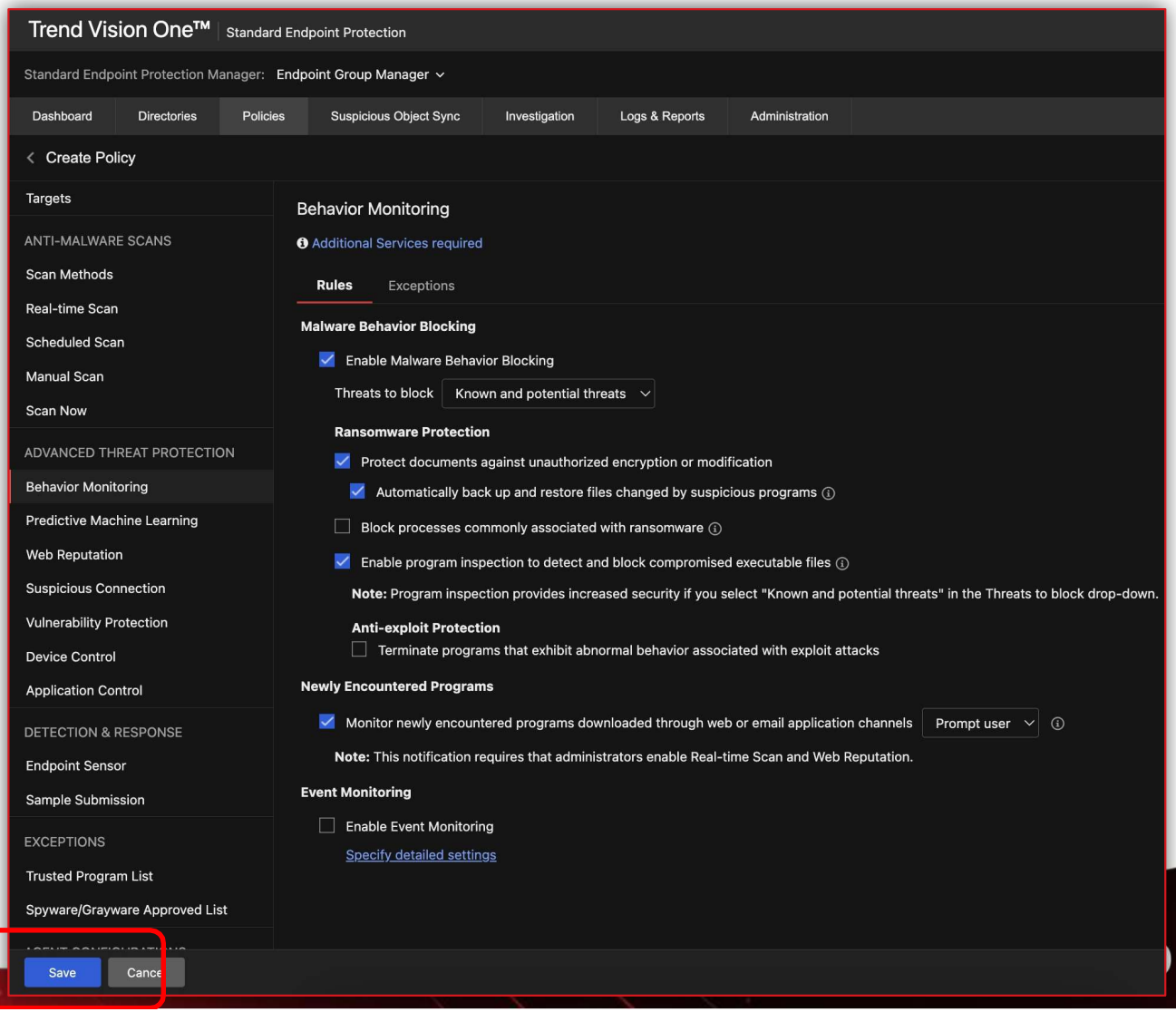
# Policy Management

Select product

Select targets

Define settings

Deploy

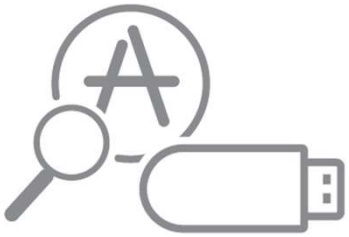


# V1 Endpoint Security - Integration

# Active Directory Integration



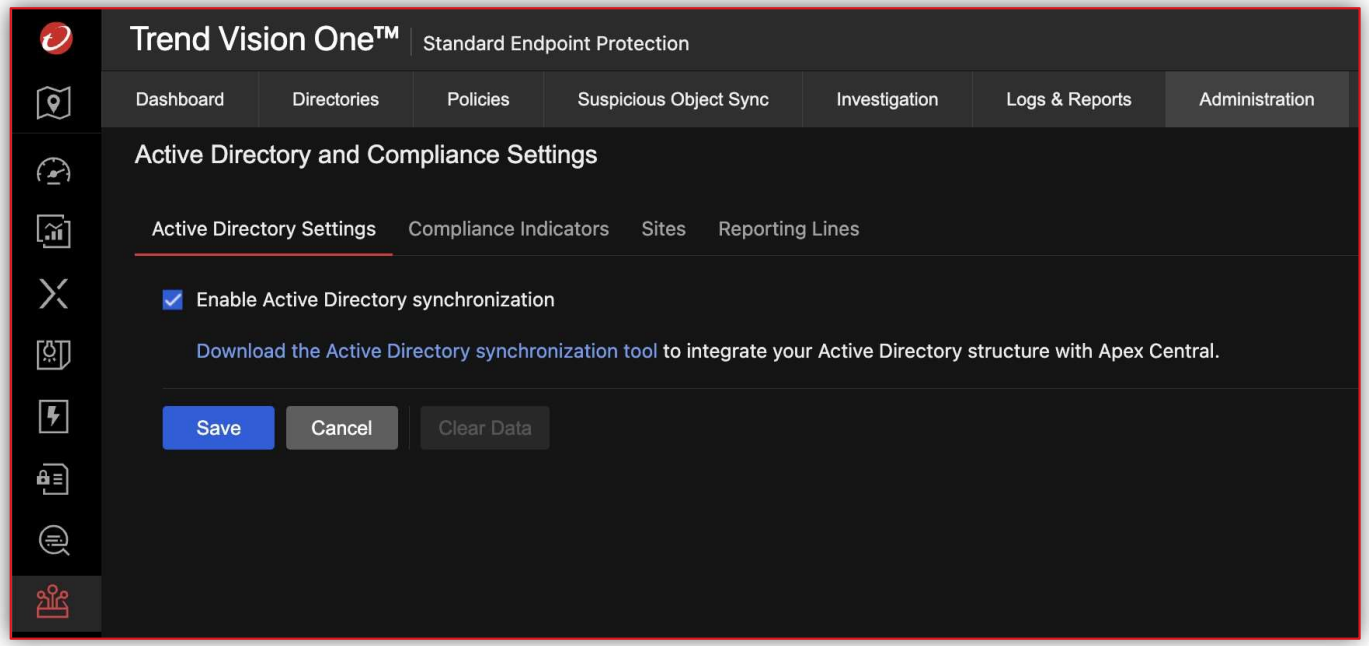
- Asigna el directorio de usuarios/terminales de acuerdo con su estructura organizativa existente e integra la información de los puntos finales (como las detecciones de amenazas y los estados de las políticas) con la información de usuario de Active Directory (como el historial de inicio de sesión y los datos de contacto).



- Cree reglas de control de aplicaciones basadas en usuarios y reglas de control de dispositivos basadas en usuarios y grupos de Active Directory.

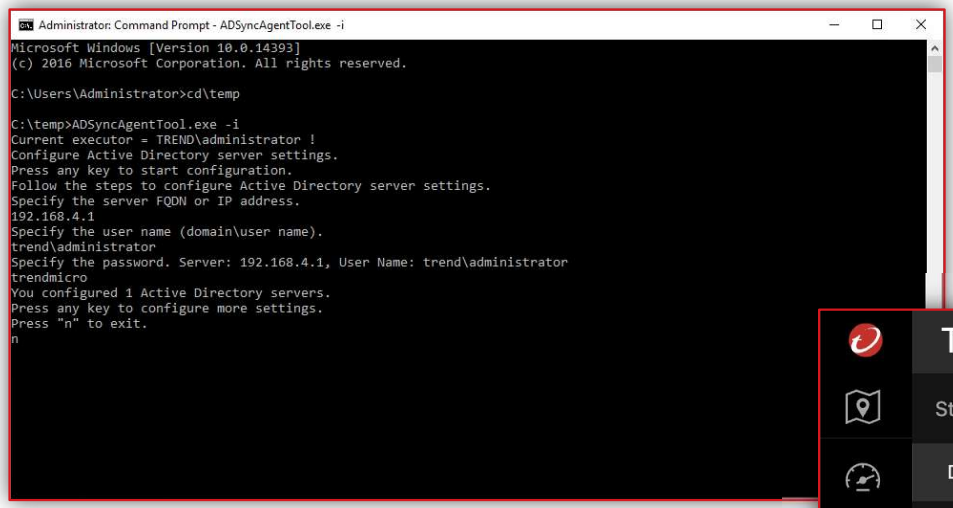
# Active Directory Integration

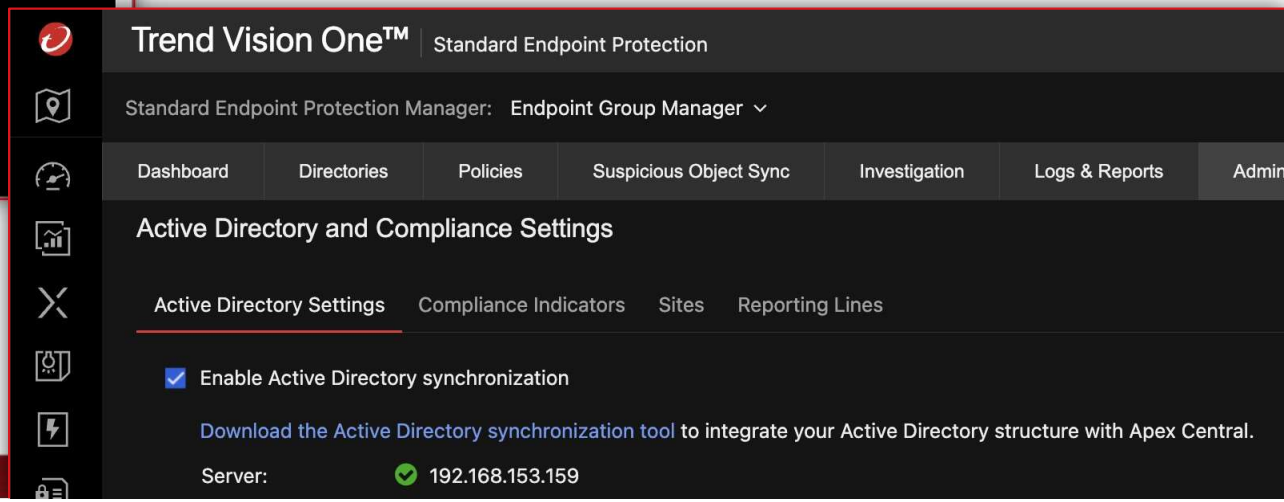
- Al descargar un nuevo agente de sincronización, se desactivan los agentes descargados anteriormente y se detiene la sincronización de los servidores de Active Directory configurados anteriormente.



# Active Directory Integration

- Al descargar un nuevo agente de sincronización, se desactivan los agentes descargados anteriormente y se detiene la sincronización de los servidores de Active Directory configurados anteriormente.



# V1 Endpoint Security - Data Loss Prevention

# Preventing Data Loss on Endpoint Computers

La prevención de pérdida de datos protege a los agentes del riesgo de pérdida o fuga de datos. La prevención de pérdida de datos salvaguarda un

datos confidenciales de la organización contra fugas accidentales o deliberadas. La prevención de pérdida de datos le permite:

Identifique la información confidencial que requiere protección mediante identificadores de datos

Crear políticas que limiten o impidan la transmisión de activos digitales a través de canales de transmisión comunes,

como correo electrónico y dispositivos externos

Exigir el cumplimiento de los estándares de privacidad establecidos

La prevención de pérdida de datos en Vision One Endpoint Security proporciona las siguientes características:

Control de activos digitales

Descubrimiento de datos

Control de dispositivos



# DLP – Control de Activos Digitales



**Create Data Identifiers**

- Expressions
- Attributes
- Keywords

**Create Template**

Combine identifiers to create condition statements

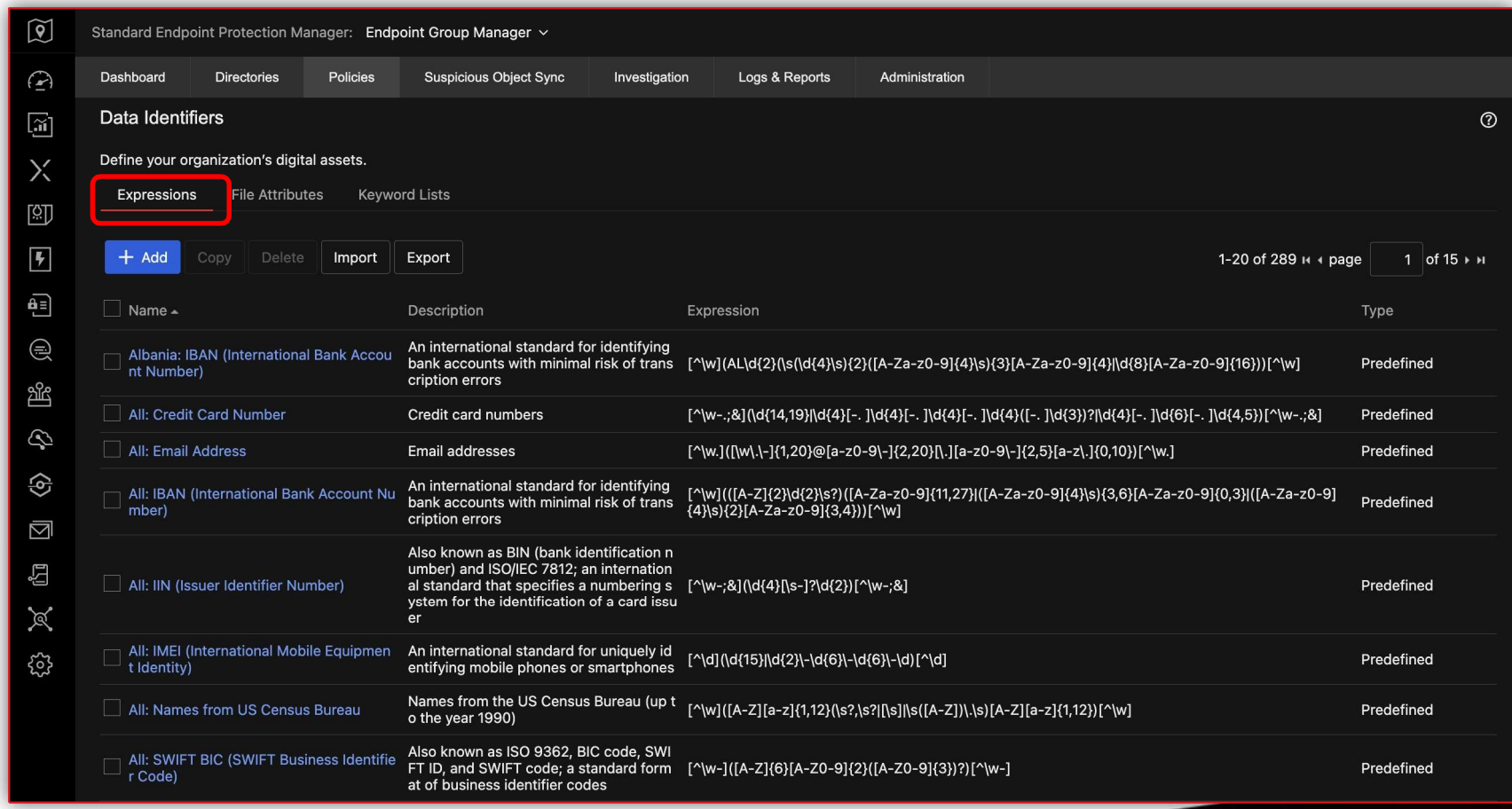
**Create Policy**

- Template
- Channel
- Action

# DLP – Digital Asset Control

Create Data Identifiers

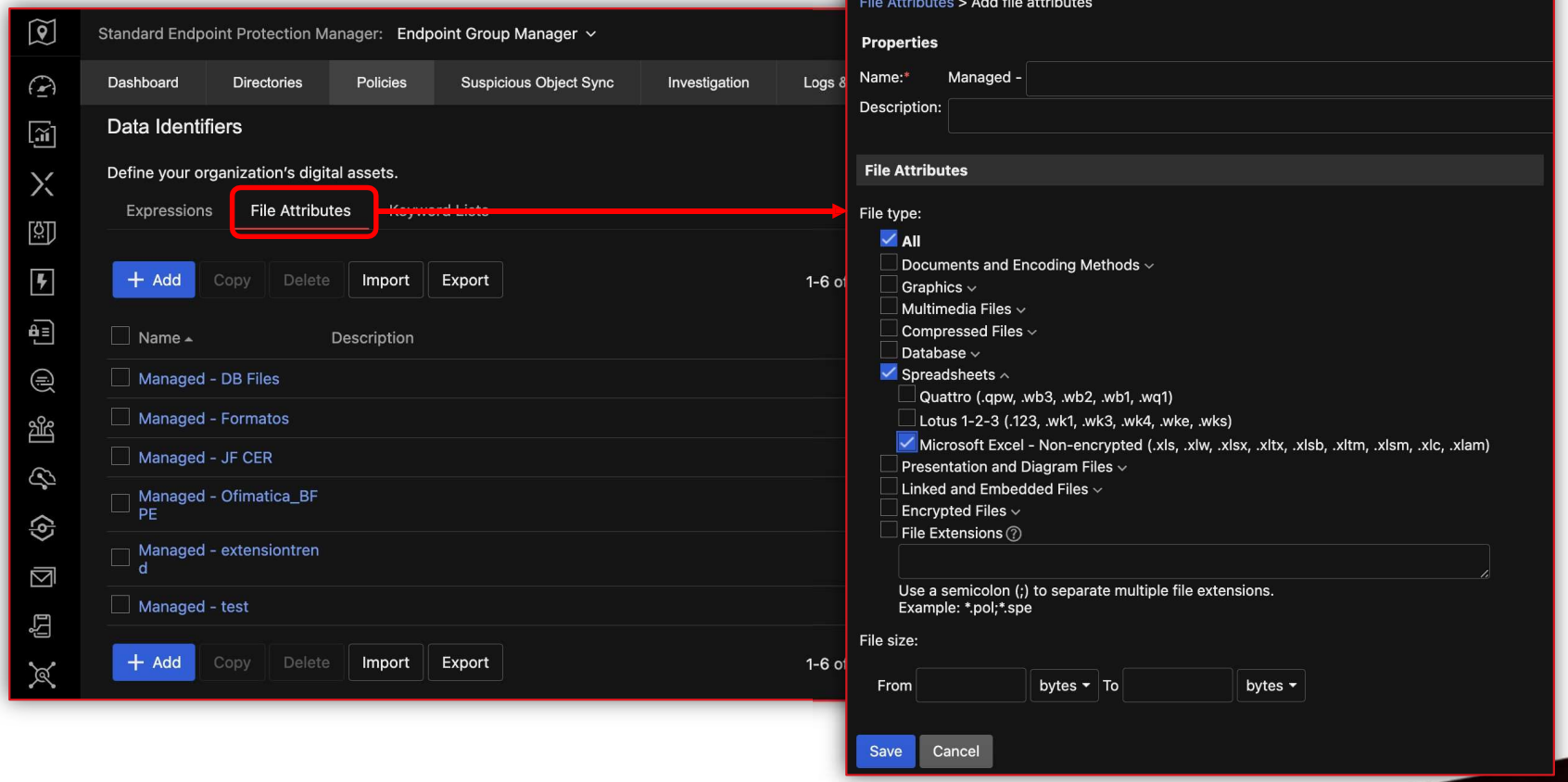
- Expressions
- Attributes
- Keywords



# DLP – Digital Asset Control

Create Data Identifiers

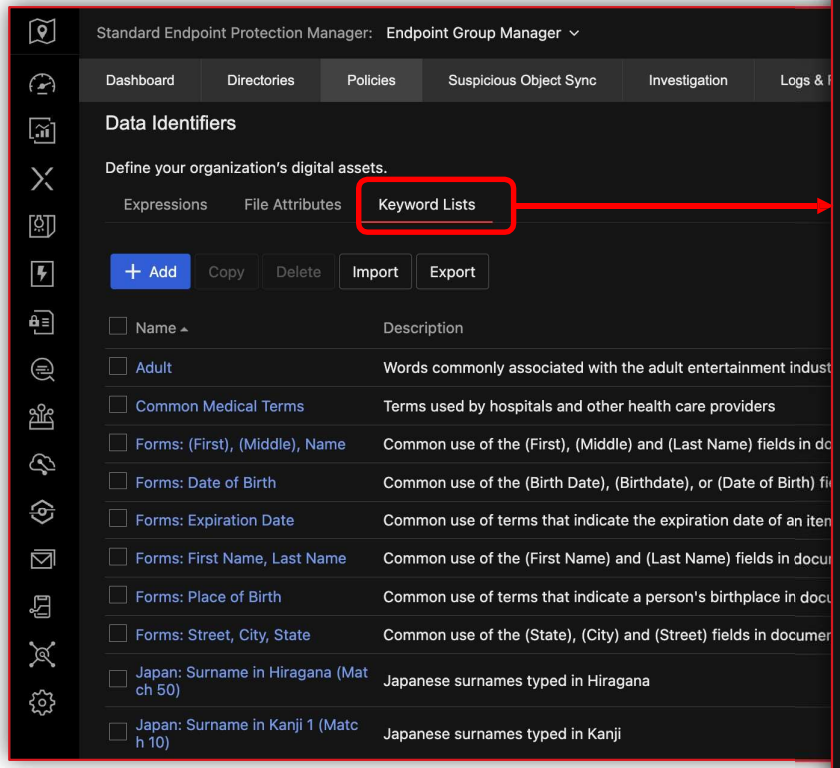
- Expressions
- Attributes
- Keywords

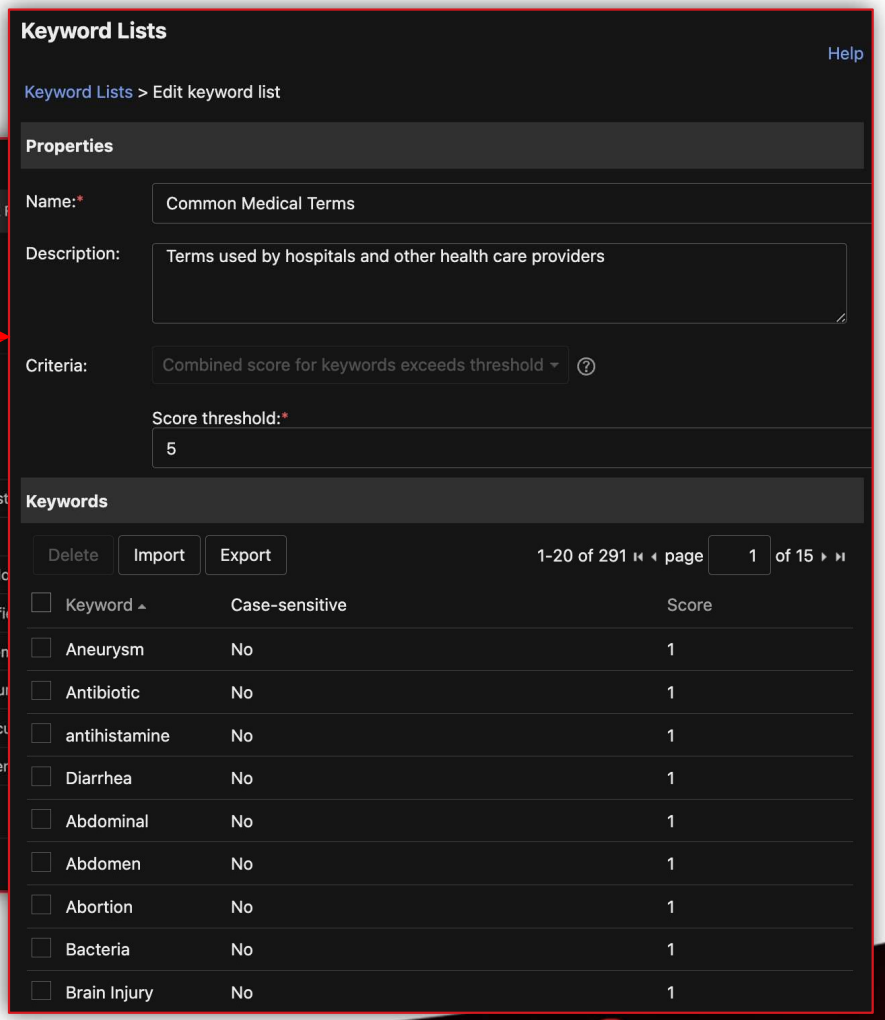


# DLP – Digital Asset Control

Create Data Identifiers

- Expressions
- Attributes
- Keywords



# DLP – Digital Asset Control



**Create Data Identifiers**

- Expressions
- Attributes
- Keywords

**Create Template**

Combine identifiers to create condition statements

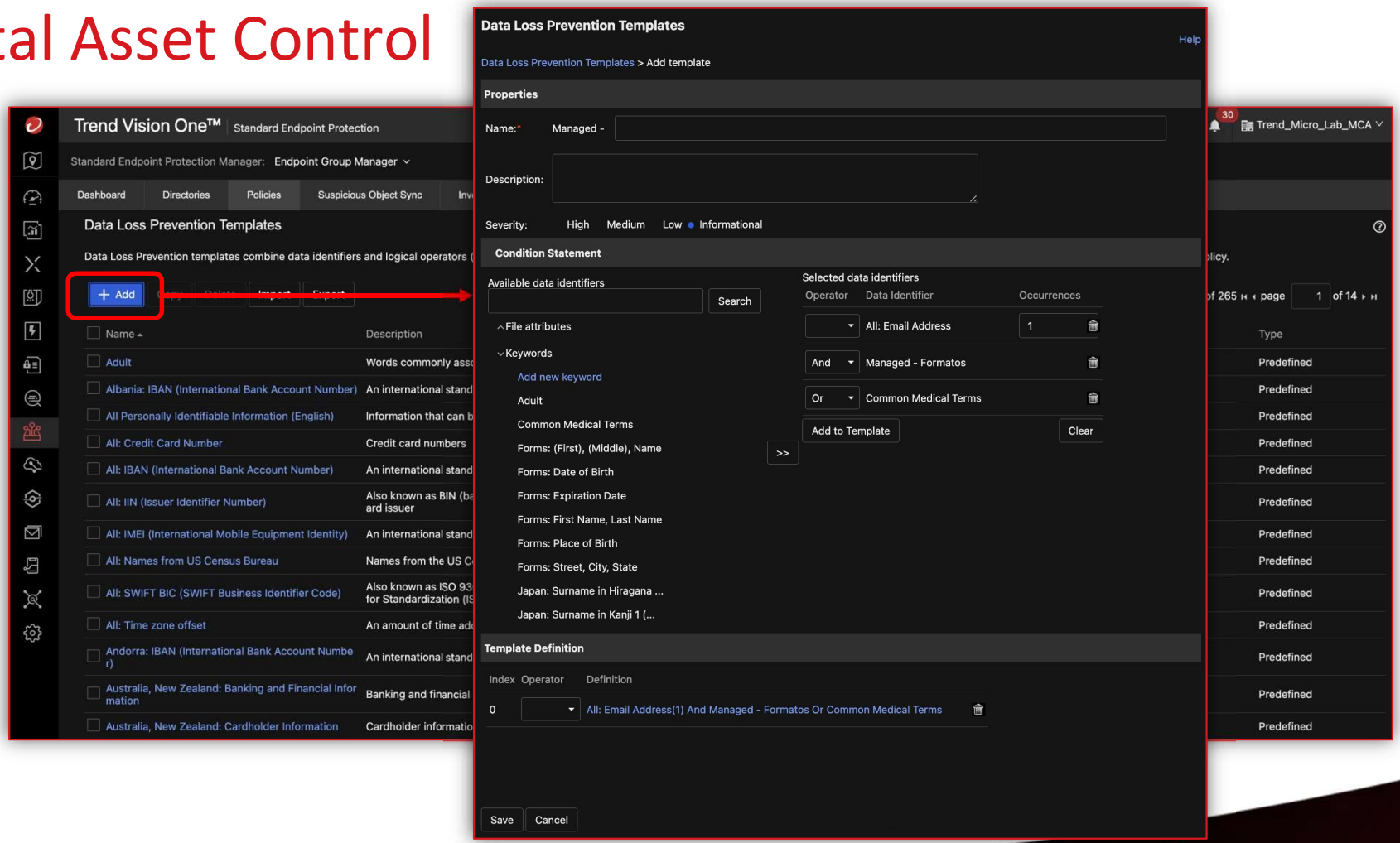
**Create Policy**

- Template
- Channel
- Action

# DLP – Digital Asset Control

Create Template

Combine identifiers to create condition statements



# DLP – Digital Asset Control



**Create Data Identifiers**

- Expressions
- Attributes
- Keywords

**Create Template**

Combine identifiers to create condition statements

**Create Policy**

- Template
- Channel
- Action

# DLP – Digital Asset Control

Create Policy

- Template
- Channel
- Action





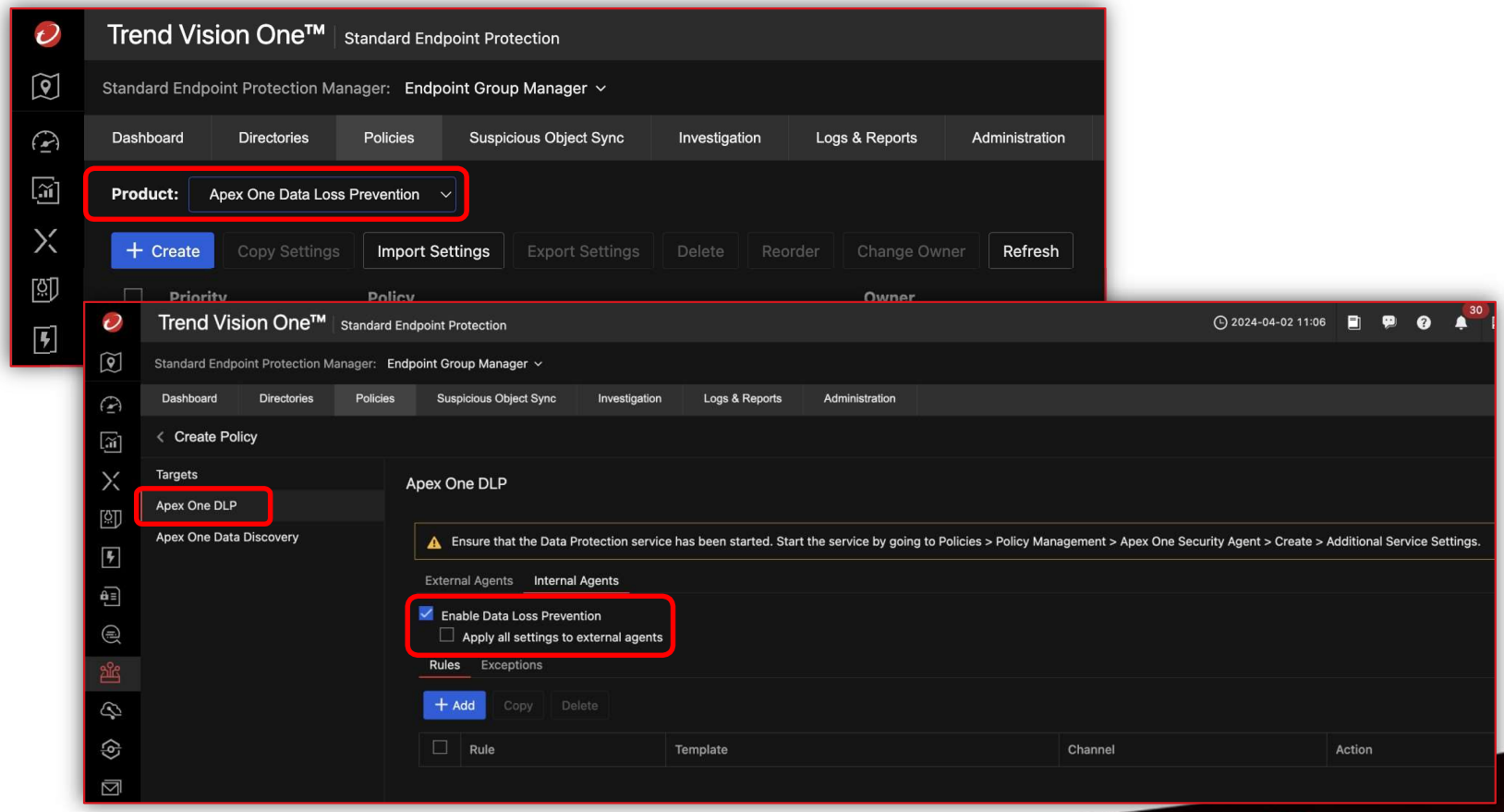



Template Channel Action

# DLP – Digital Asset Control

Create Policy

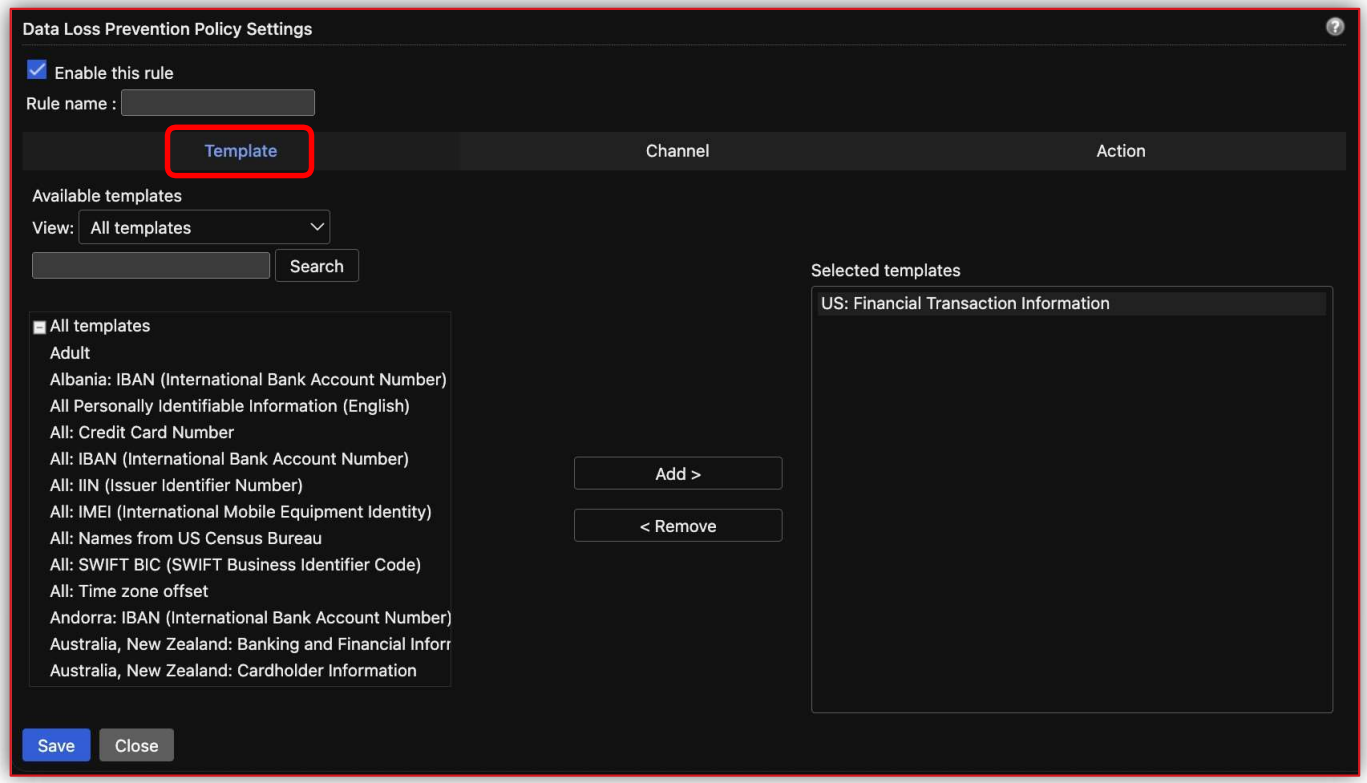
- Template
- Channel
- Action



# DLP – Digital Asset Control

Create Policy

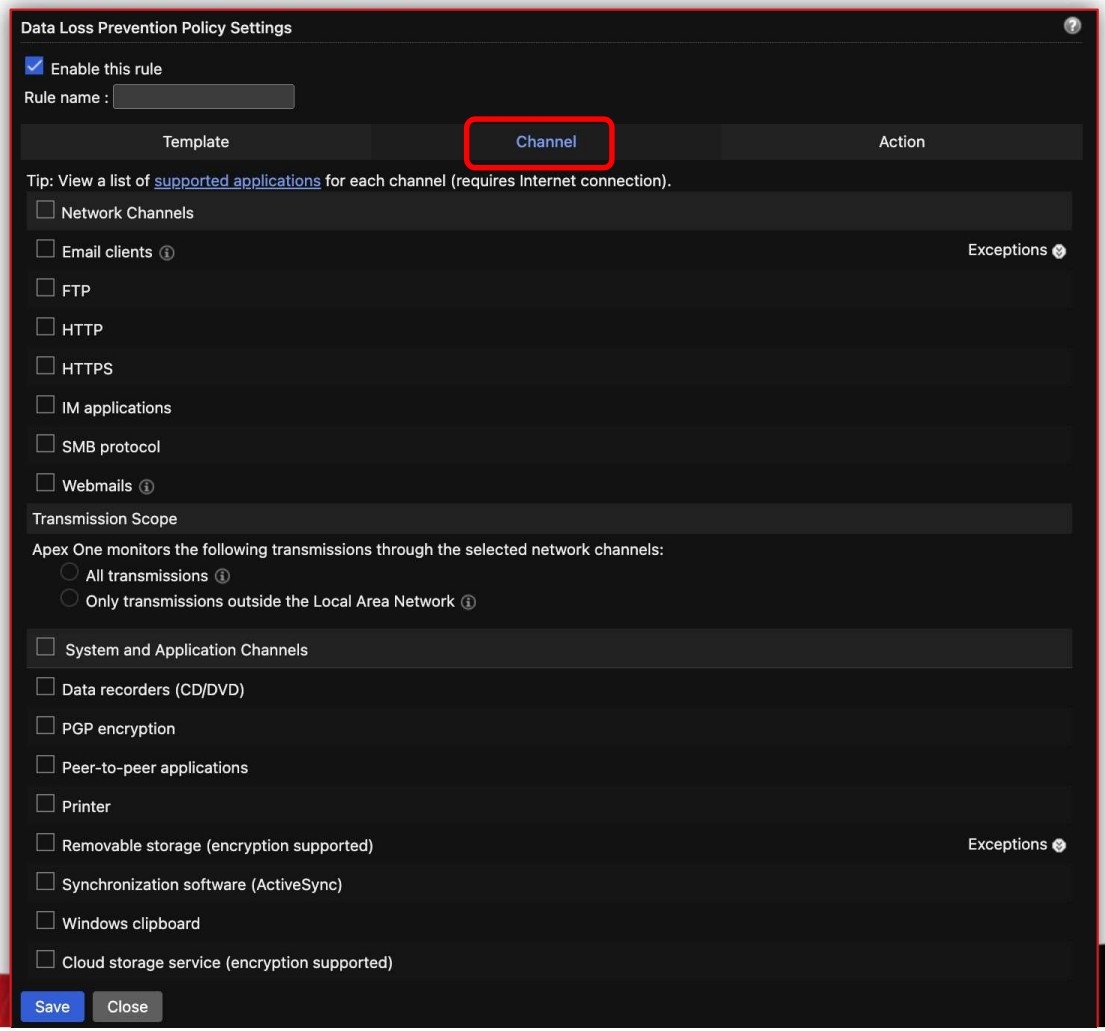
- Template
- Channel
- Action



# DLP – Digital Asset Control

Create Policy

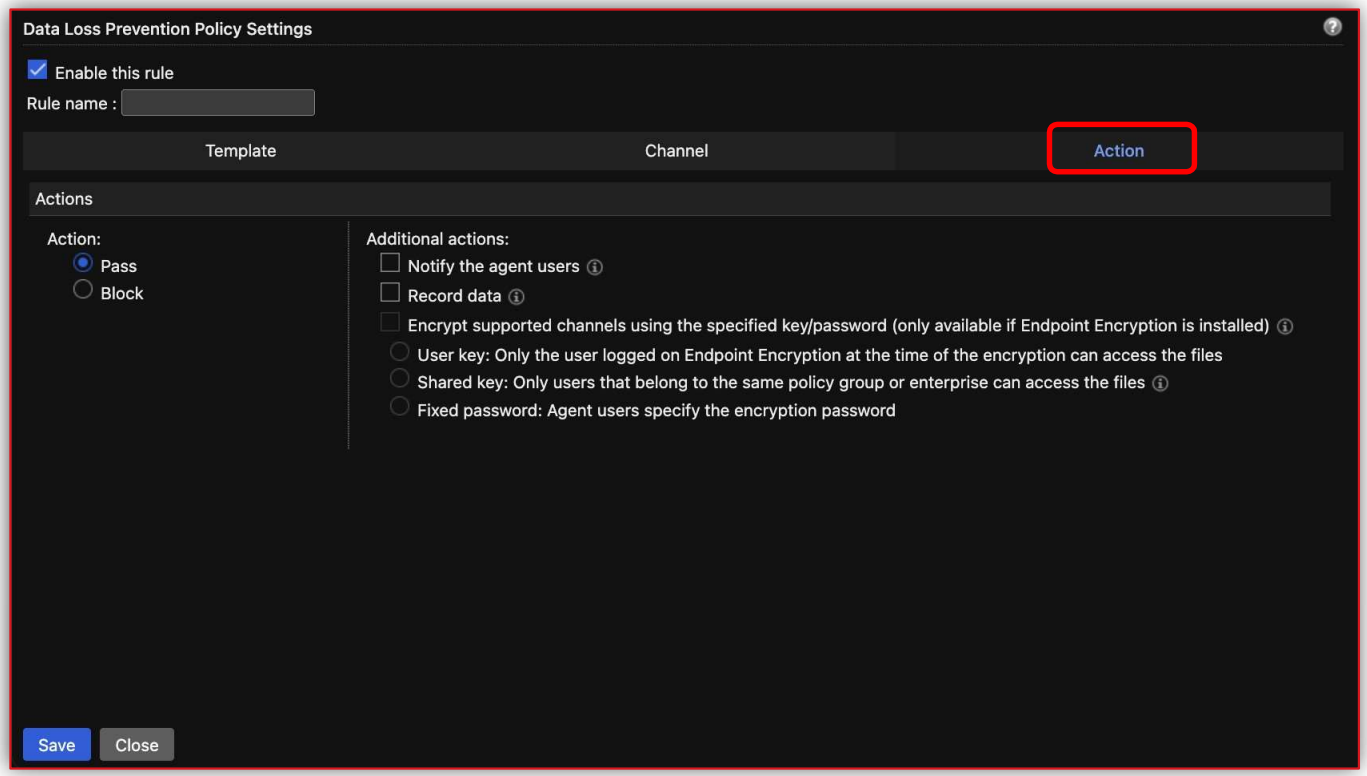
- Template
- Channel
- Action



# DLP – Digital Asset Control

Create Policy

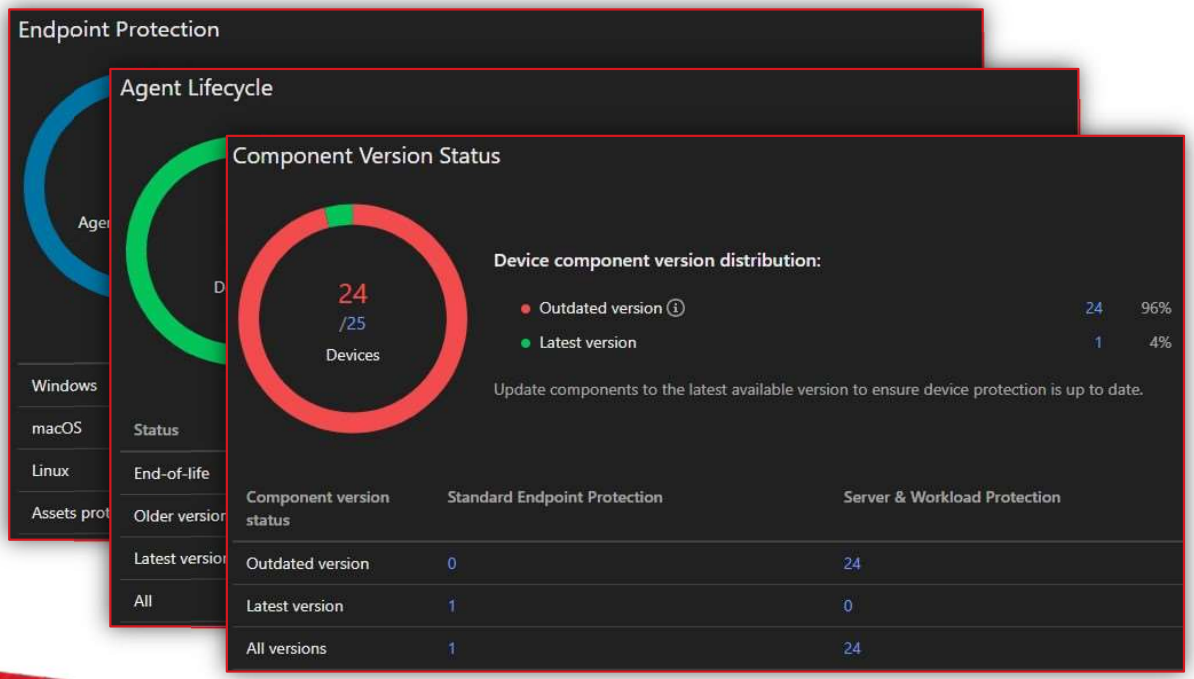
- Template
- Channel
- Action

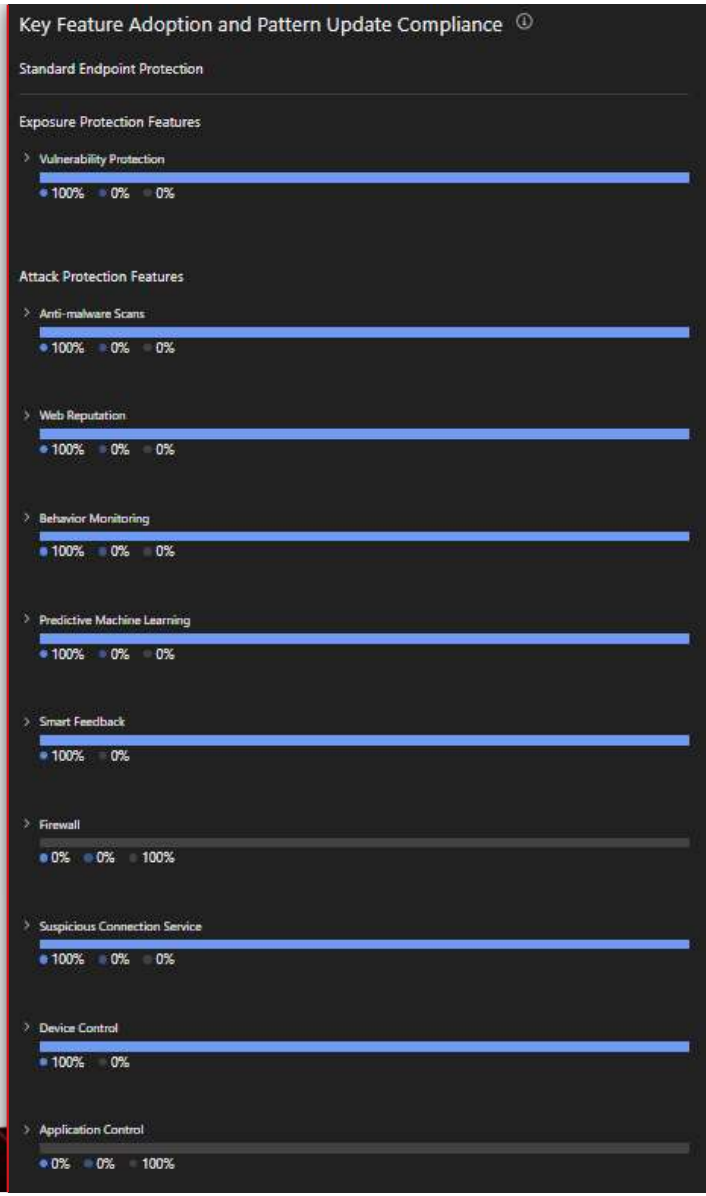


# V1 Endpoint Security - Solución de problemas e investigación

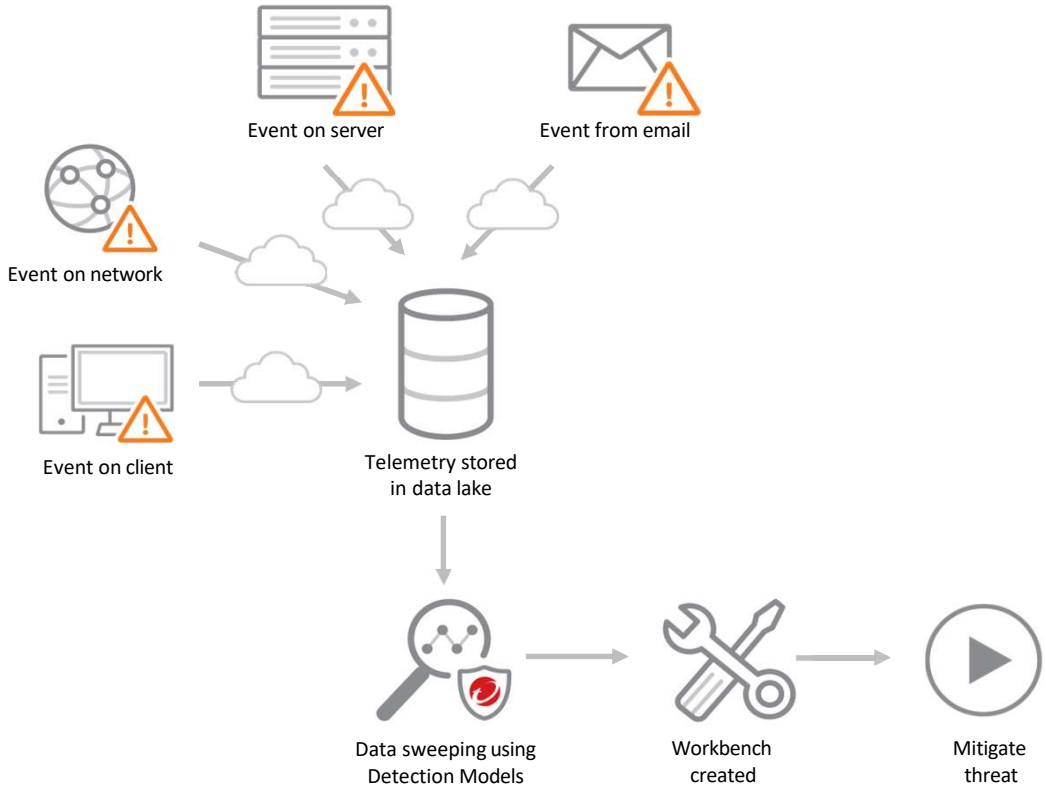
# Security Configuration

El **Security Configuration Index** es una calificación completa del estado de protección de Trend Micro de su organización. El índice se basa en factores que incluyen la implementación de agentes y sensores, y las tasas de adopción de características clave para las capas de seguridad de endpoints, correo electrónico y red. Mejore su configuración de seguridad para mejorar el **Security Configuration Index**.

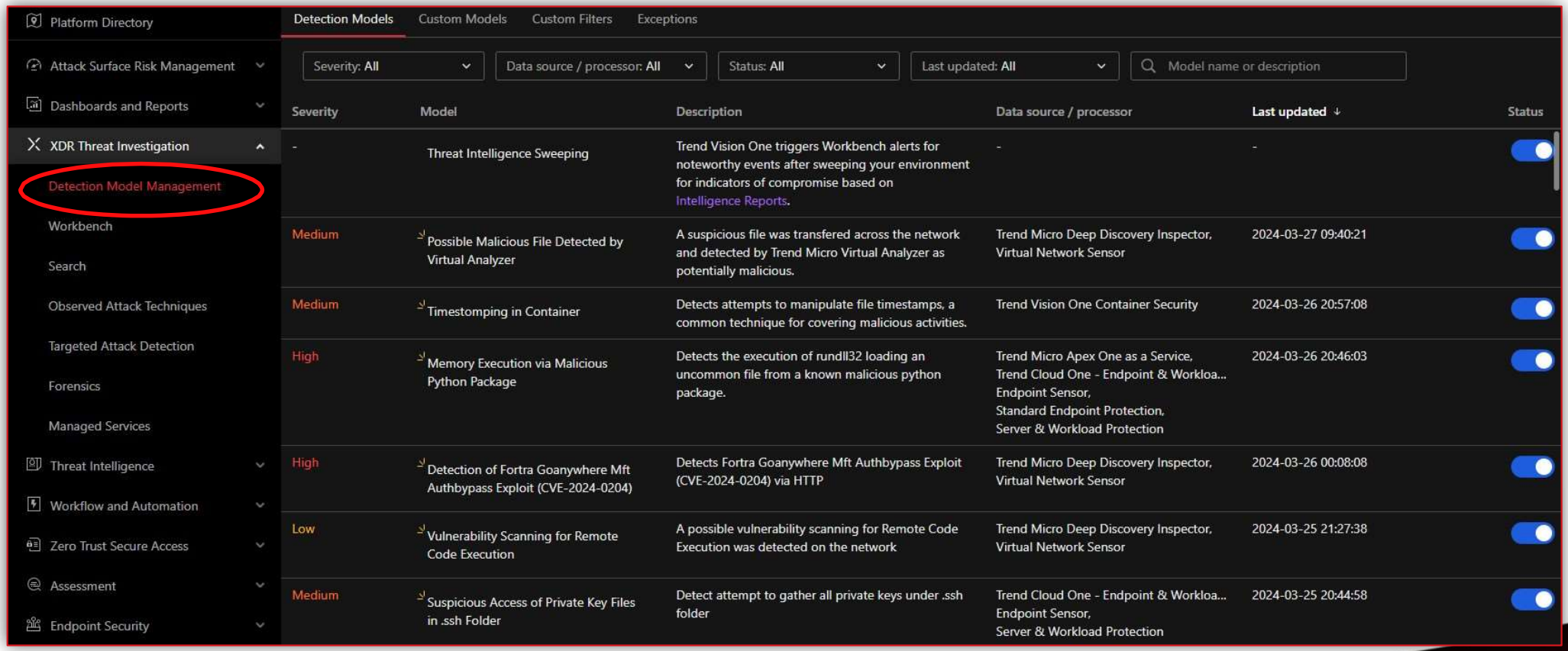


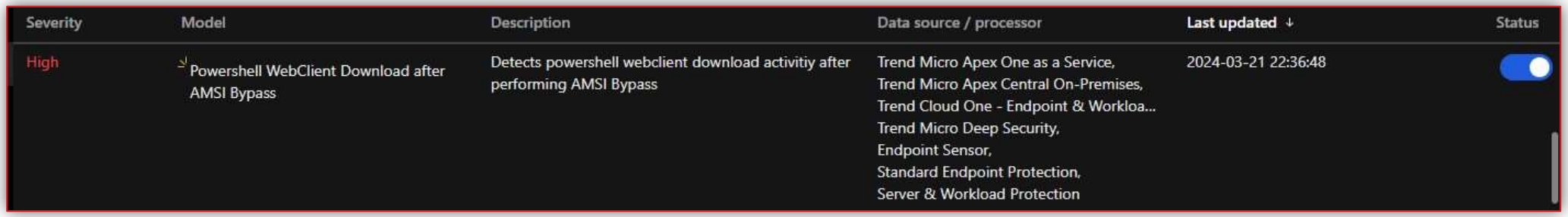
# Detection Models



# Detection Model Management



# Model Details



| Severity | Model | Description | Data source / processor | Last updated ↓ | Status |
|---|---|---|---|---|---|
| High | Powershell WebClient Download after AMSI Bypass | Detects powershell webclient download activitiy after performing AMSI Bypass | Trend Micro Apex One as a Service, Trend Micro Apex Central On-Premises, Trend Cloud One - Endpoint & Workloa... Trend Micro Deep Security, Endpoint Sensor, Standard Endpoint Protection, Server & Workload Protection | 2024-03-21 22:36:48 | |

The severity level Trend Micro Vision One assigns to the model depends on the type of event and MITRE information. The available severity levels include:

- **Critical**: This event exhibits strong evidence of compromise for targeted attacks, Advanced Persistent Threats (APTs), or cybercrime operations
- **High**: This event exhibits highly suspicious indicators associated with targeted attacks, APTs, or cybercrime operations
- **Medium**: This event exhibits suspicious indicators possibly associated with malware infections, policy violations, or cybercrime operations
- **Low**: This event exhibits mildly suspicious indicators useful for security monitoring or threat hunting

Each model is identified by a unique name, assigned by the Trend Micro security analysts

A short description of the detection model is displayed for information purposes

The products to which this detection model applies

The time range during which Trend Micro last updated the model

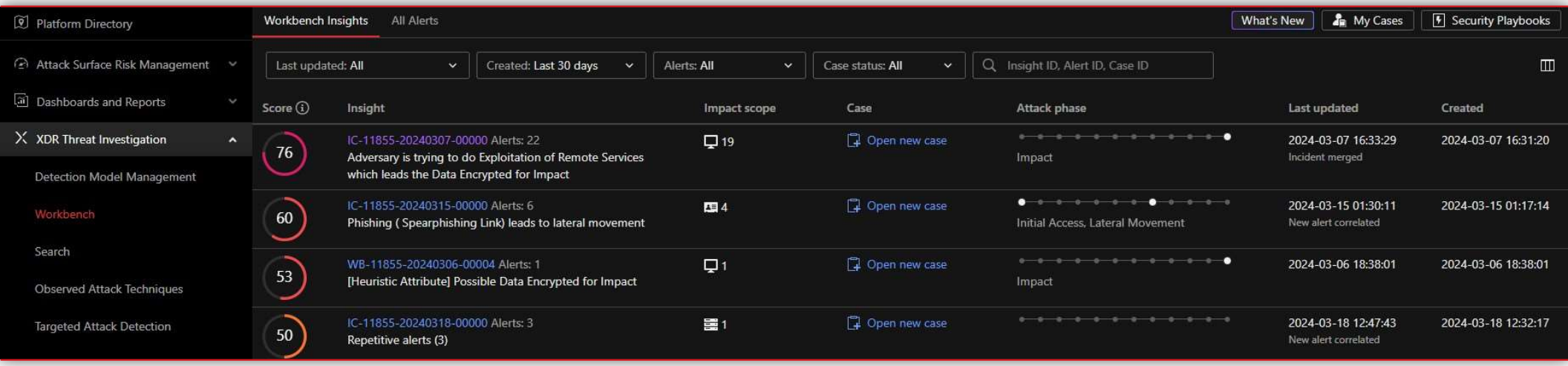
Trend Micro Vision One automatically enables the alert triggers for supported products in your environment. Any model can be disabled by clicking the status icon

# Workbench Insights

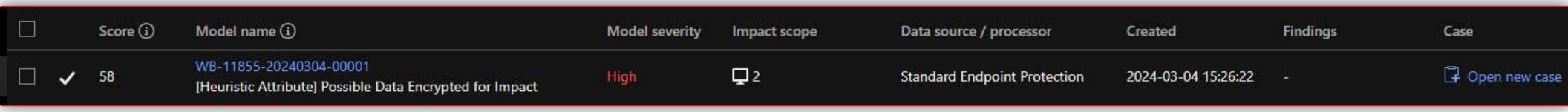
Identify and mitigate potential system breaches and incidents in your environment.

**Workbench Insights** (**XDR Threat Investigation** → **Workbench**) displays a list of high-priority insights that let you start your investigations intelligently.

There are two types of Workbench insights: Correlated alerts and standalone alerts. Trend Vision One creates insights using advanced correlation and machine learning techniques.



# Workbench Alert Details




Displays the current status of the alert or investigation triggered in the Workbench, including:

- Open
- In Progress
- Closed
- Close - False Positive

The overall severity assigned to the alert. Trend Micro Vision One calculates the score based on the severity of the matched detection model and the impact scope of the alert

A unique identifier for the alert. Click the Workbench ID to view the summary of the event

The severity assigned to a model that triggered the alert is displayed

Displays the number of entities that the alert affects within the company network

The product that is providing the data to the Workbench app

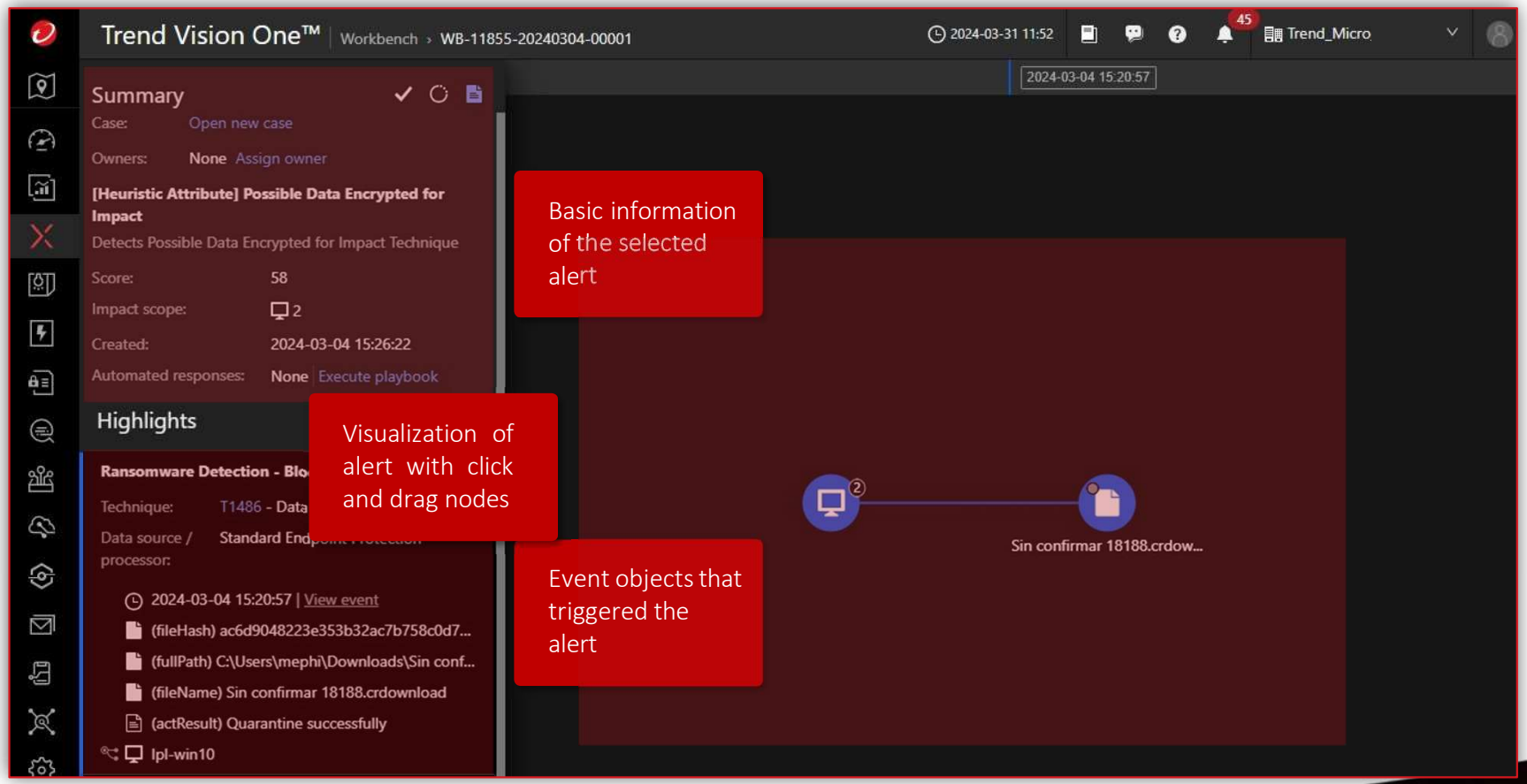
Displays the date and time Trend Micro Vision One generated the alert

Findings: The findings of the alert investigation.

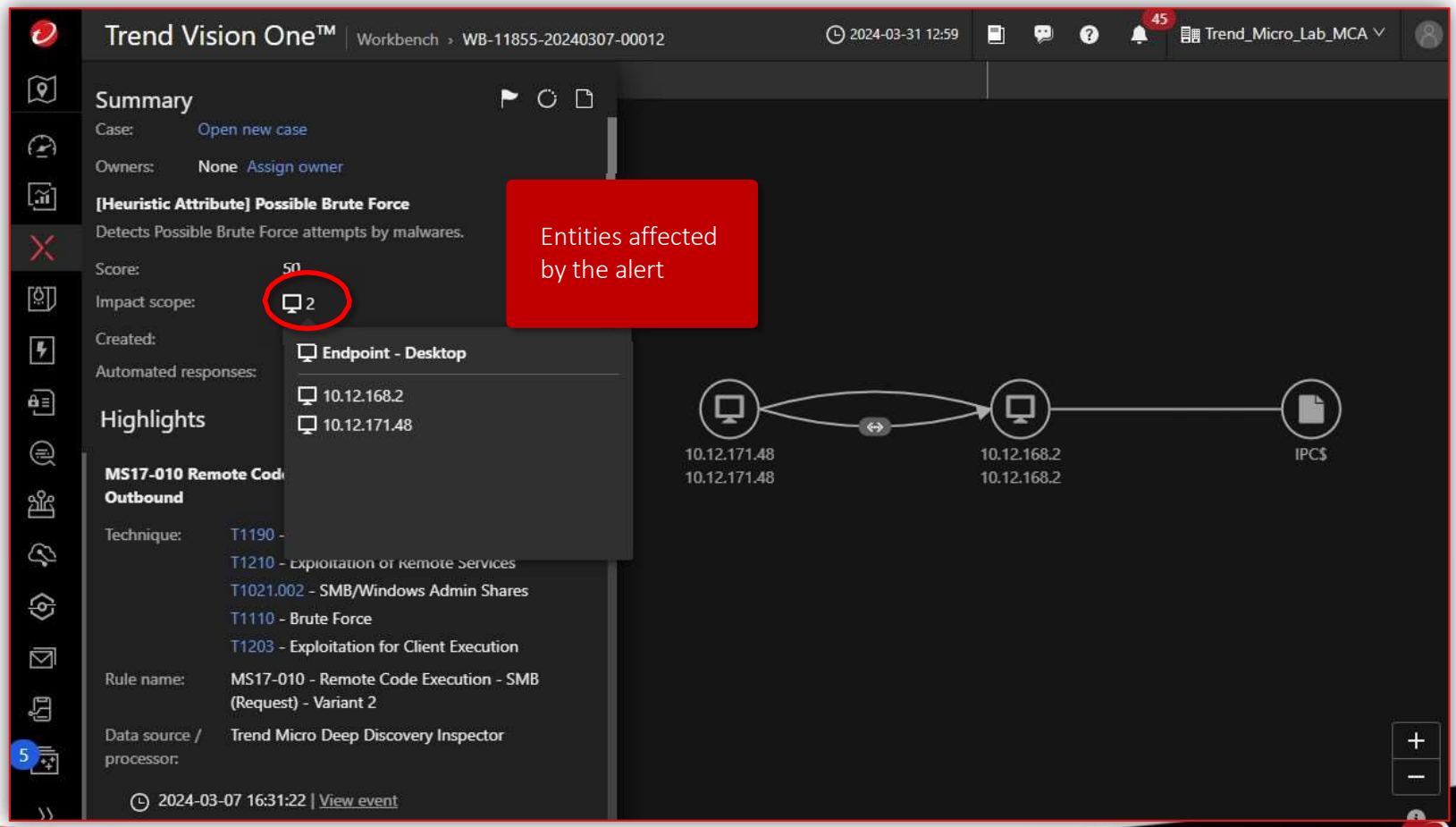
Available values:

- Confirmed incident: The investigation confirmed the occurrence of threats or malicious activities.
- False positive: No malicious activity found.
- Benign true positive: The investigation has confirmed the presence of a genuine threat that poses no risk to the organization.
- Benign true positives are the result of penetration test or other legitimate activities in your environment.
- Noteworthy: Observations have identified suspicious activity that requires more investigation.

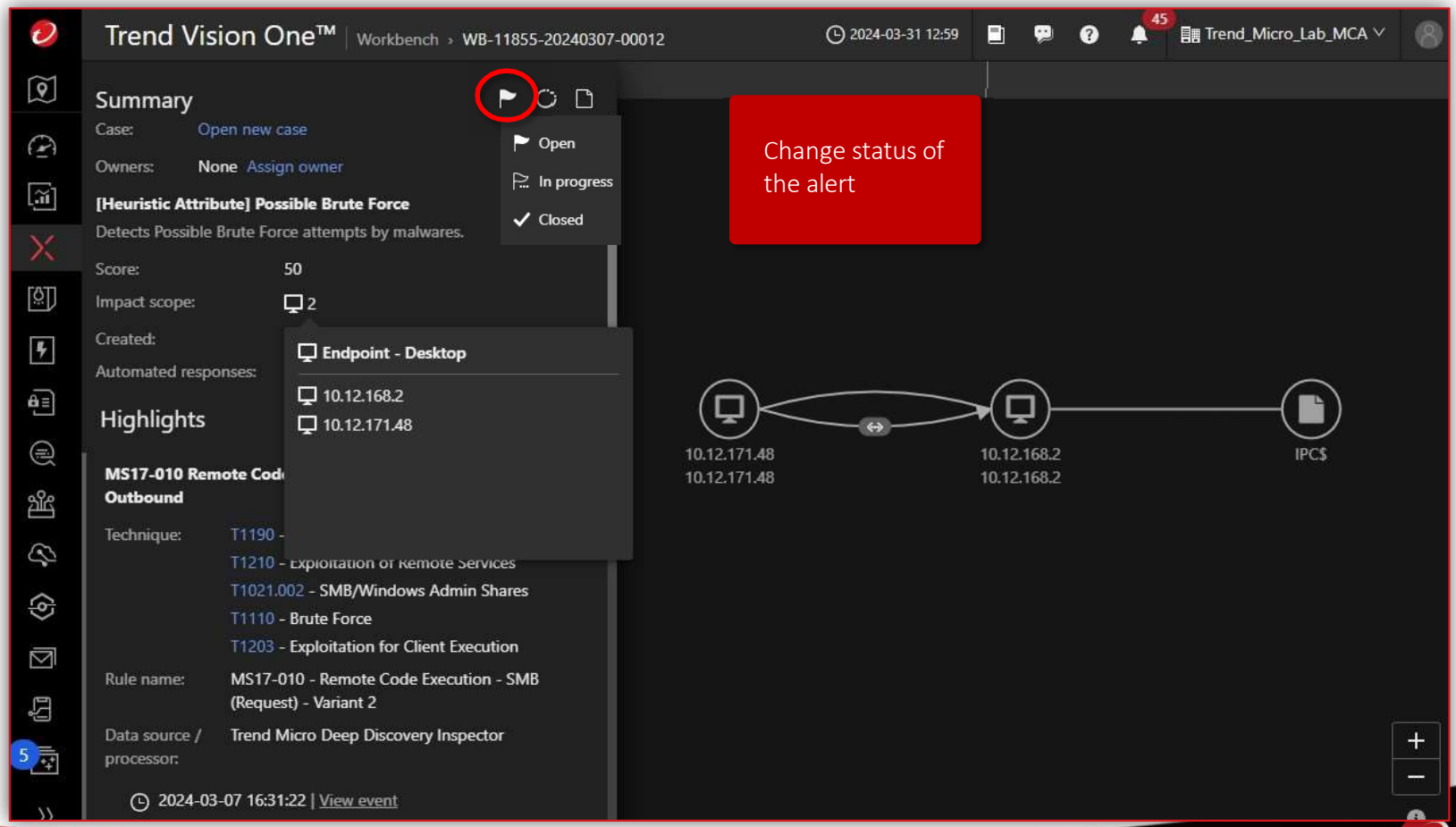
# Alert Details



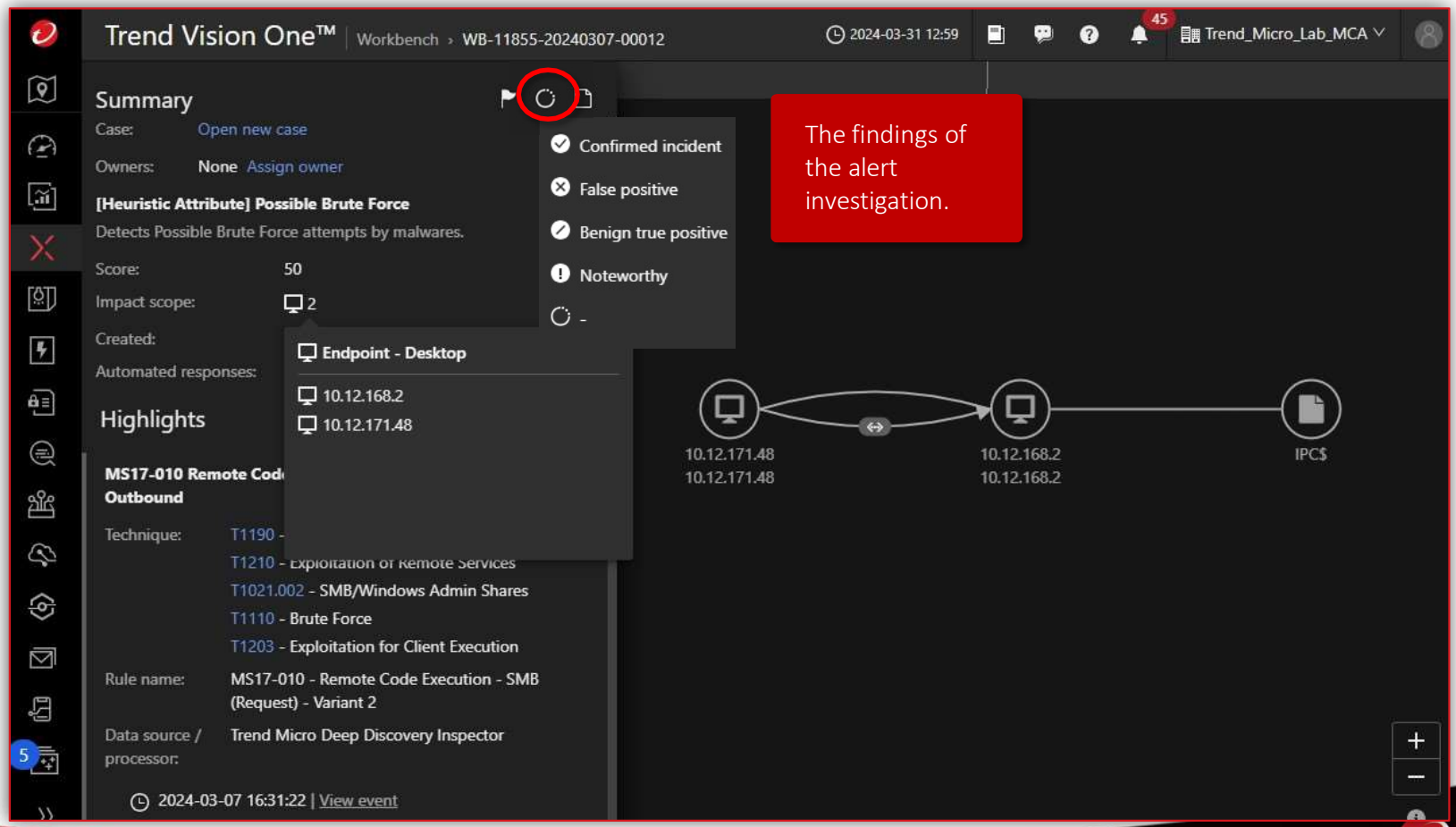
# Navigating Within a Workbench



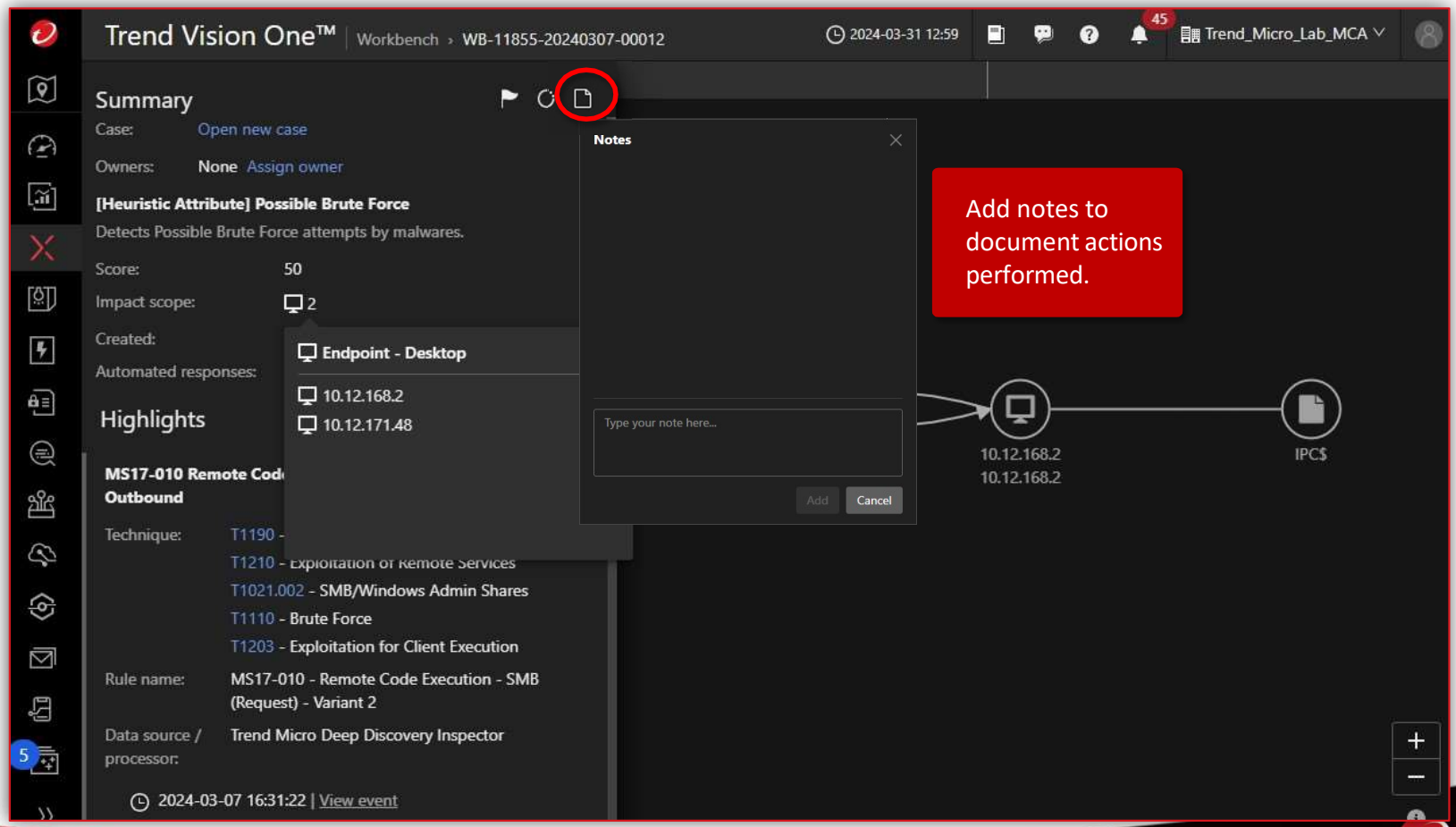
# Navigating Within a Workbench



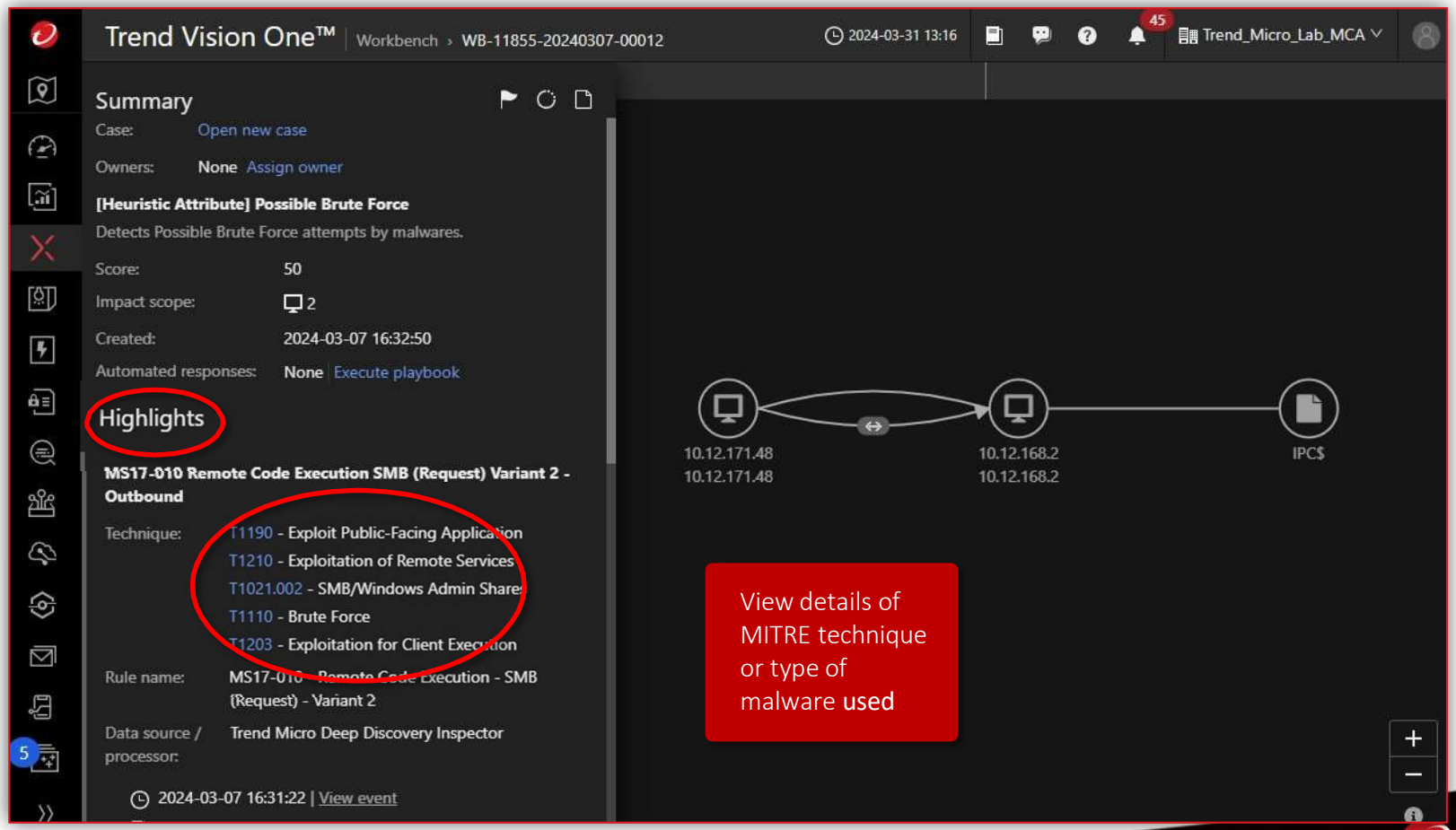
# Navigating Within a Workbench



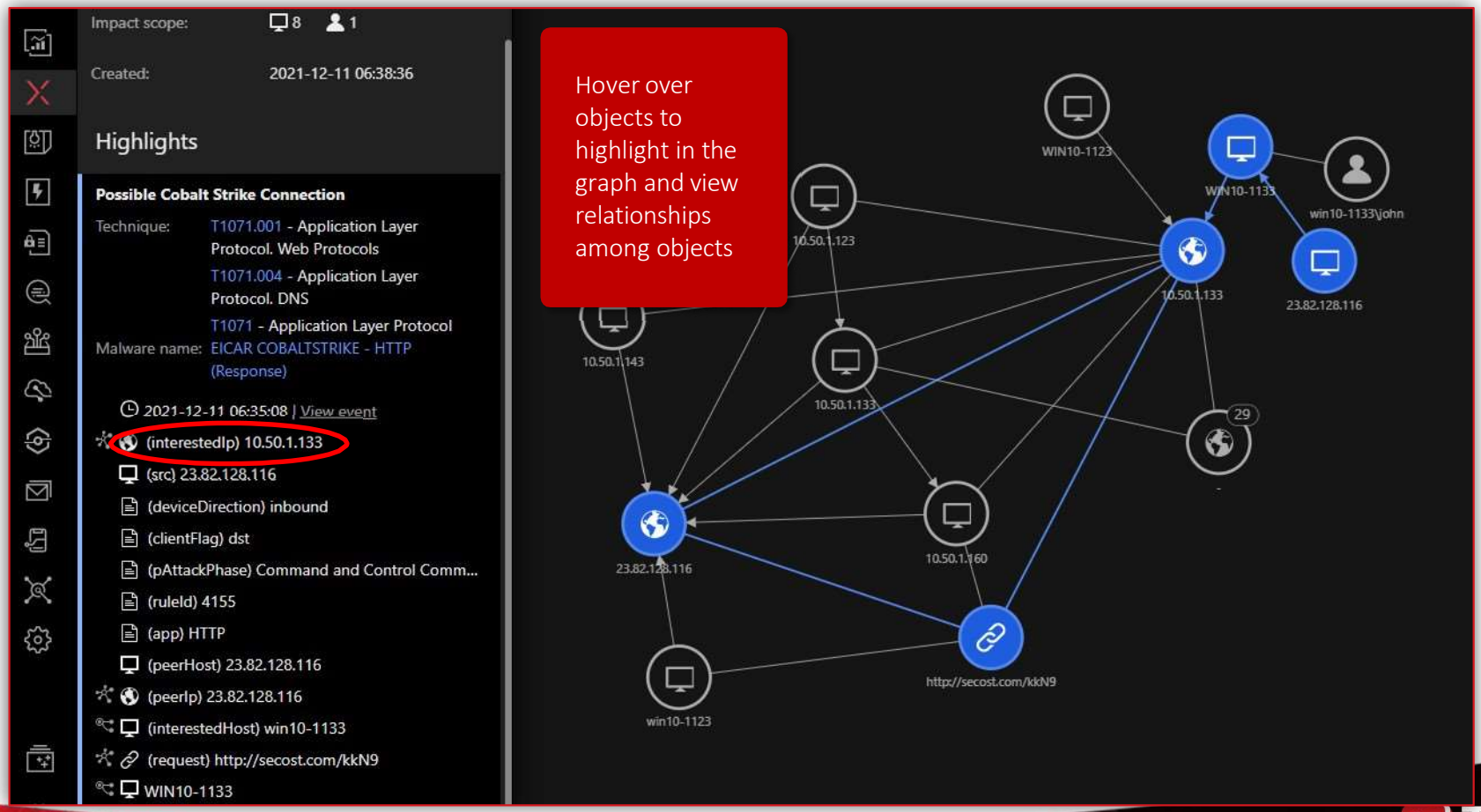
# Navigating Within a Workbench



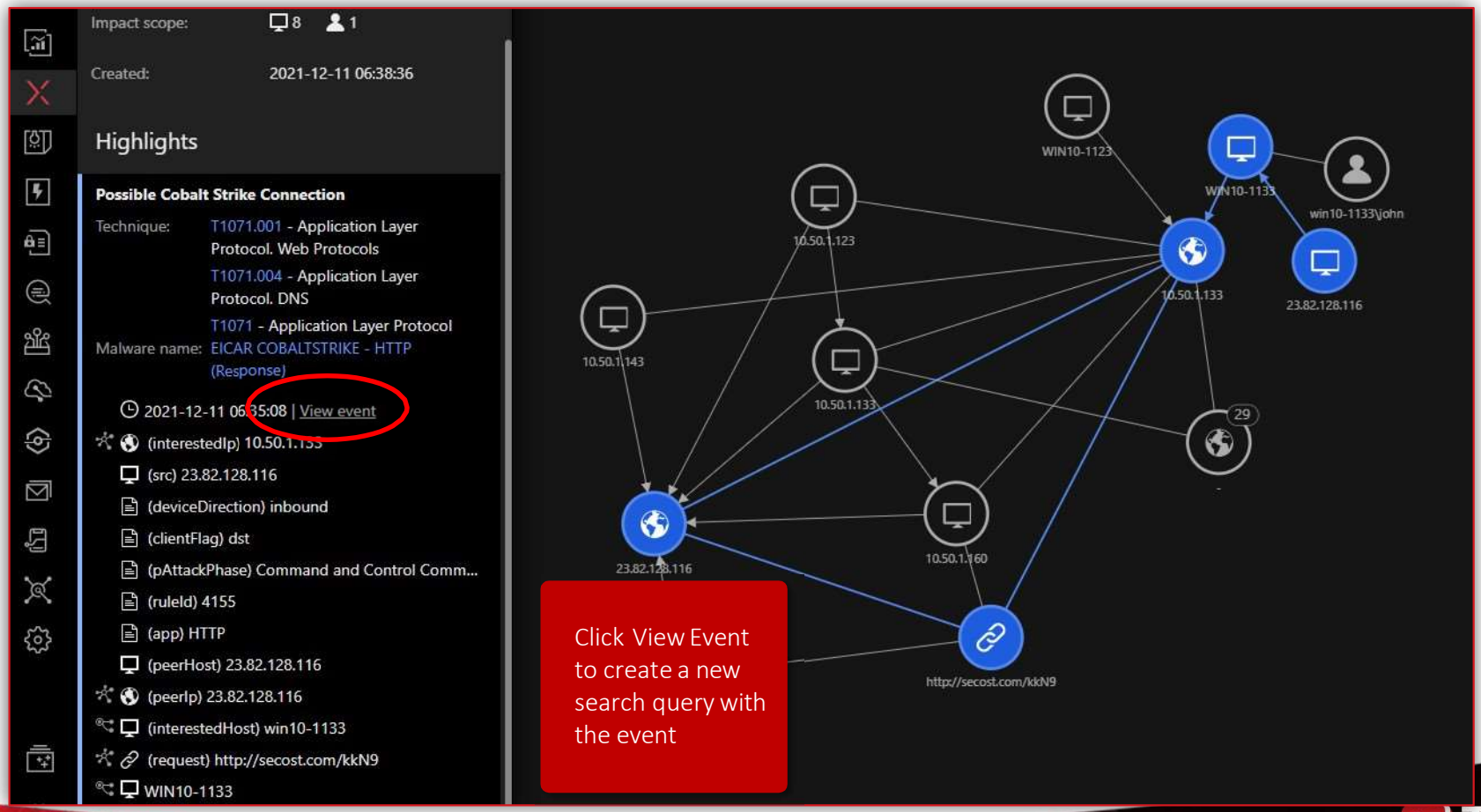
# Navigating Within a Workbench



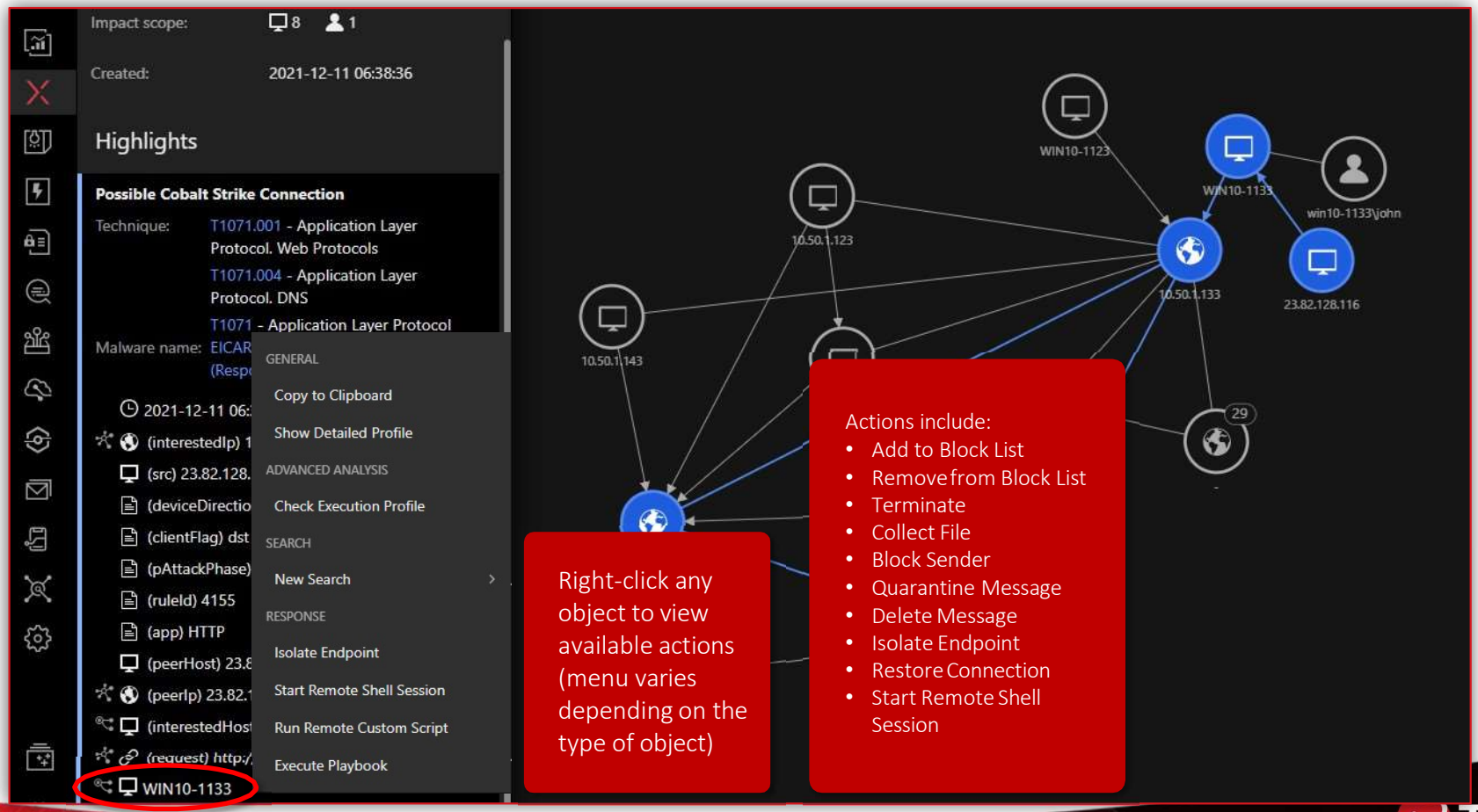
# Navigating Within a Workbench



# Navigating Within a Workbench



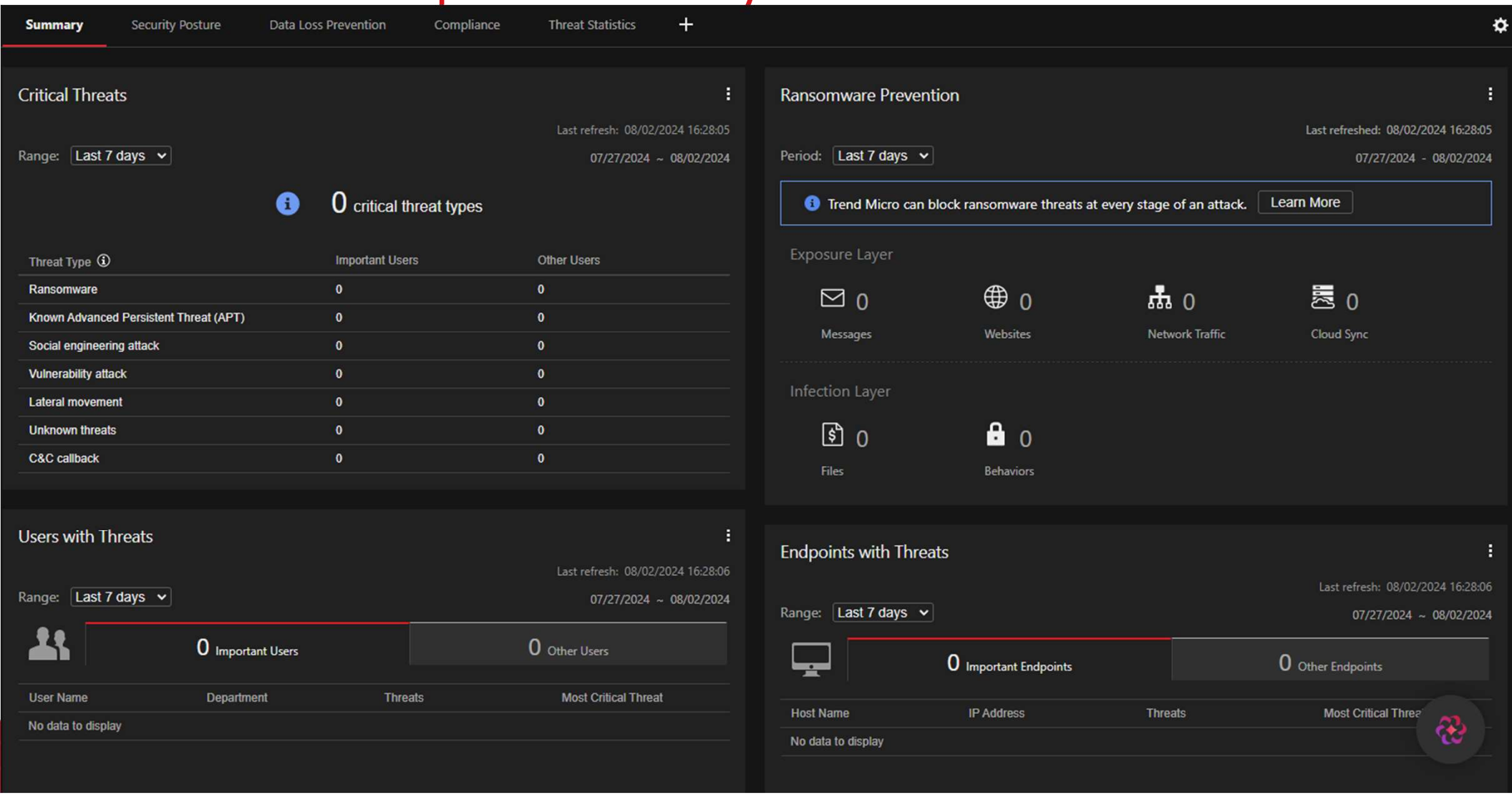
# Navigating Within a Workbench



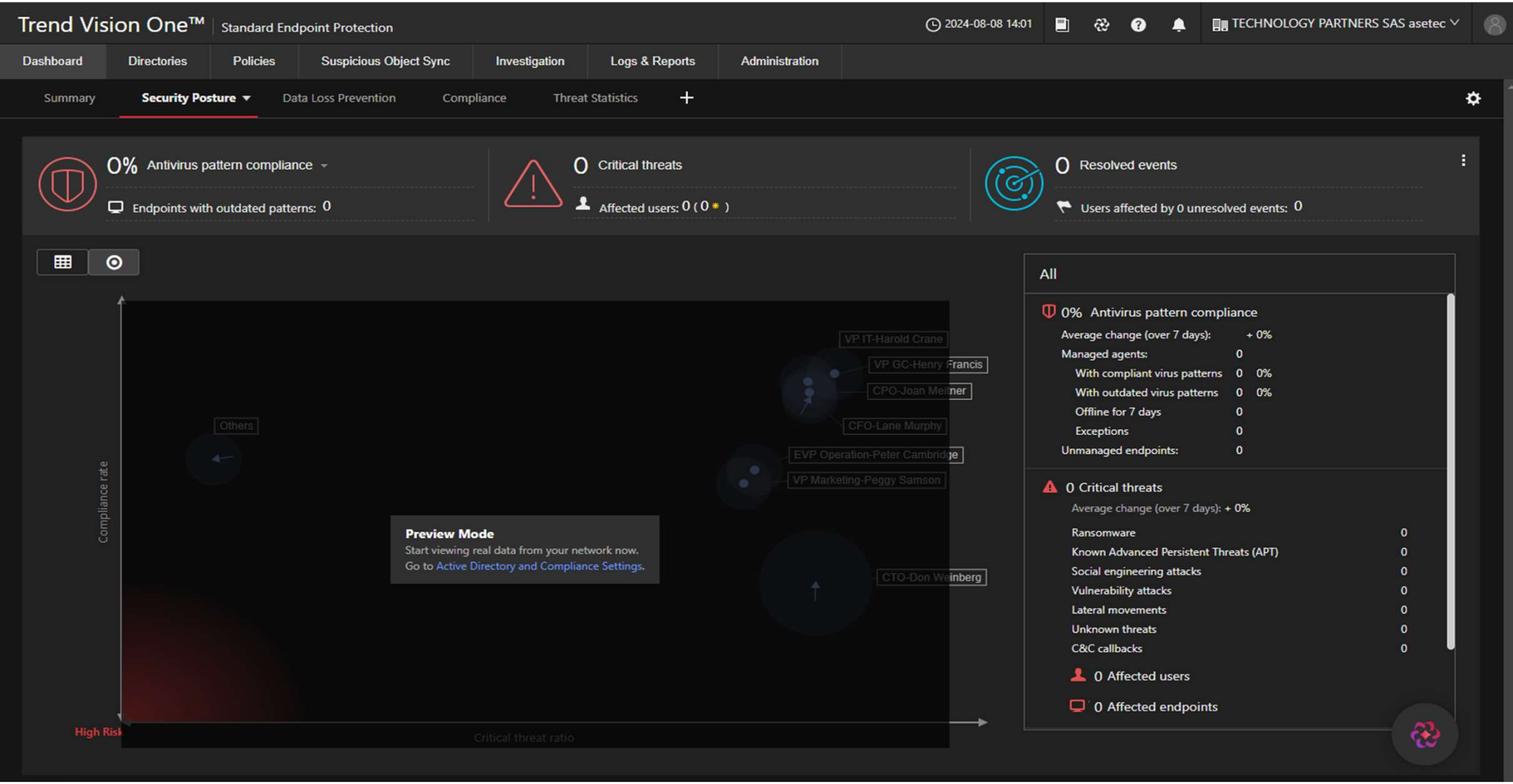
# Consola de Administración– Standard Endpoint Security Protection



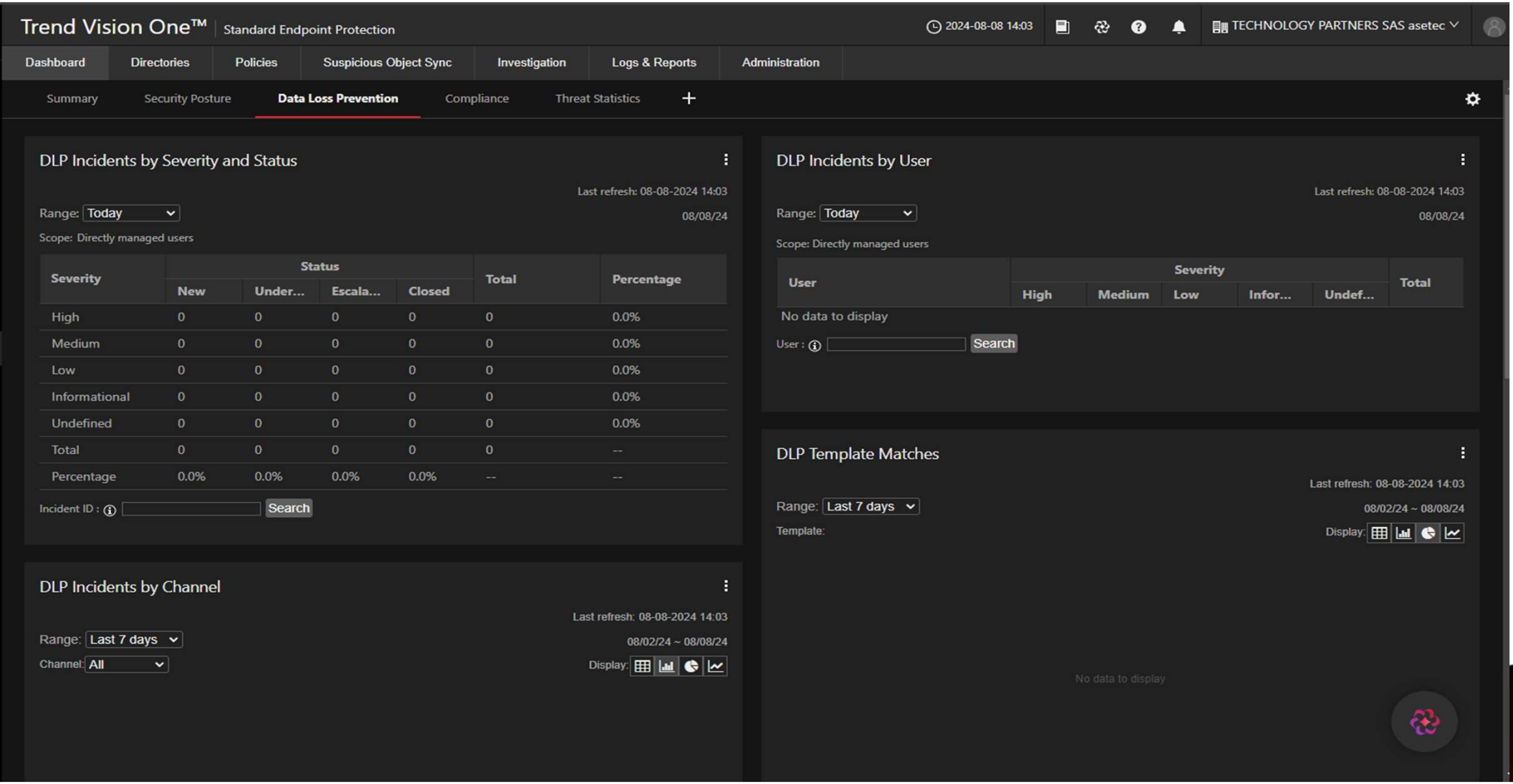
# Standard Enpoint Security Protection - Dashboard



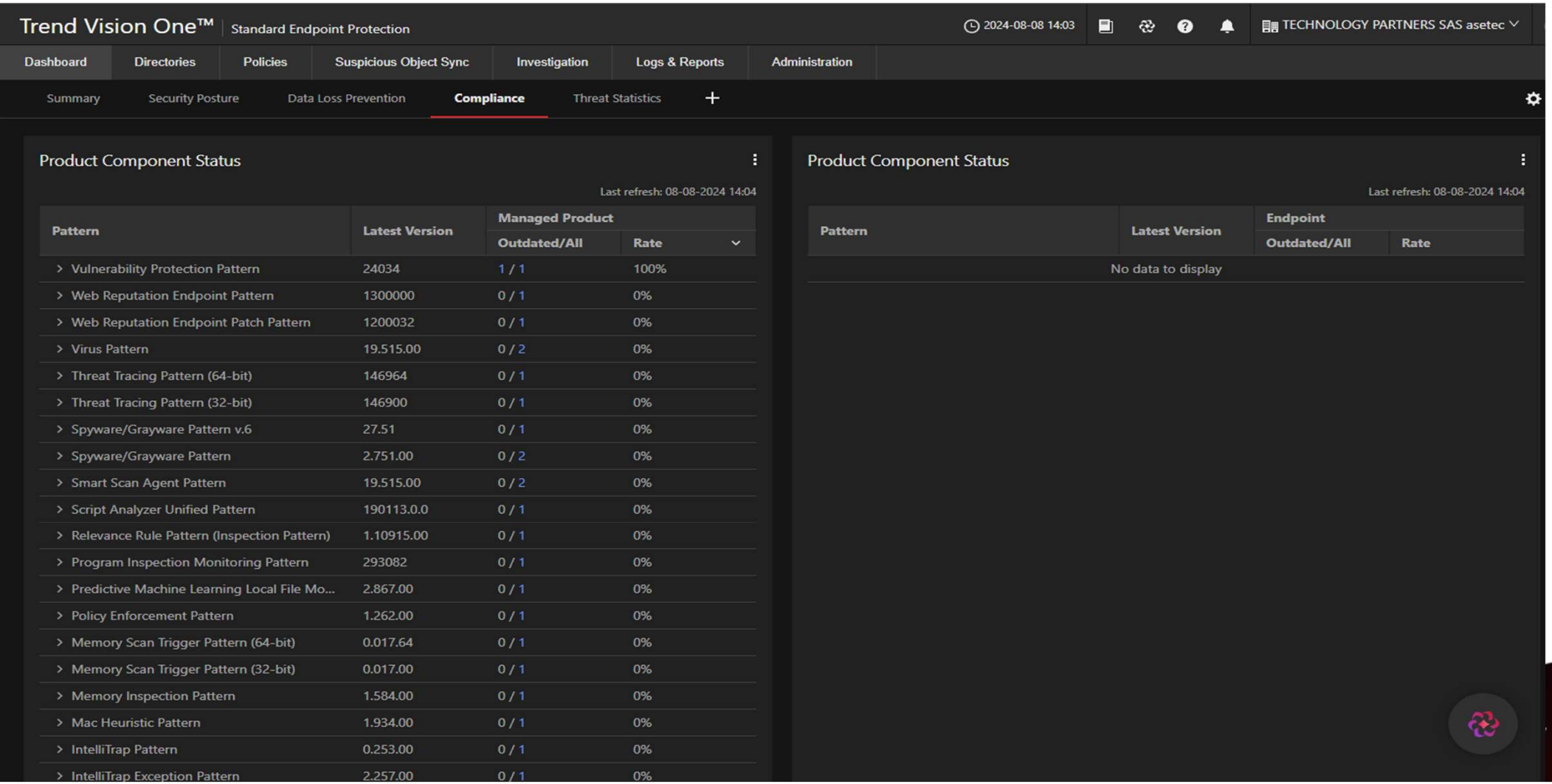
# Dashboard – Security Posture



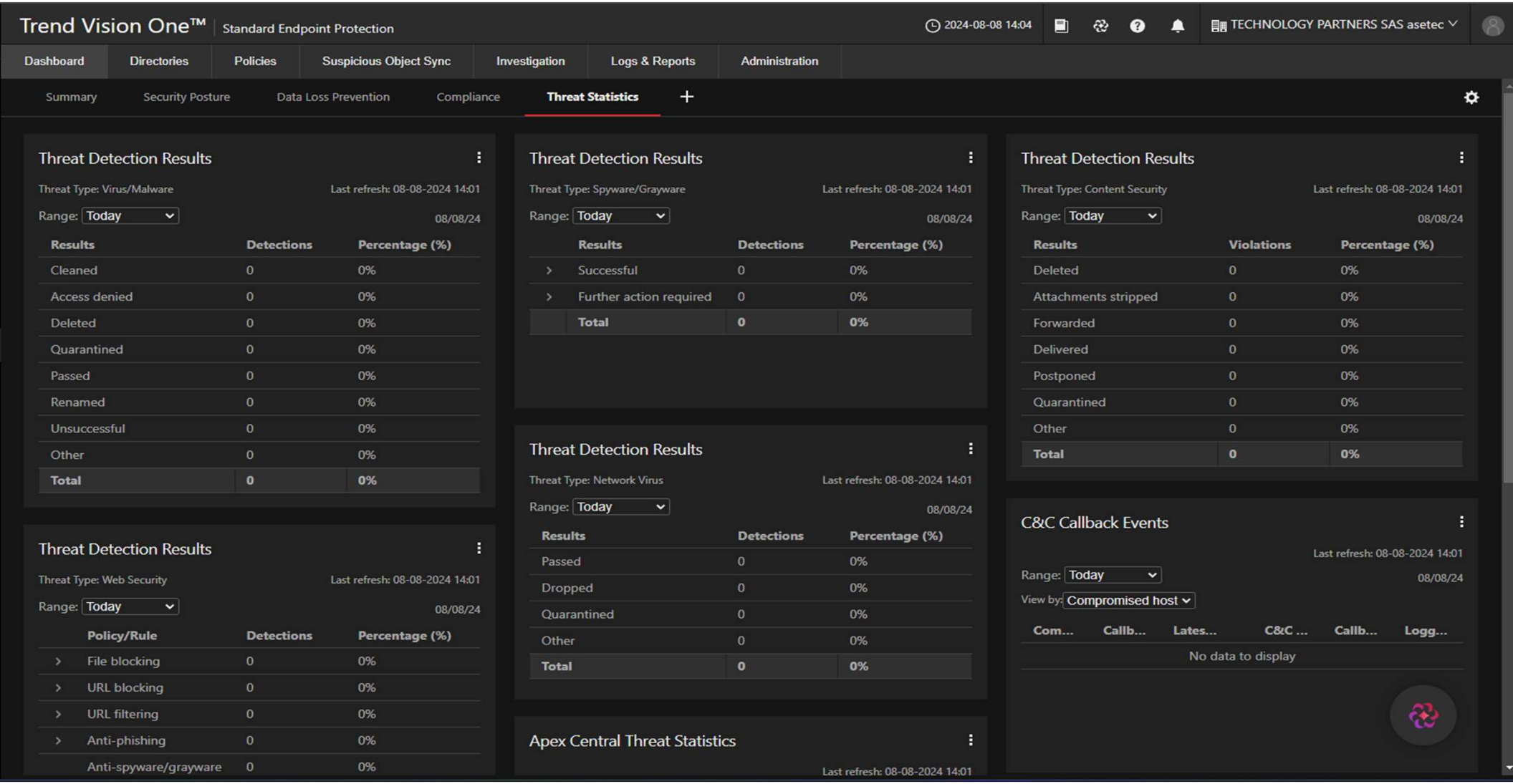
# Dashboard – Data los Prevention



# Dashboard – Compliance



# Dashboard – Threat Statistics



# Dashboard – Add Widgets - Customization

Trend Vision One™ | Standard Endpoint Protection

2024-08-08 14:07 | TECHNOLOGY PARTNERS SAS asetec

Dashboard | Directories | Policies | Suspicious Object Sync | Investigation | Logs & Reports | Administration

Add Widgets

All Widgets (33)

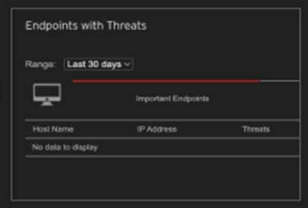
Search

- Most Recent Widgets (26)
- All Widgets (33)
- Compliance (4)
- Data Discovery (4)
- Data Loss Prevention (7)
- Apex One (5)
- Threat Statistics (11)
- Apex Central (16)
- Apex One (Mac) (1)

**Critical Threats**

Critical threats that require immediate attention and the users affected by these threats.

Apex Central
07/31/2024




**Endpoints with Threats**

Endpoints that require attention based on the threats that are found on the endpoints.

Apex Central
07/31/2024



**Operation Center**

Operation Center

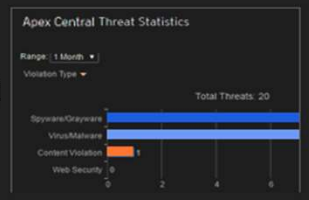
Apex Central
07/31/2024




**Ransomware Prevention**

Ransomware threat summary for users and endpoints across the network.

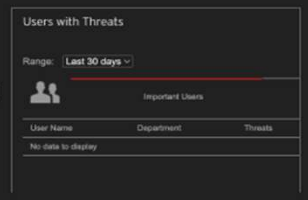
Apex Central
07/31/2024




**Apex Central Threat Statistics**

Displays the number of threat detections and the ratio of threats compared to the total number of detections by violation type or managed product type.

Apex Central, Threat Statistics



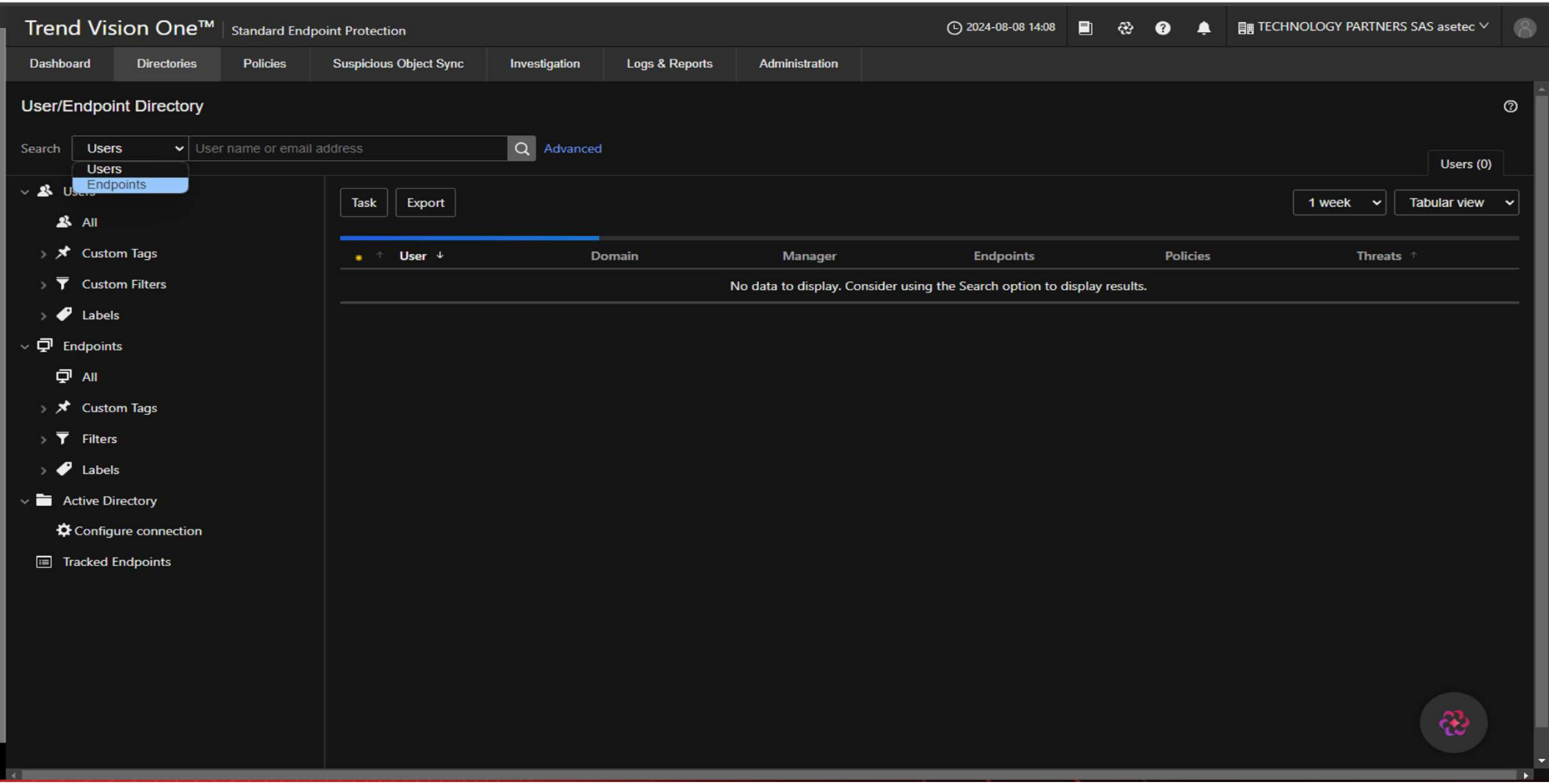

**Users with Threats**

Users that require attention based on the threats that are found on the user's endpoints and outside threats that affect them.

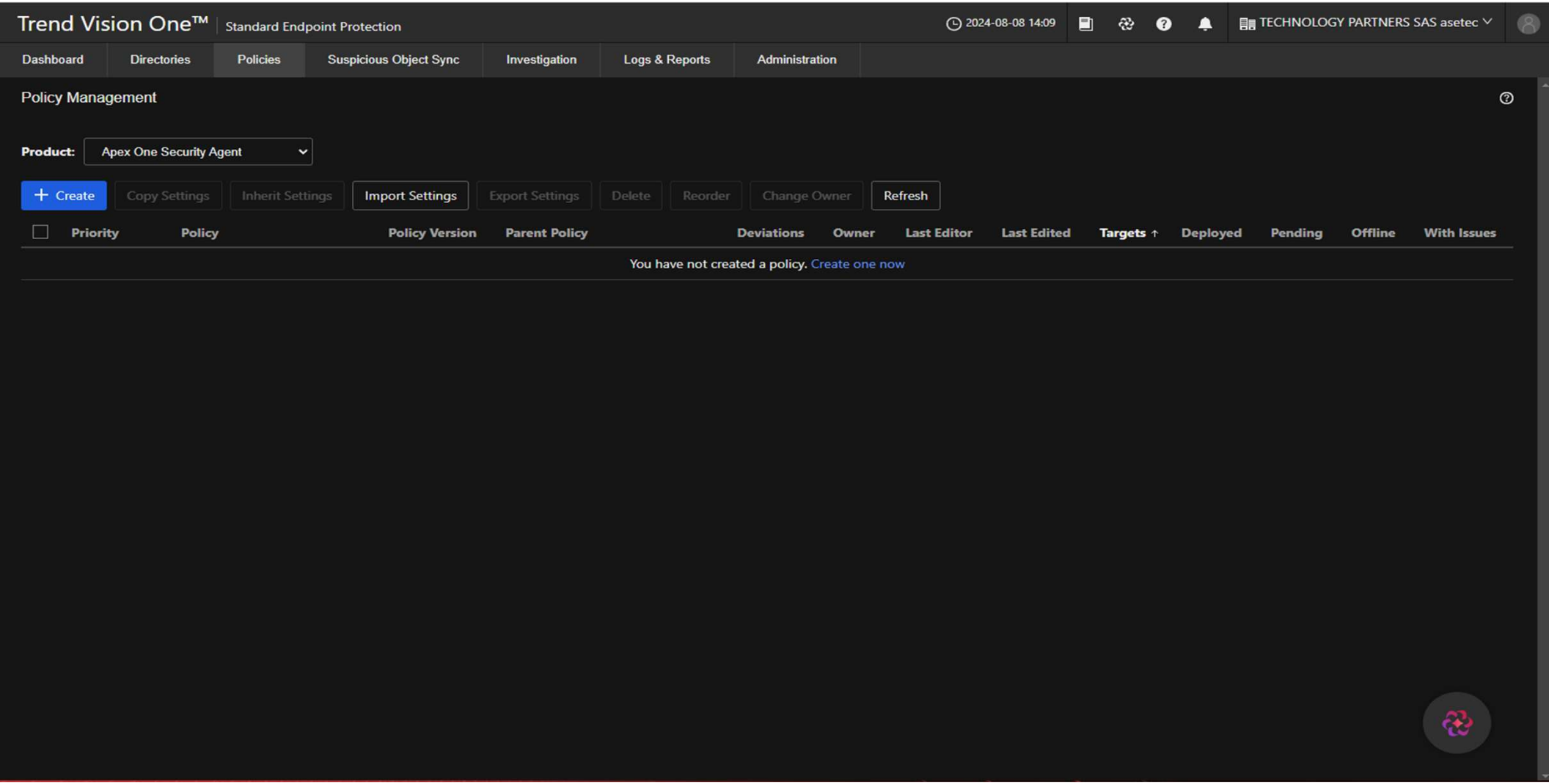
Apex Central

Add (0) | Cancel

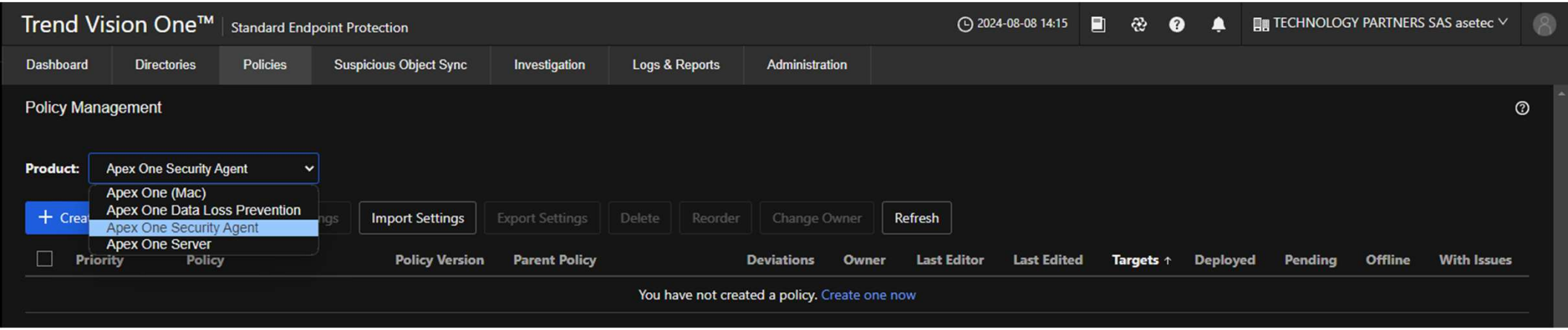
# Directories



# Policies


Trend Vision One™
Standard Endpoint Protection
2024-08-08 14:09
TECHNOLOGY PARTNERS SAS asetec
Dashboard
Directories
Policies
Suspicious Object Sync
Investigation
Logs & Reports
Administration
Policy Management
Product:
Apex One Security Agent
+ Create
Copy Settings
Inherit Settings
Import Settings
Export Settings
Delete
Reorder
Change Owner
Refresh
Priority
Policy
Policy Version
Parent Policy
Deviations
Owner
Last Editor
Last Edited
Targets
Deployed
Pending
Offline
With Issues
You have not created a policy. Create one now

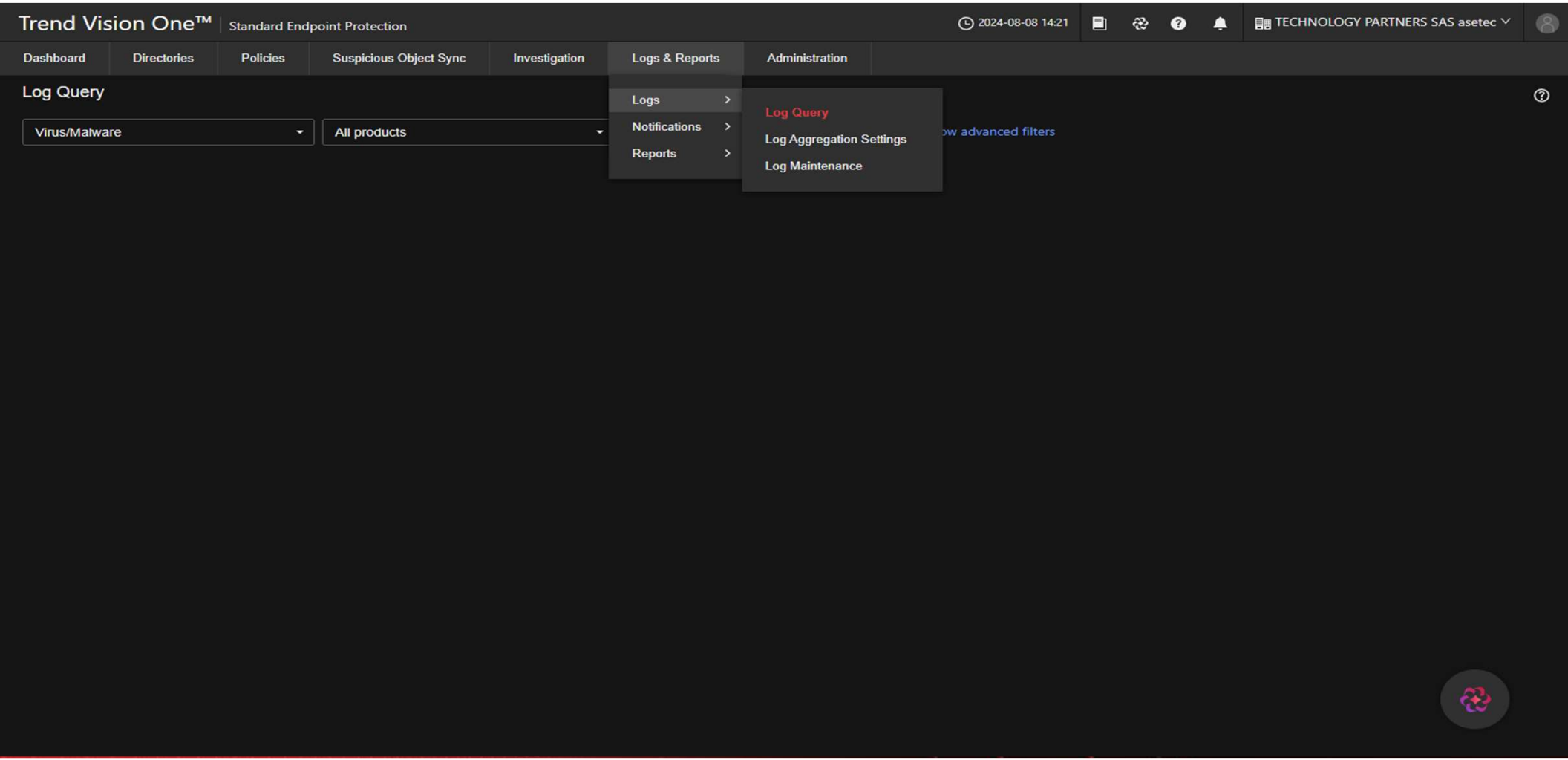
# Policies



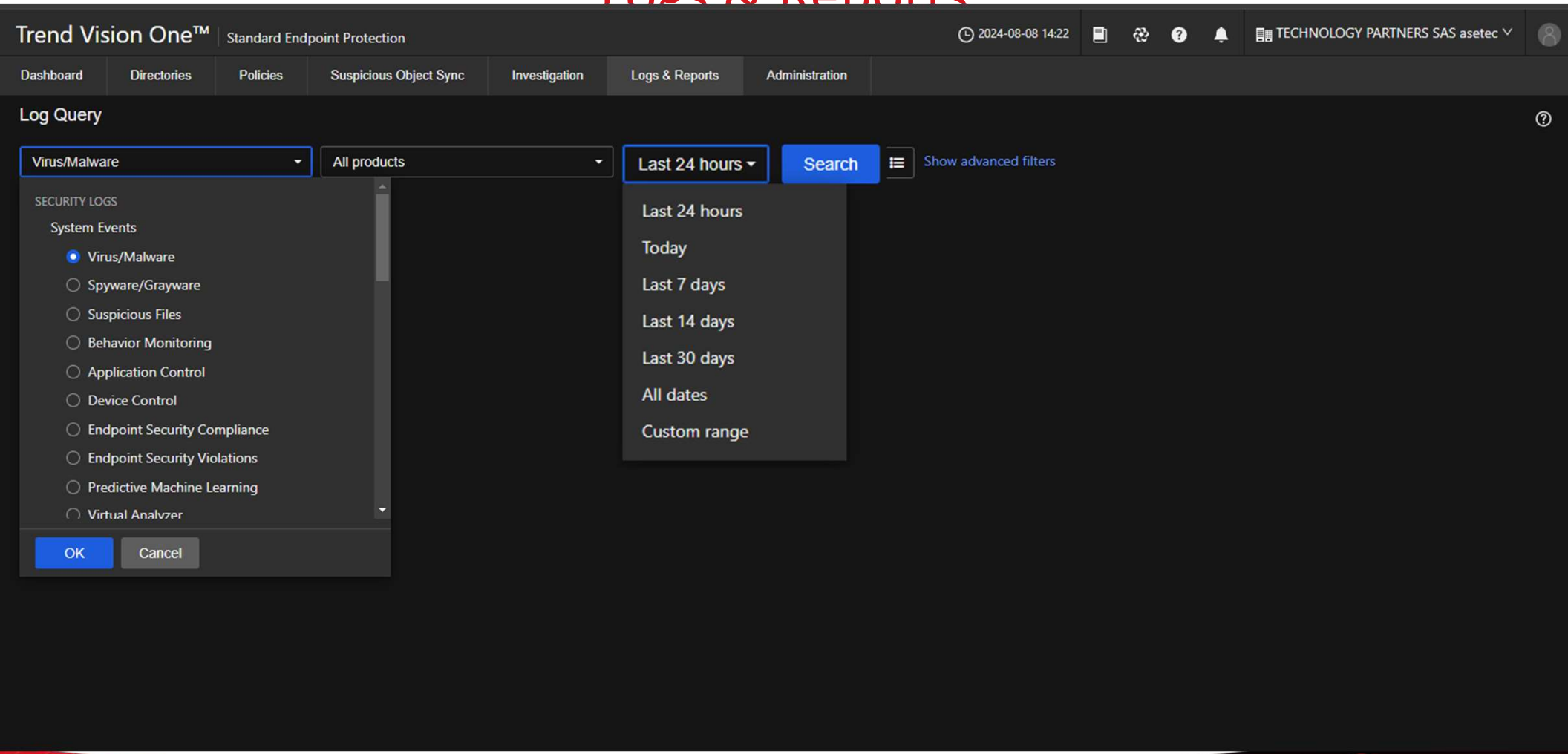

SE PUEDEN AGREGAR 4 TIPOS DE POLÍTICAS

1. APEX ONE SECURITY AGENTS (WINDOWS)
2. APEX ONE (MAC)
3. APEX ONE DATA LOSS PREVENTION
4. APEX ONE SERVER

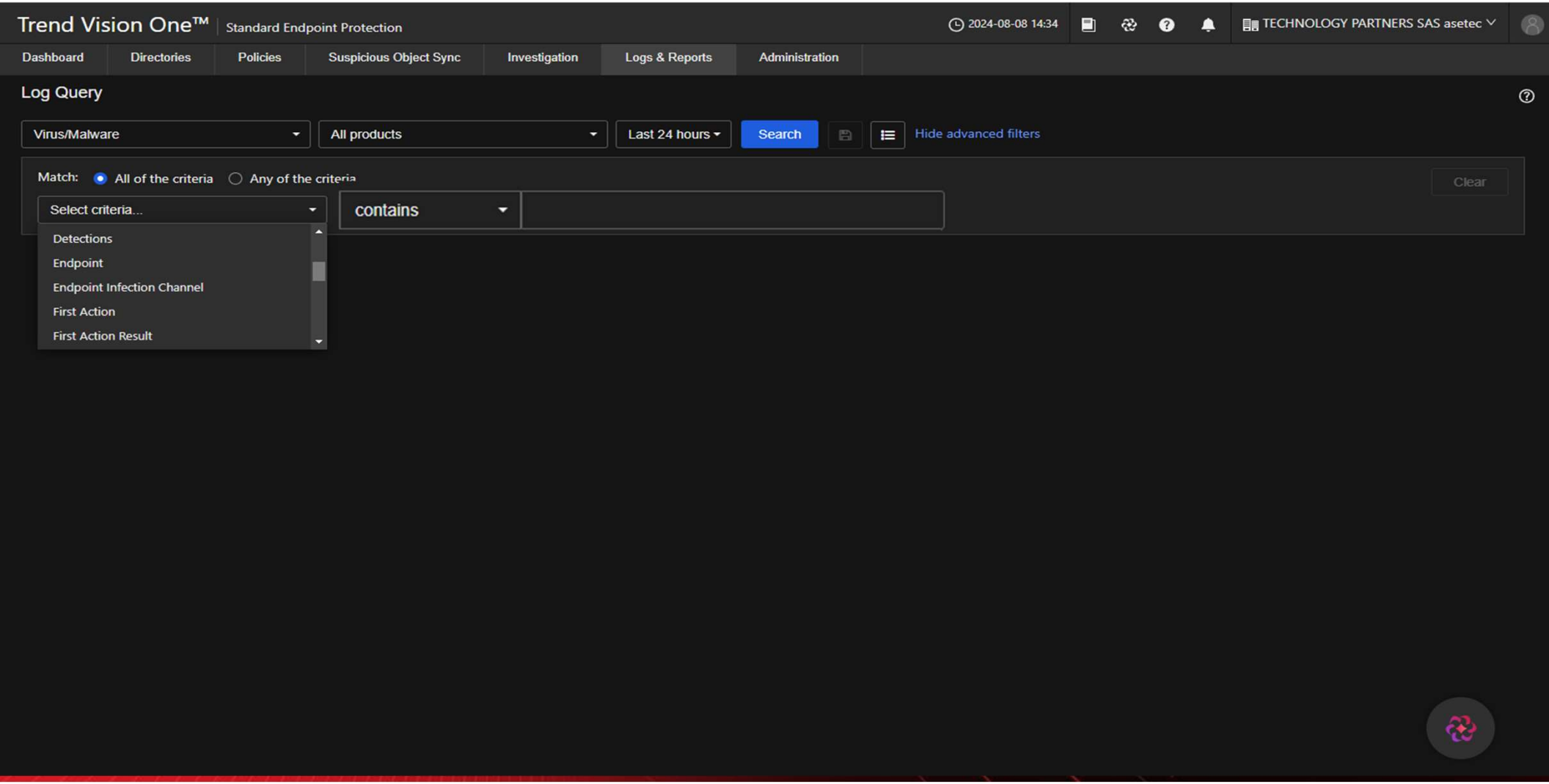
# Logs & Reports



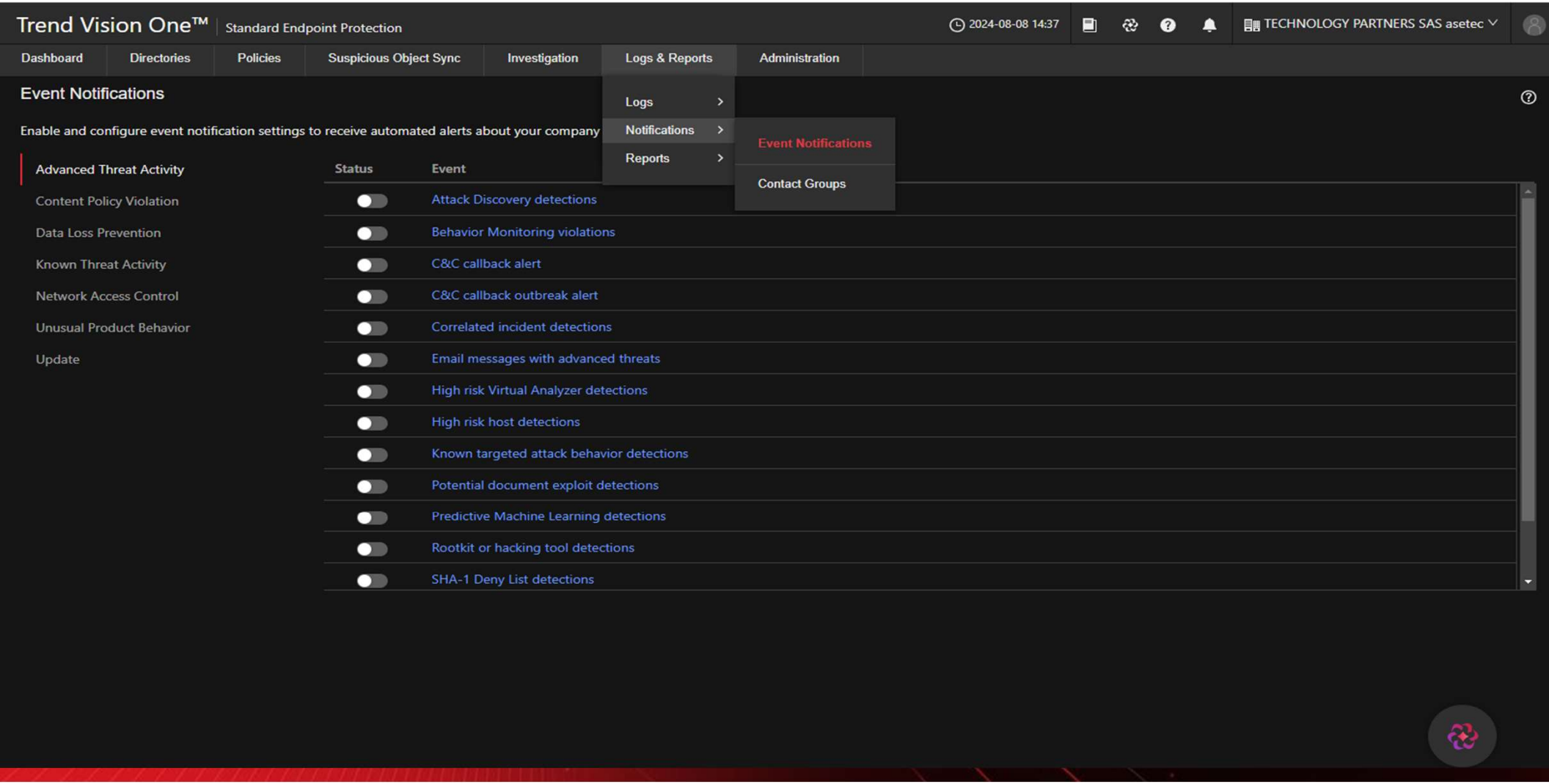
# Logs & Reports



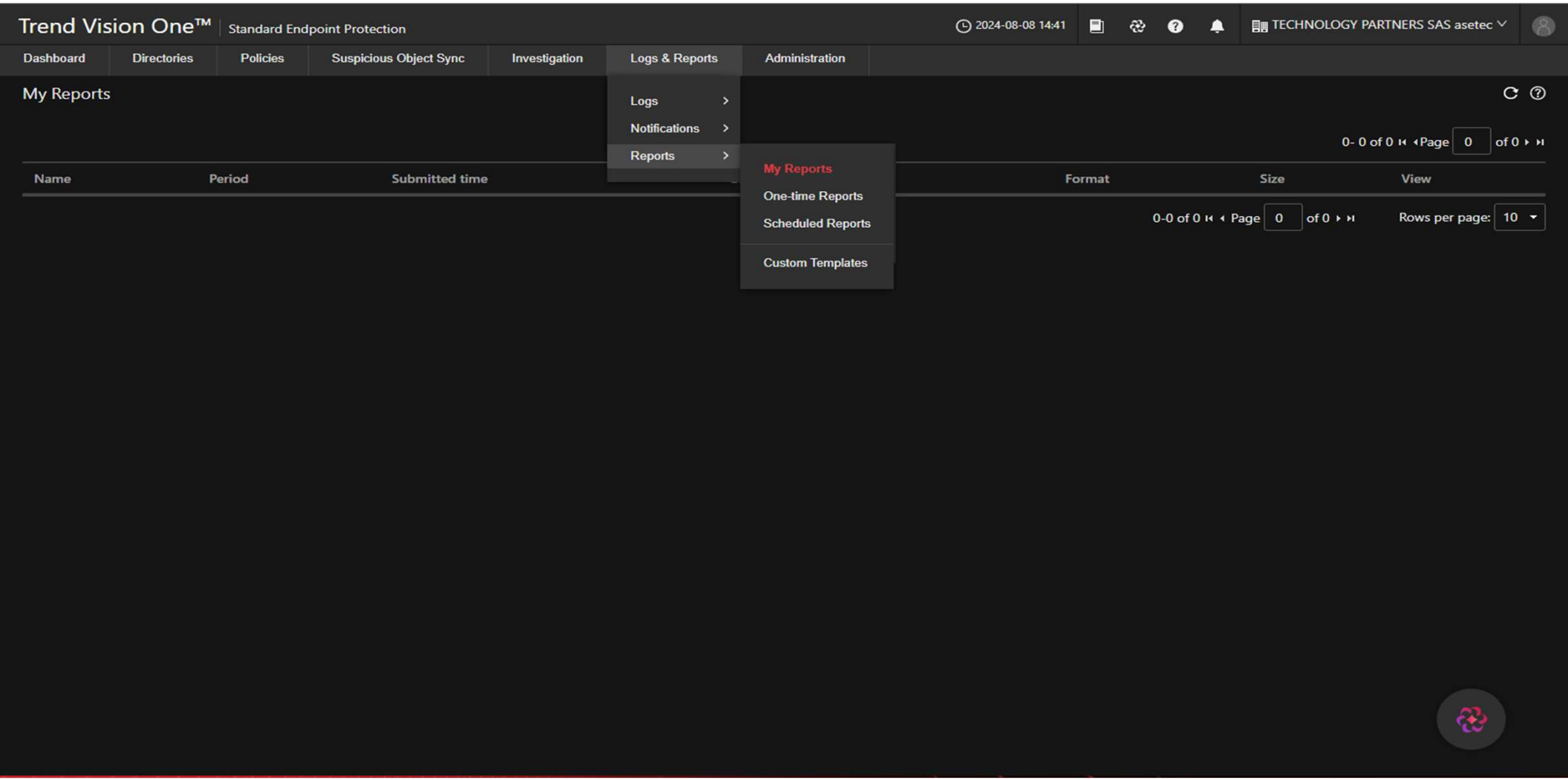
# Logs & Reports



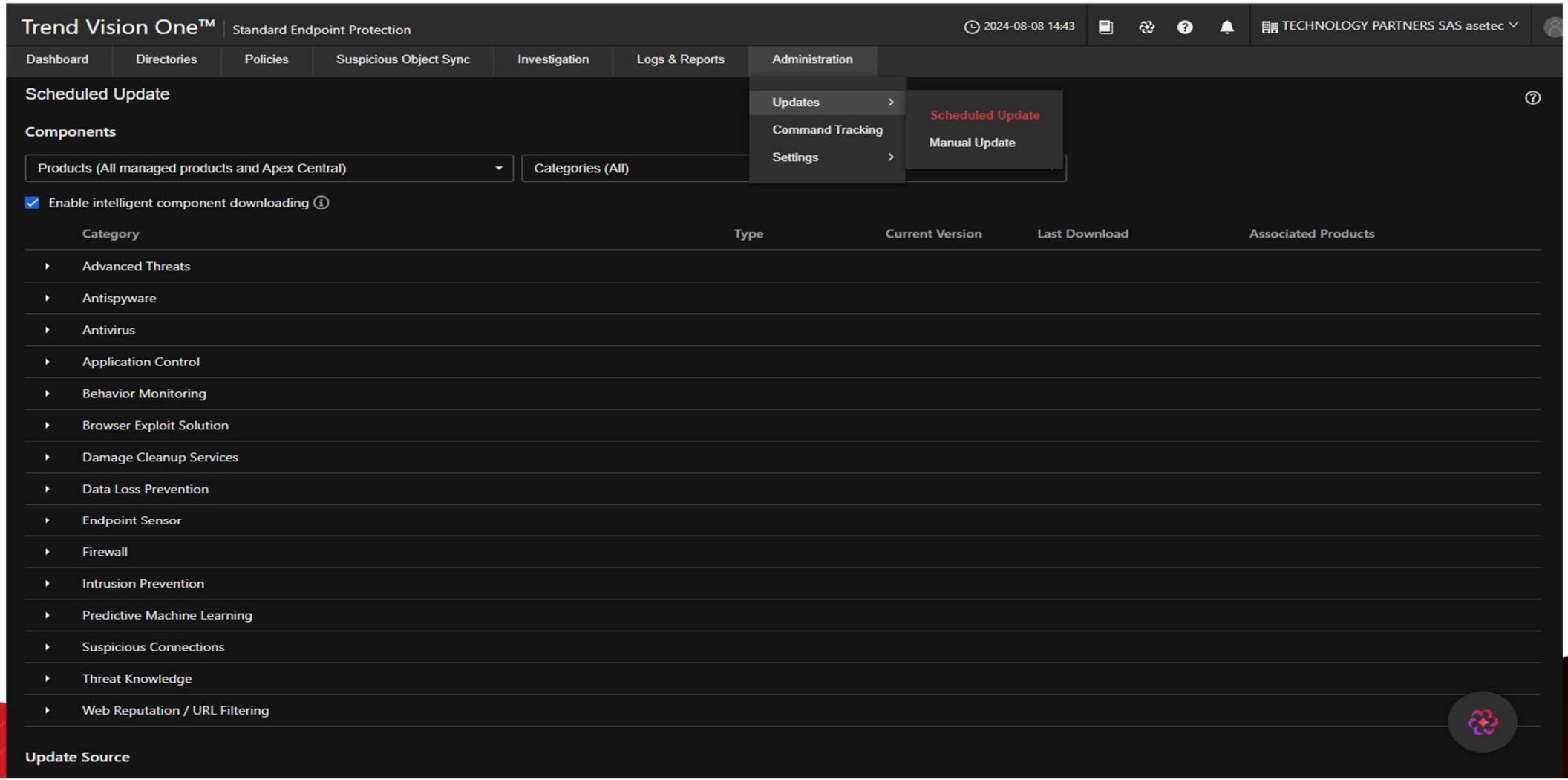
# Logs & Reports – Event Notifications



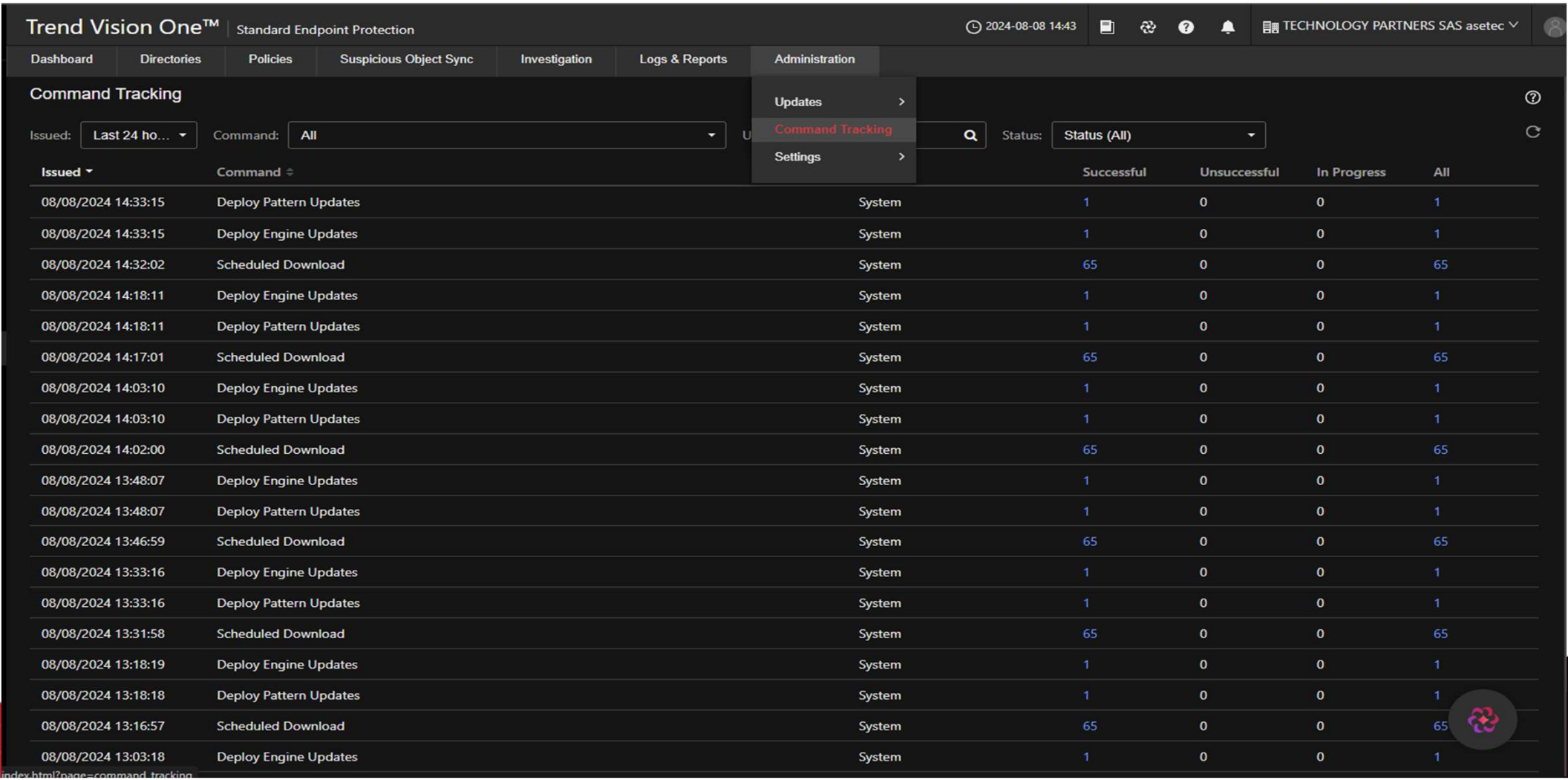
# Logs & Reports – My Reports *



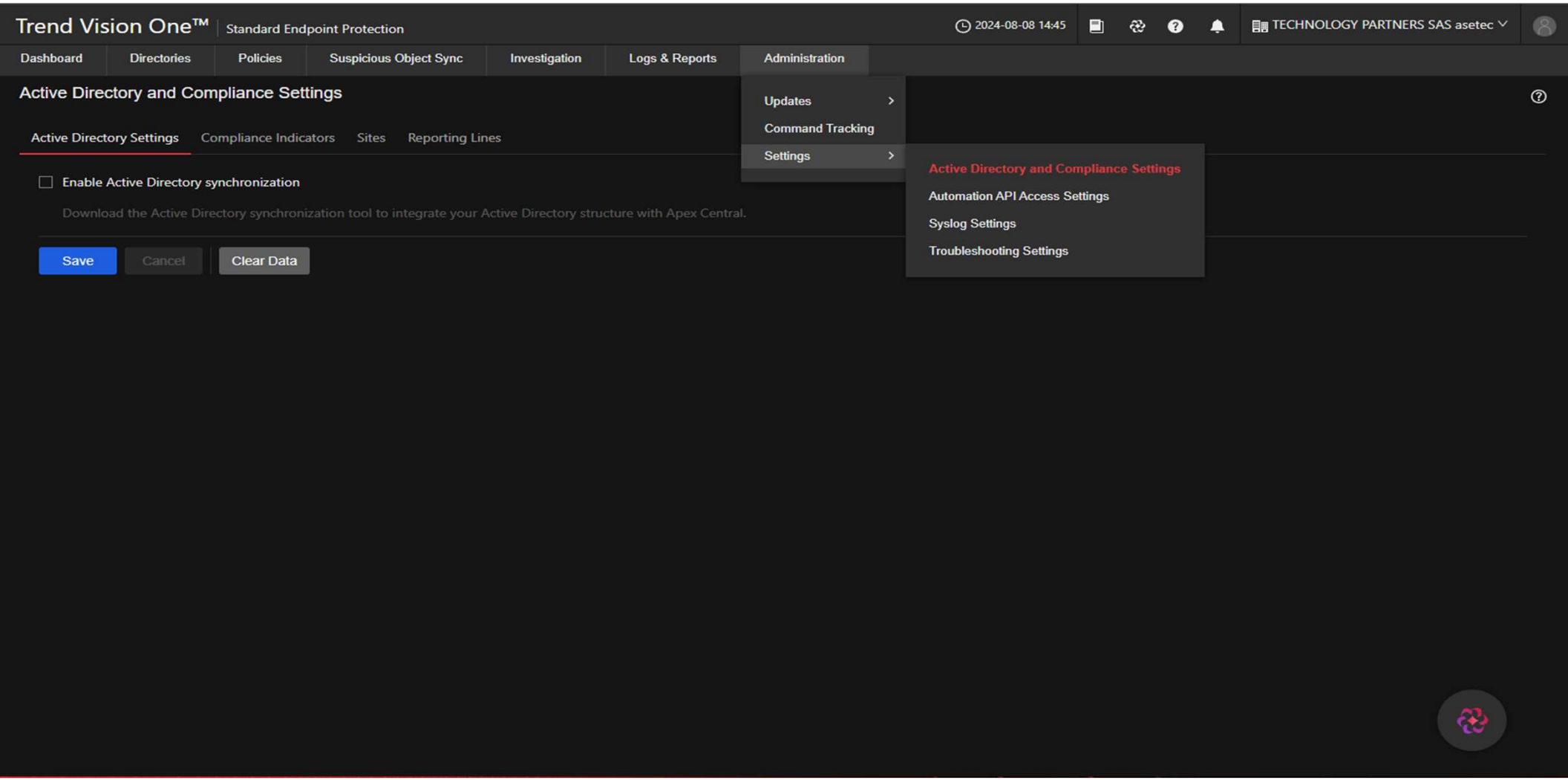
# Administration - Updates



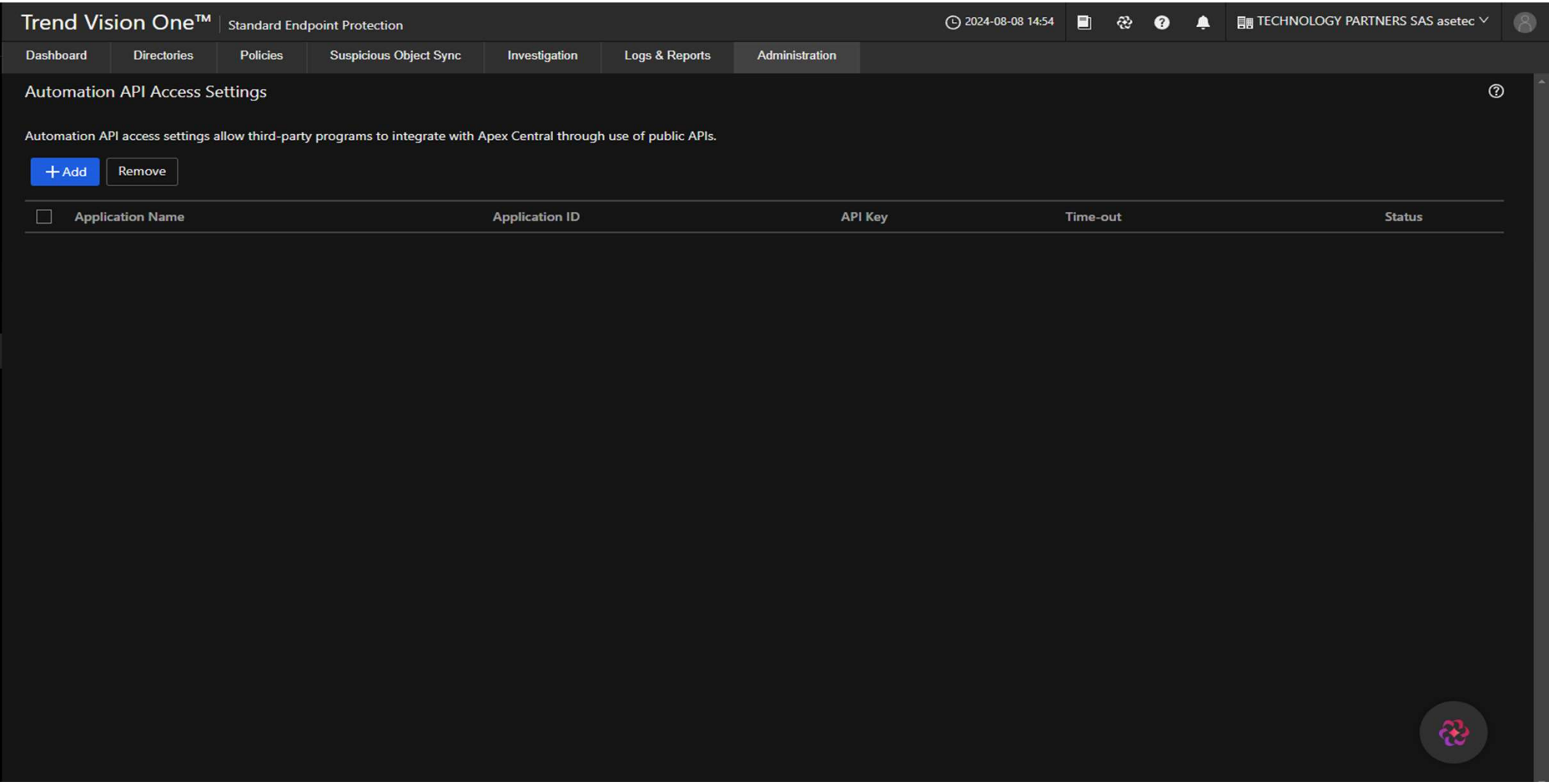
# Administration – Command Tracking



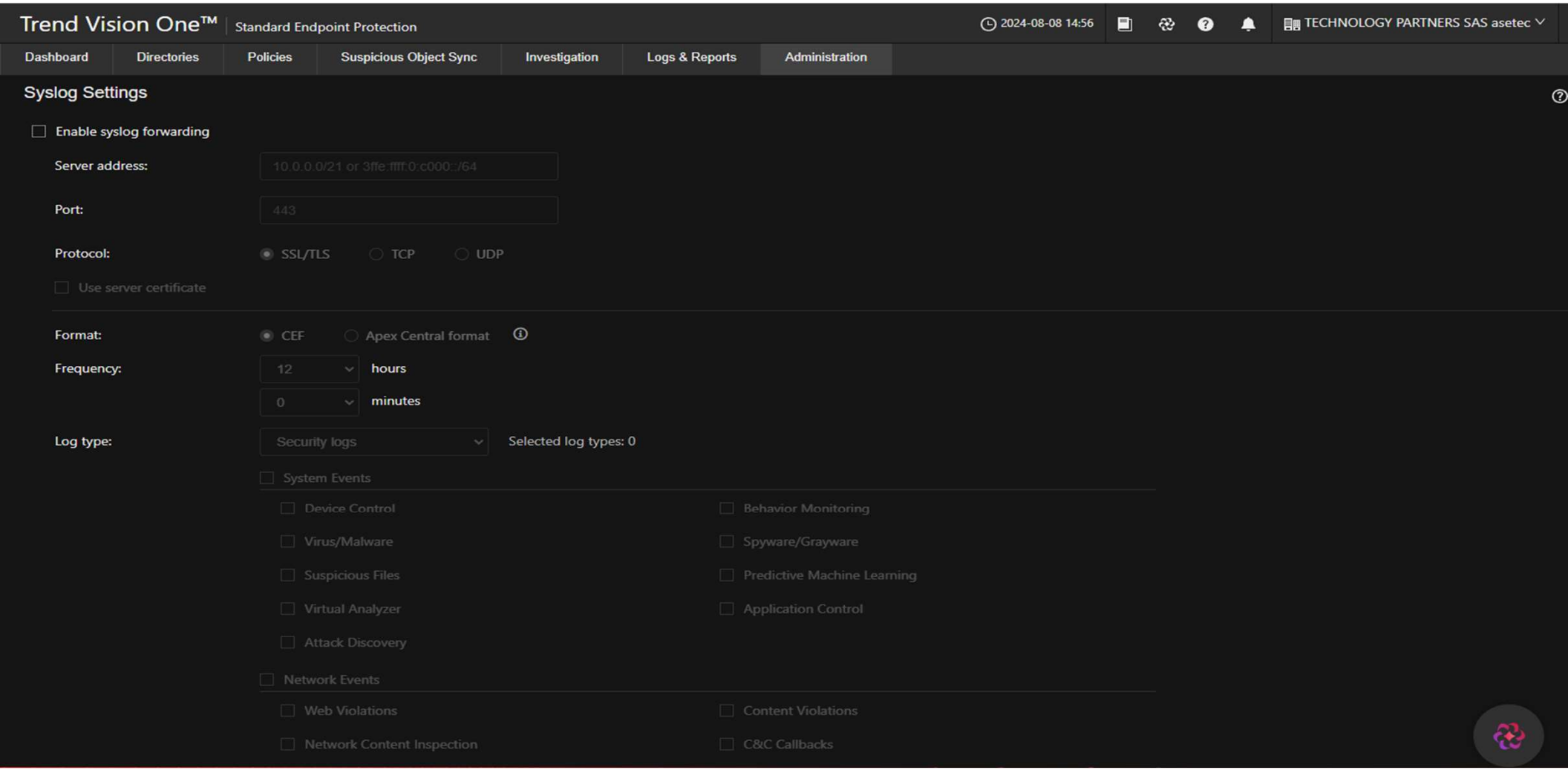
# Administration – AD and Compliance Settings



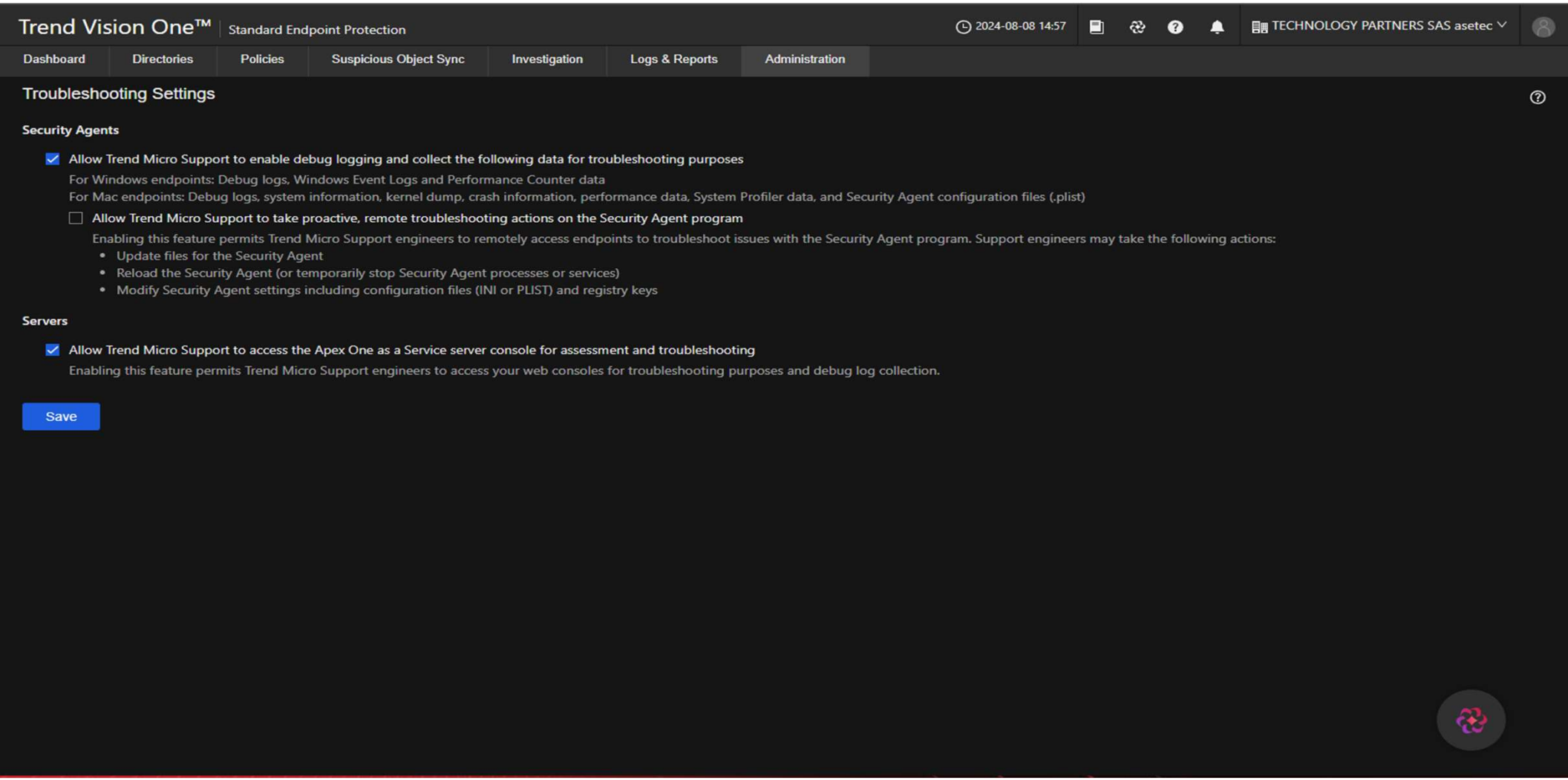
# Administration – Automation api Access Settings



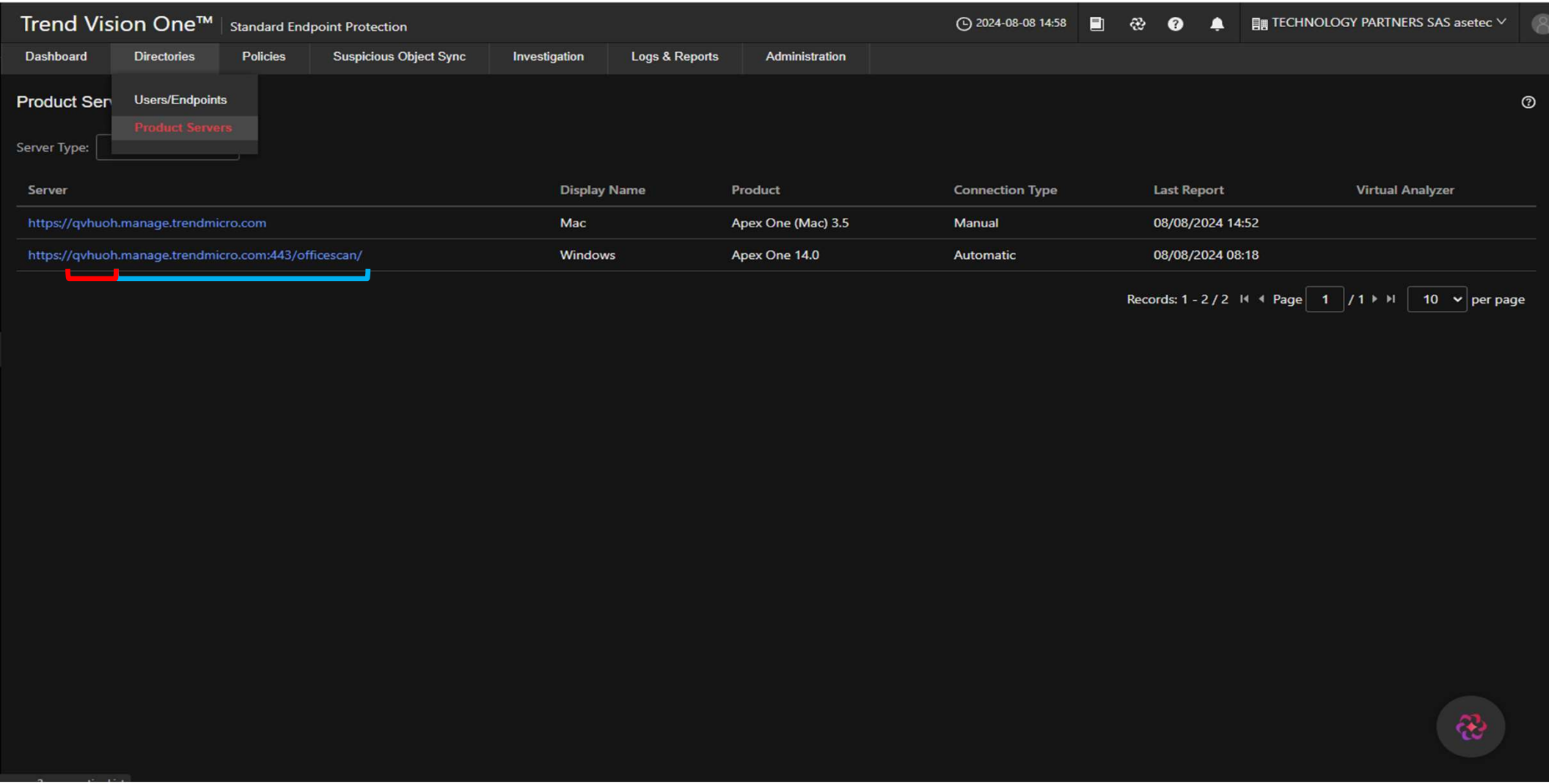
# Administration – Syslog Settings



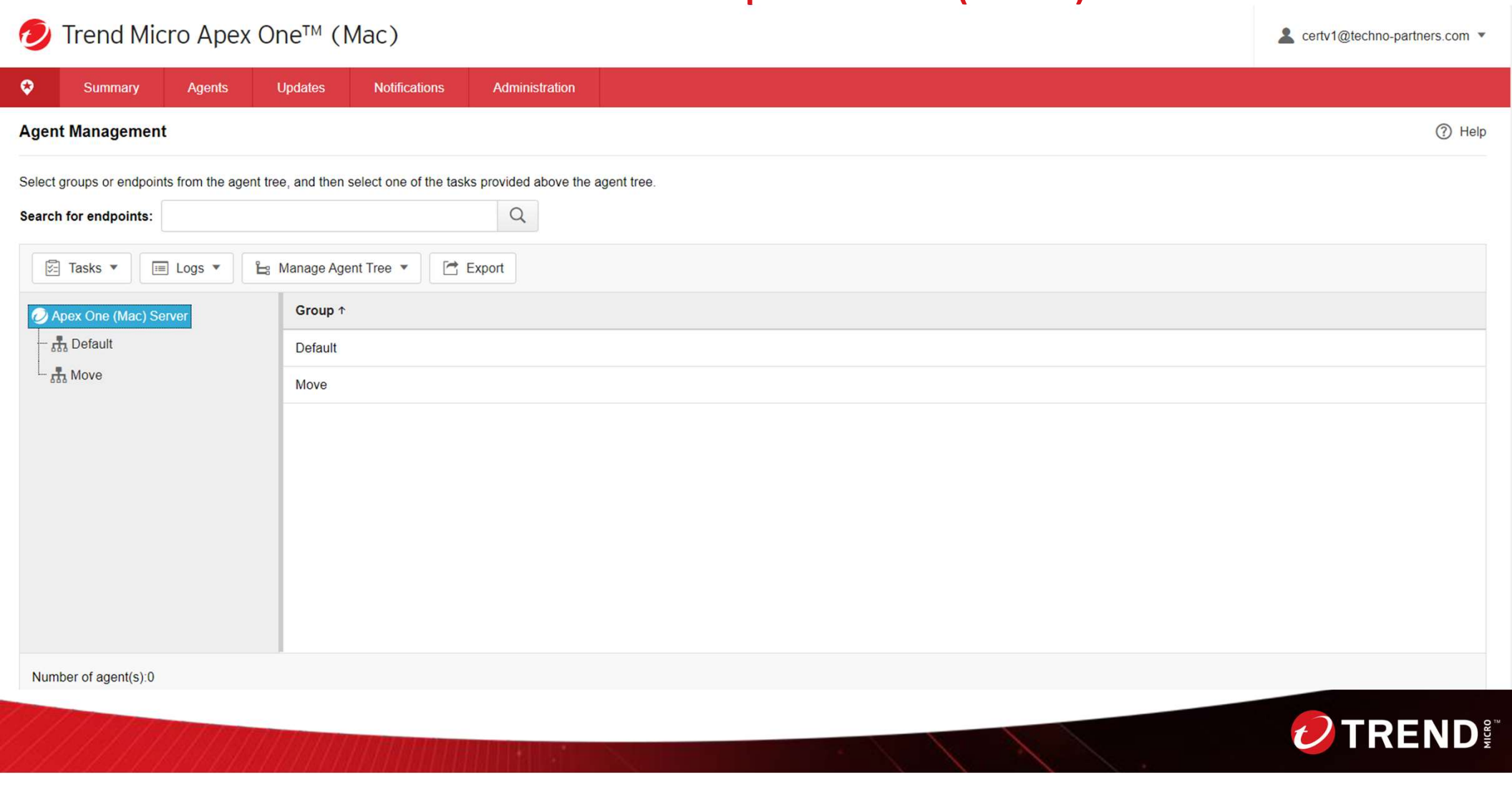
# Administration – Troubleshooting Settings



# Directories – Product Servers



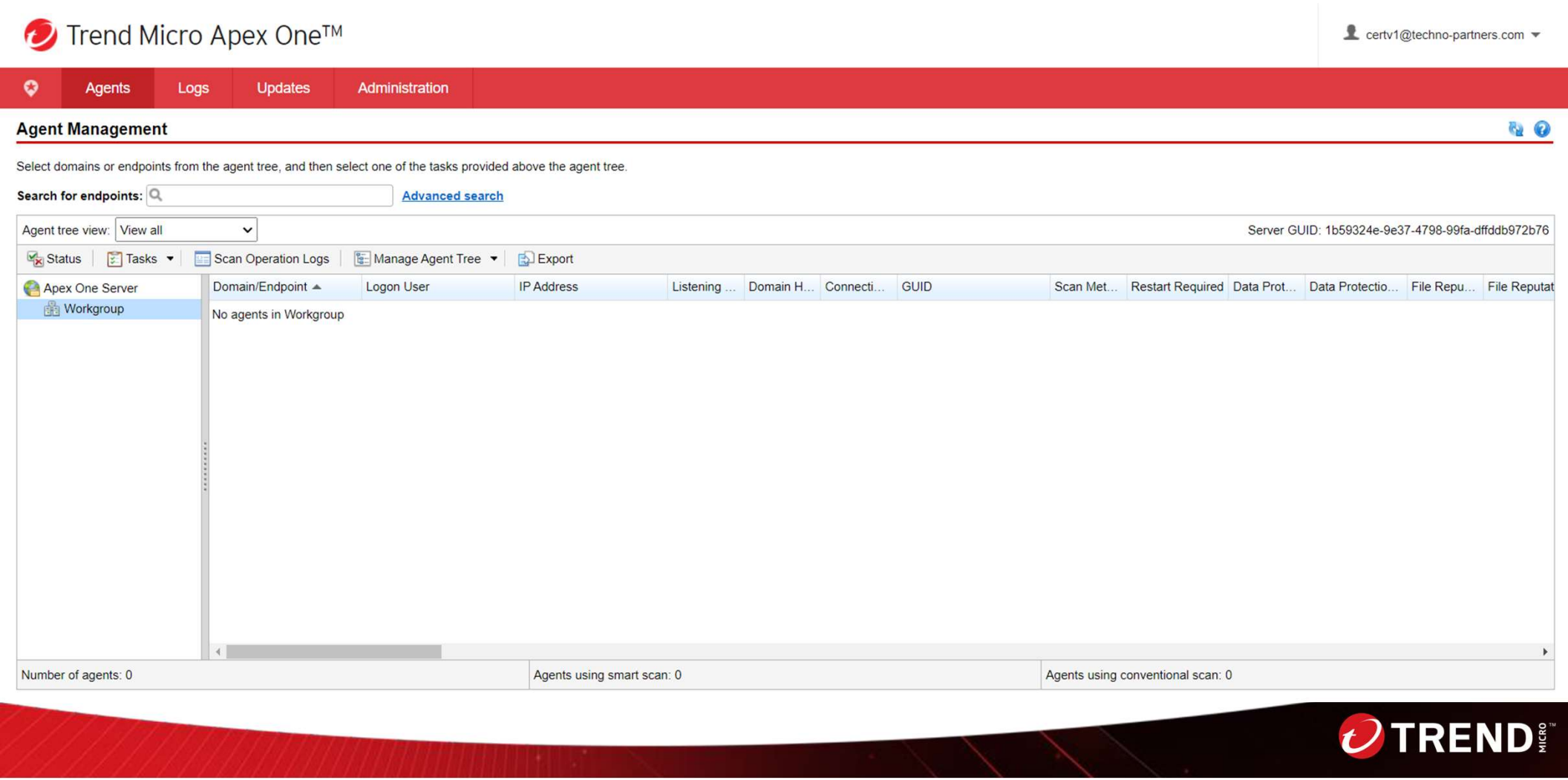
# Trendmicro Apex One (Mac)



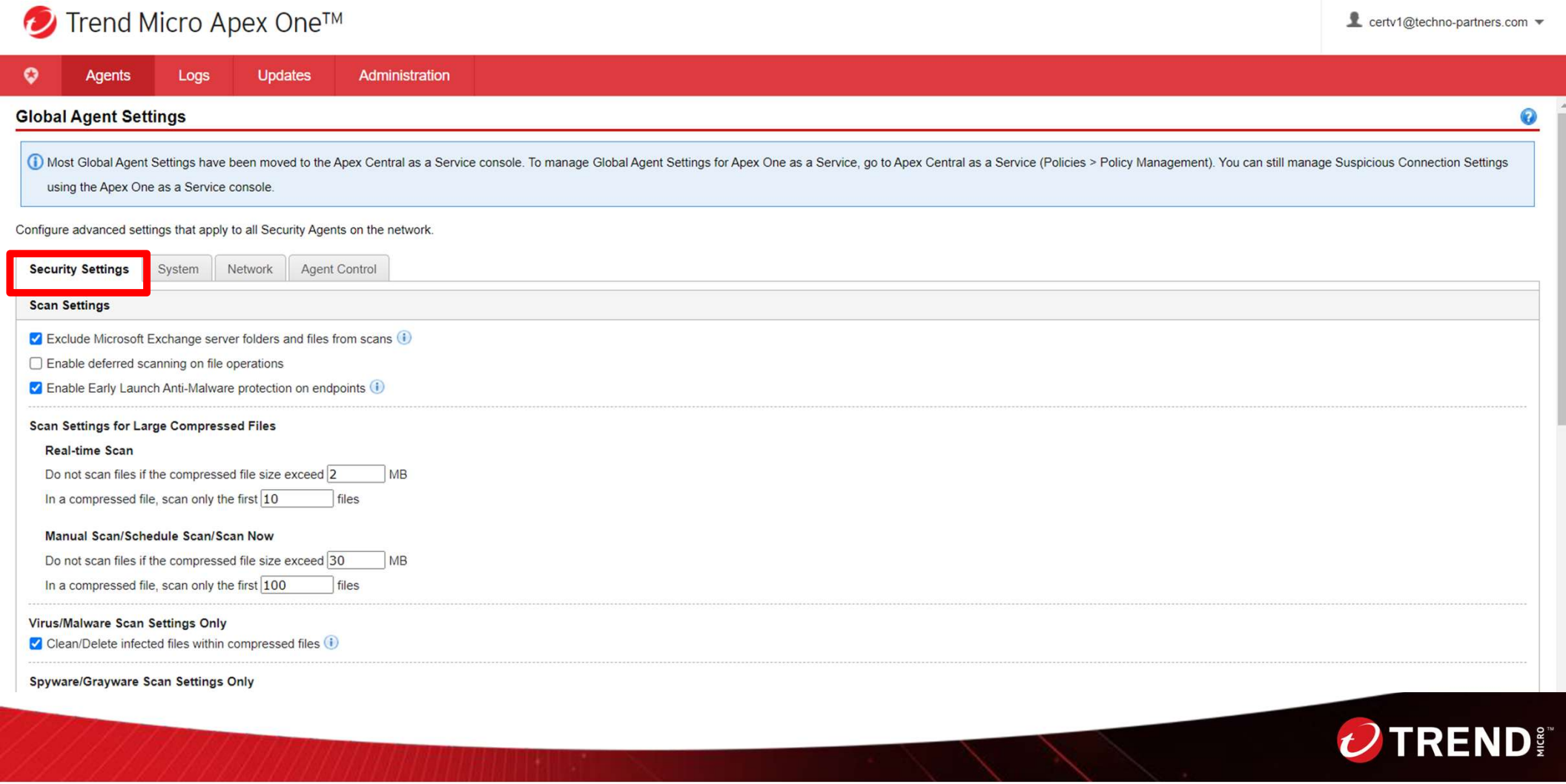
# Trendmicro Apex One – Favoritos



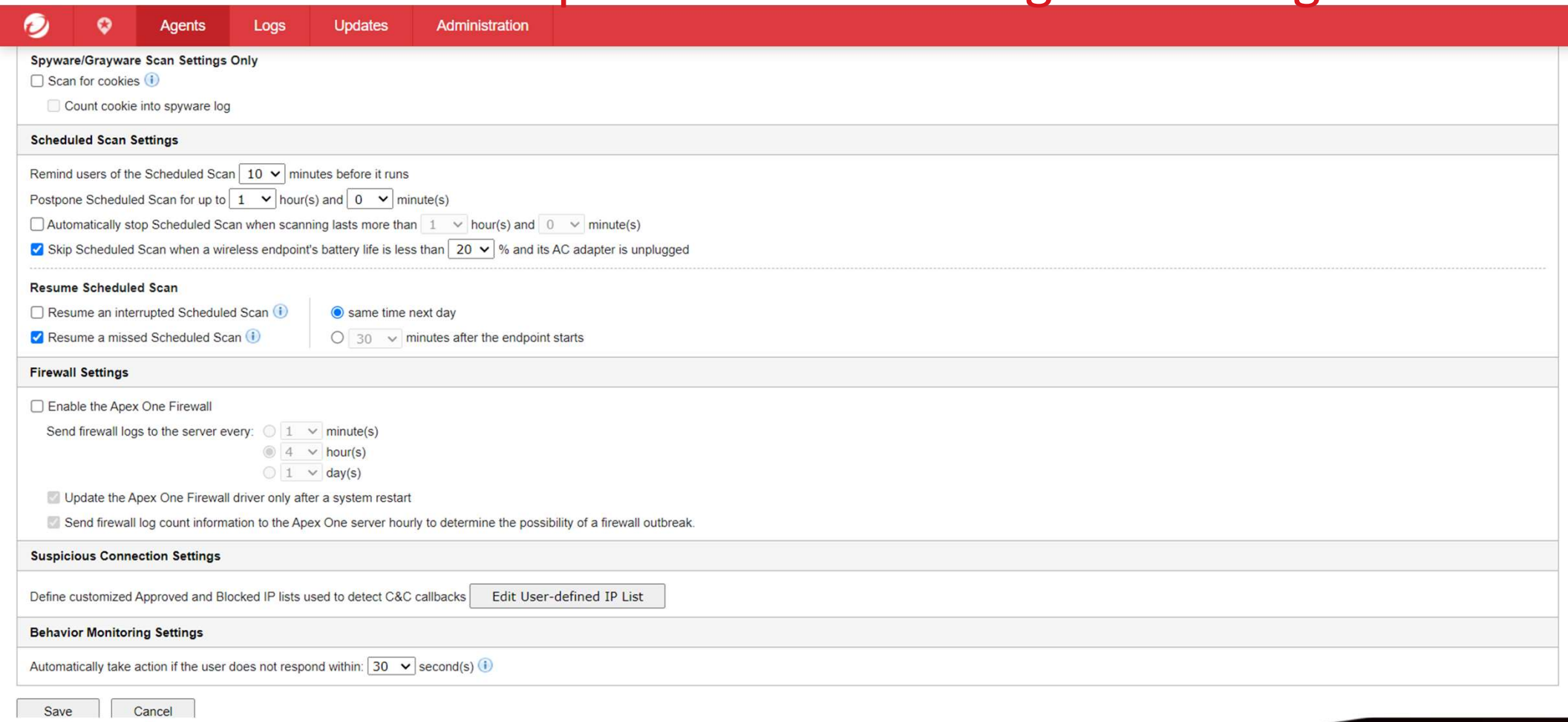
# Trendmicro Apex One – Agent Management



# Trendmicro Apex One – Global Agent Settings



# Trendmicro Apex One – Global Agent Settings



# Trendmicro Apex One – Global Agent Settings

Security Settings | **System** | Network | Agent Control

**Certified Safe Software Service Settings**

☑ Enable the Certified Safe Software Service for Behavior Monitoring, Firewall, and antivirus scans

**Smart Protection Service Proxy**

☐ Use configured Smart Protection Sources for service queries

The service proxy is used by the following features:

- Predictive Machine Learning
- Behavior Monitoring

Note: If a supported Smart Protection Server is not available for service proxy queries, agents send query requests directly to the Trend Micro Smart Protection Network.

**Services Restart**

☑ Automatically restart any Security Agent service if the service terminates unexpectedly

Restart the service after 1 minute(s)

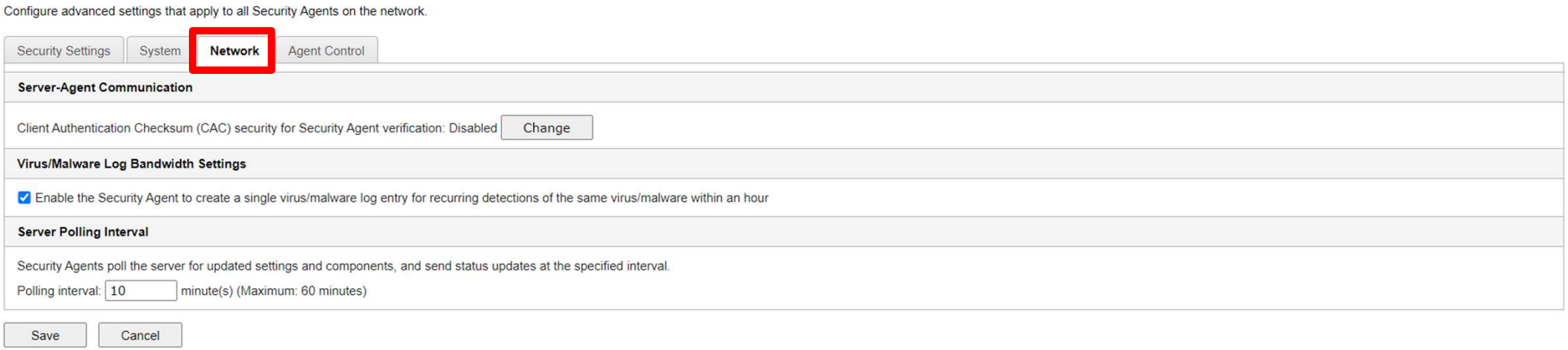
If the first attempt to restart the service is unsuccessful, retry 2 times

Reset the unsuccessful restart count after 1 hour(s)

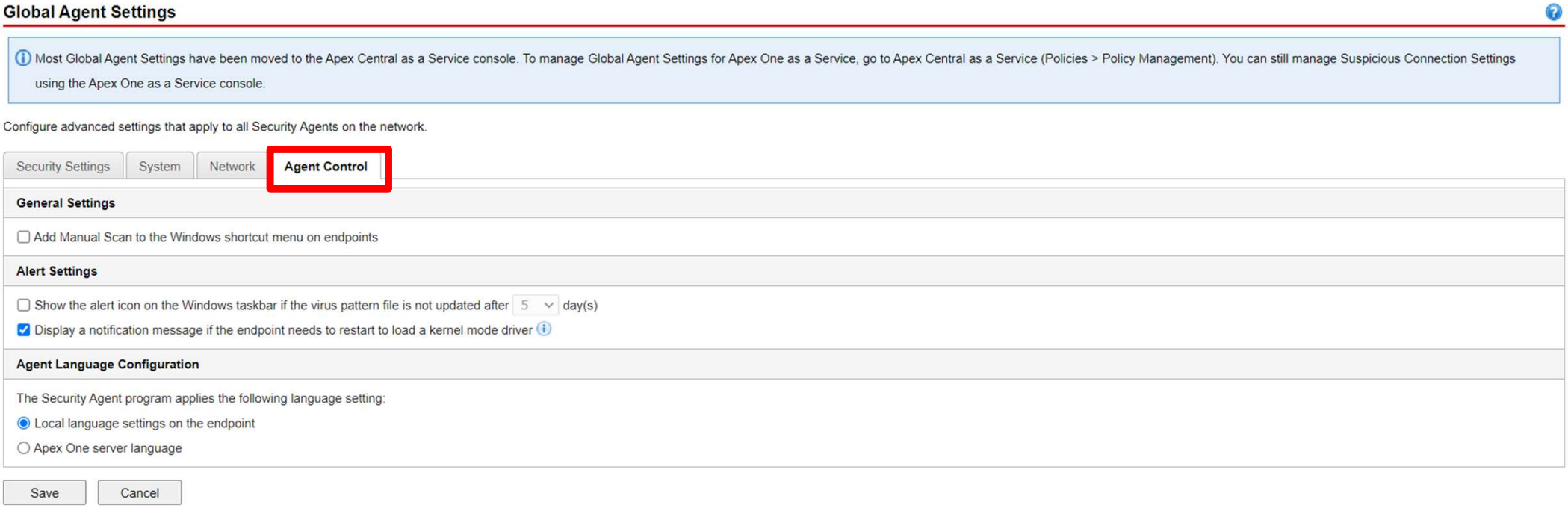
Save | Cancel

TREND MICRO

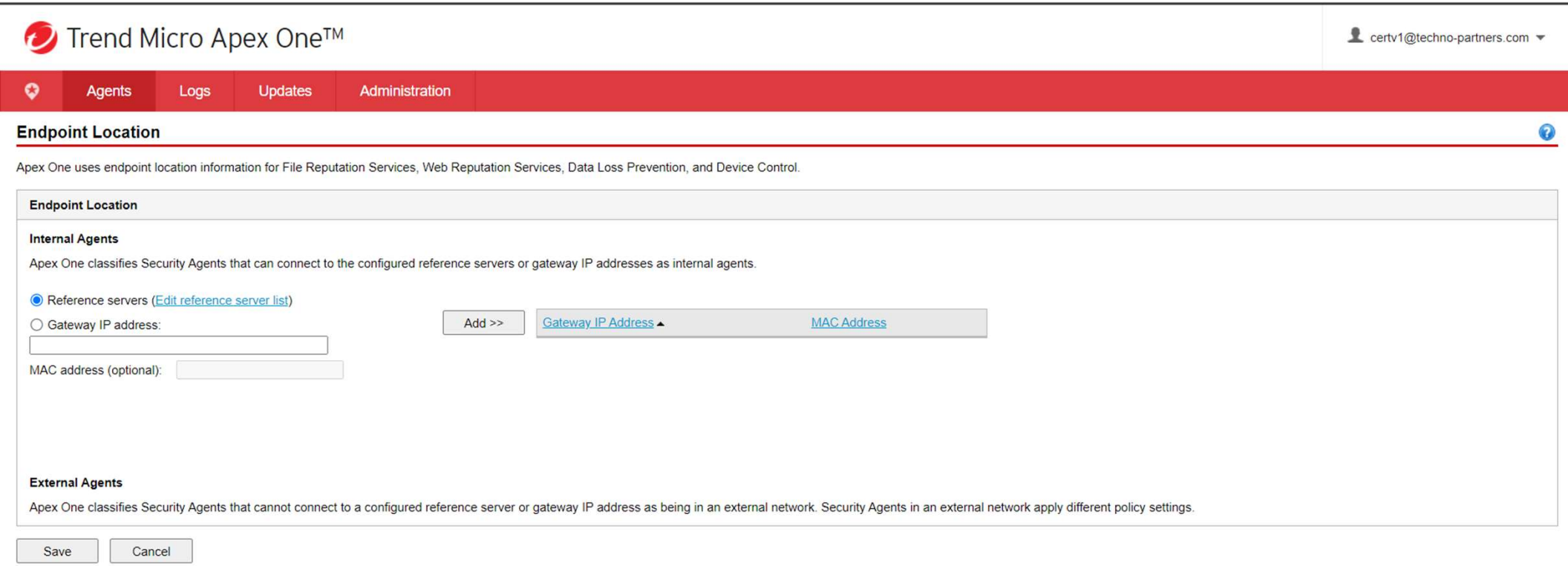
# Trendmicro Apex One – Global Agent Settings



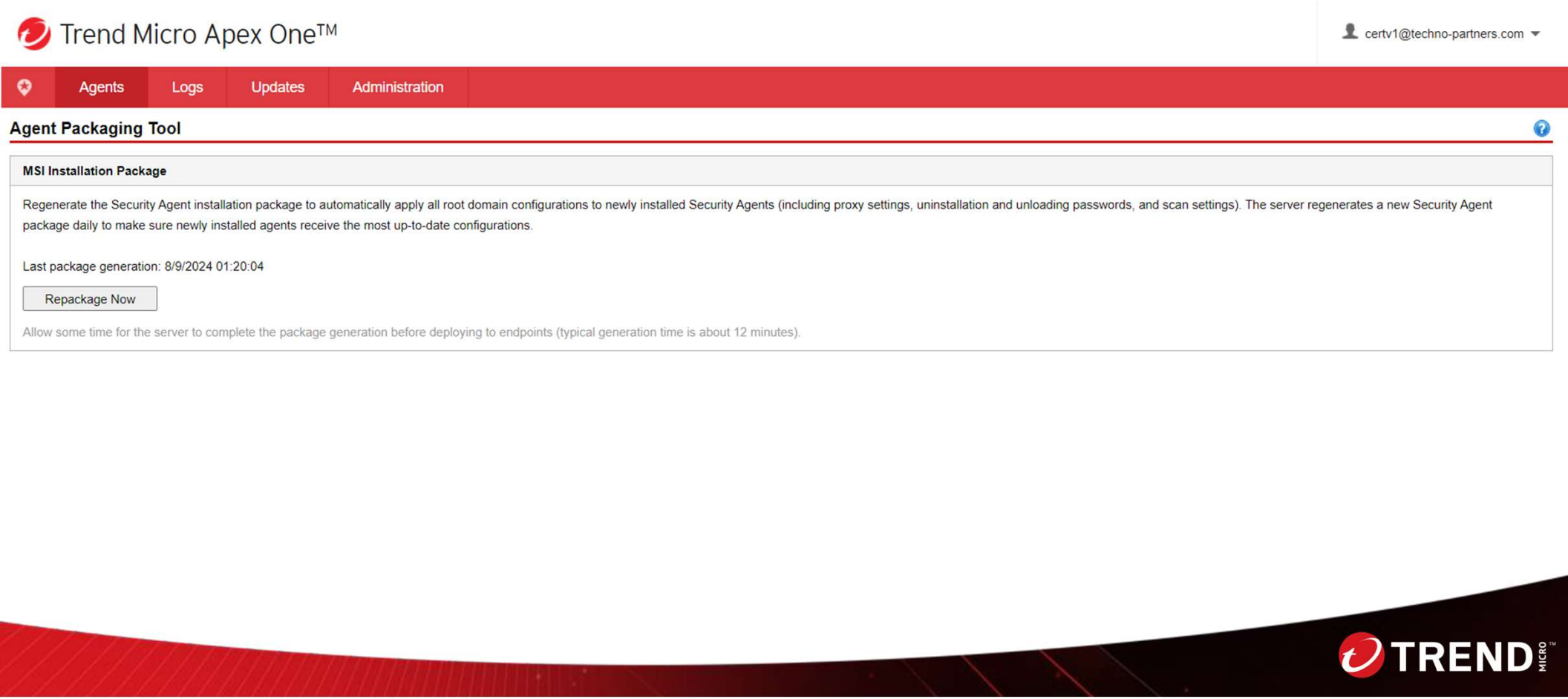
# Trendmicro Apex One – Global Agent Settings



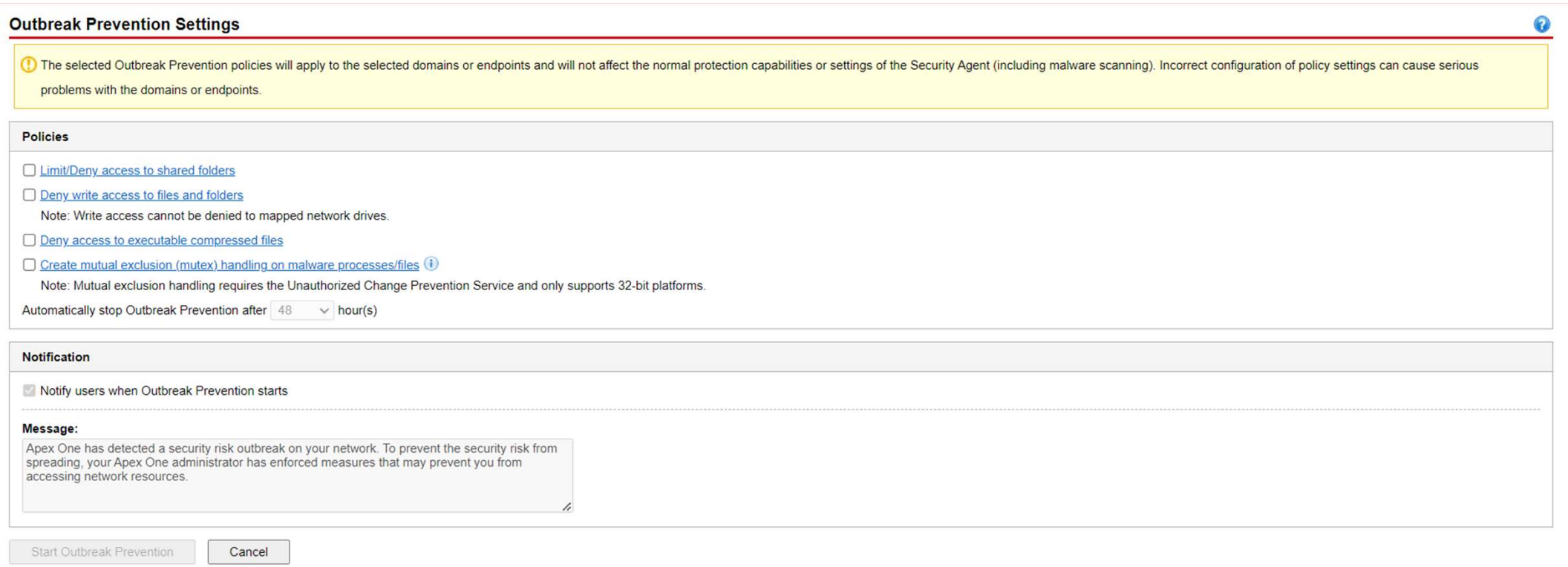
# Administration – Endpoint Location



# Administration – Agent Packaging Tool



# Administration – Agent Packaging Tool



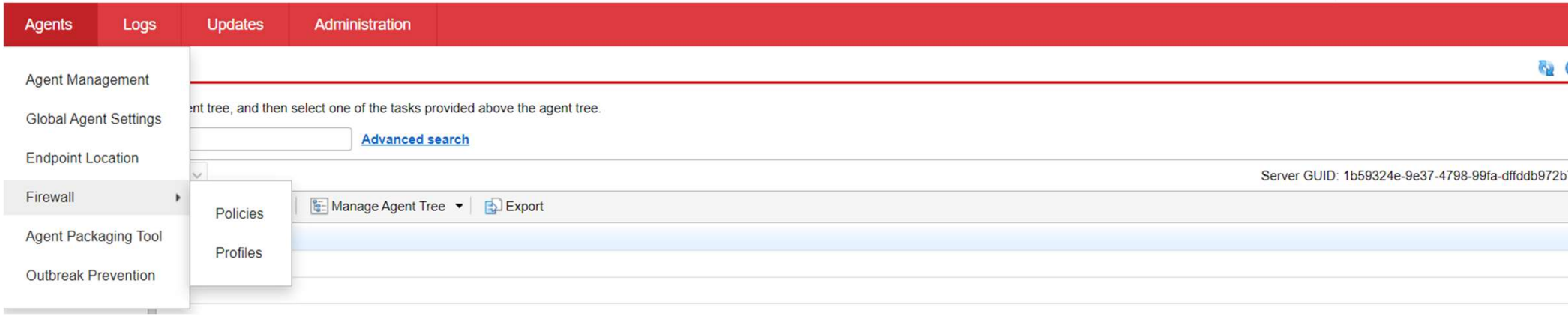
# Cortafuegos en Standard Enpoint Security Protection

Es mandatorio para usar y activar el cortafuegos de endpoint security standard ir a Agents – Global Agent – y en la pestaña security Settings hacer click en el apartado Firewall Settings - Enable the Apex One Firewall.



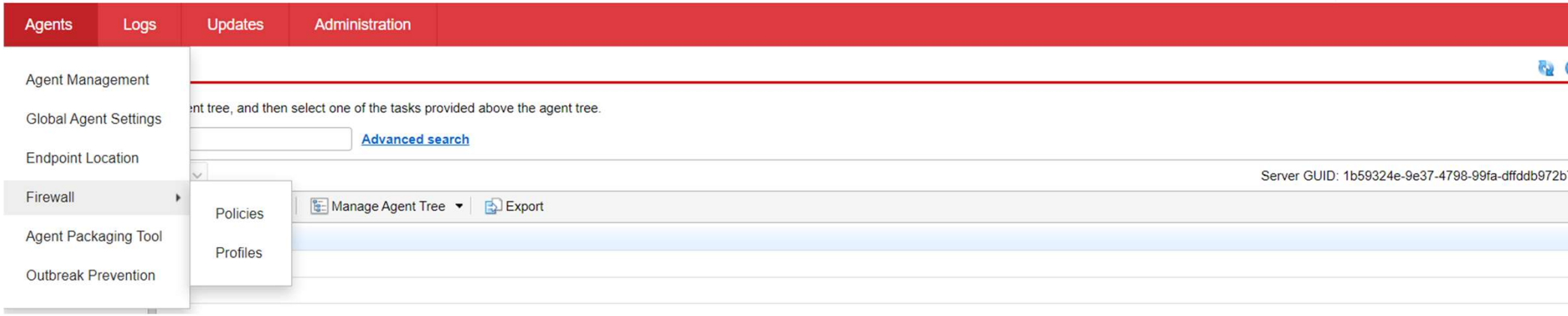
# Cortafuegos en Standard Enpoint Security Protection

Es mandatorio para usar y activar el cortafuegos de endpoint security standard ir a Agents – Global Agent – y en la pestaña security Settings hacer click en el apartado Firewall Settings - Enable the Apex One Firewall.



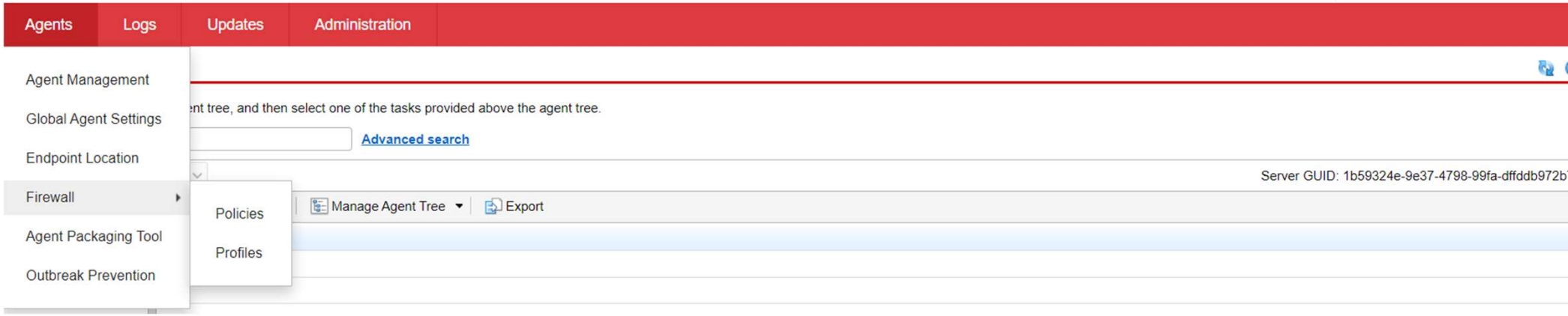
# Cortafuegos en Standard Enpoint Security Protection

Es mandatorio para usar y activar el cortafuegos de endpoint security standard ir a Agents – Global Agent – y en la pestaña security Settings hacer click en el apartado Firewall Settings - Enable the Apex One Firewall.



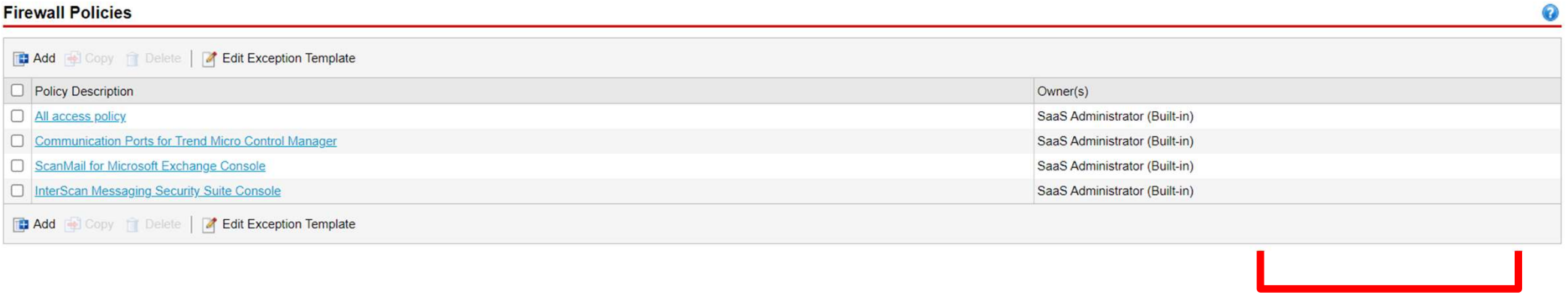
# Cortafuegos en Standard Enpoint Security Protection

Es mandatorio para usar y activar el cortafuegos de endpoint security standard ir a Agents – Global Agent – y en la pestaña security Settings hacer click en el apartado Firewall Settings - Enable the Apex One Firewall.



# Cortafuegos - Policies

Es mandatorio para usar y activar el cortafuegos de endpoint security standard ir a Agents – Global Agent – y en la pestaña security Settings hacer click en el apartado Firewall Settings - Enable the Apex One Firewall.



# Cortafuegos – Agregar Política

**Edit Policy**

Firewall Policies > Edit Policy

**Firewall Policy**

Name: All access policy

Security level (does not apply to ports in the exception list)

- ○ High — Block all inbound/outbound traffic
- ○ Medium — Block inbound traffic, allow outbound traffic
- ◉ Low — Allow all inbound/outbound traffic

**Firewall Features**

- ☑ Enable firewall
- ☐ Display a notification when a Firewall violation is detected

**Certified Safe Software List**

Applications in the Certified Safe Software List are exempt from firewall policies if the security settings have been set to High or Medium.

- ☐ Enable the local Certified Safe Software List
  - ☐ Enable the global Certified Safe Software List (Internet access required)

**Exception**

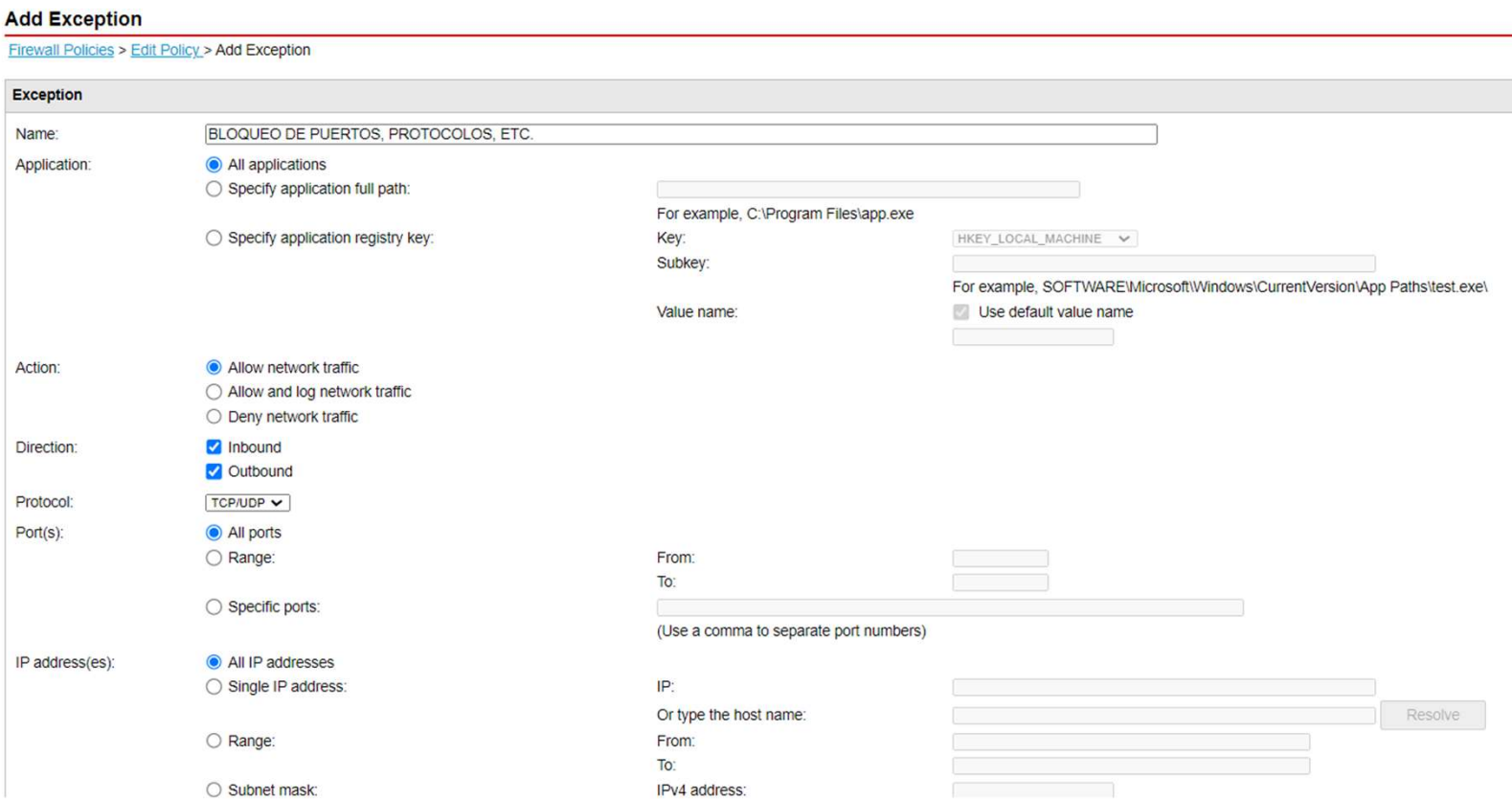
Add Delete Reorder

| ☐ | Order | Name | Action | Protocol | Port | Direction | IP Address | Application |
|---|---|---|---|---|---|---|---|---|

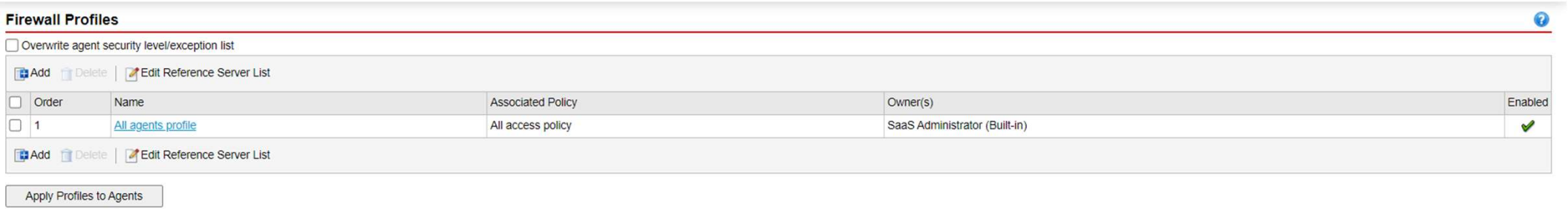
Add Delete Reorder

Save Cancel

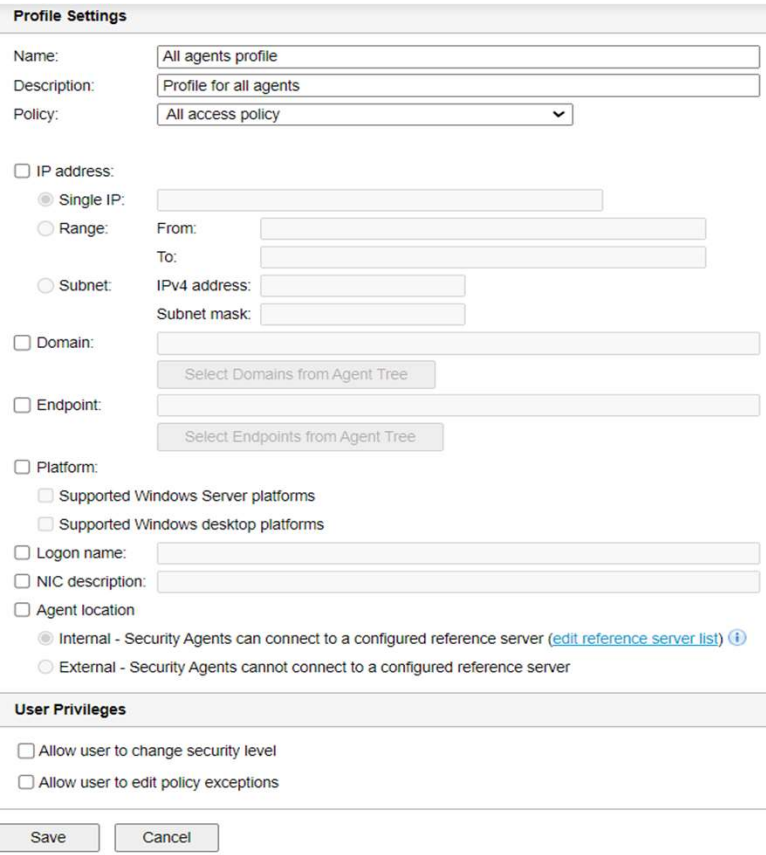
# Cortafuegos – Agregar una regla



# Cortafuegos – Perfiles



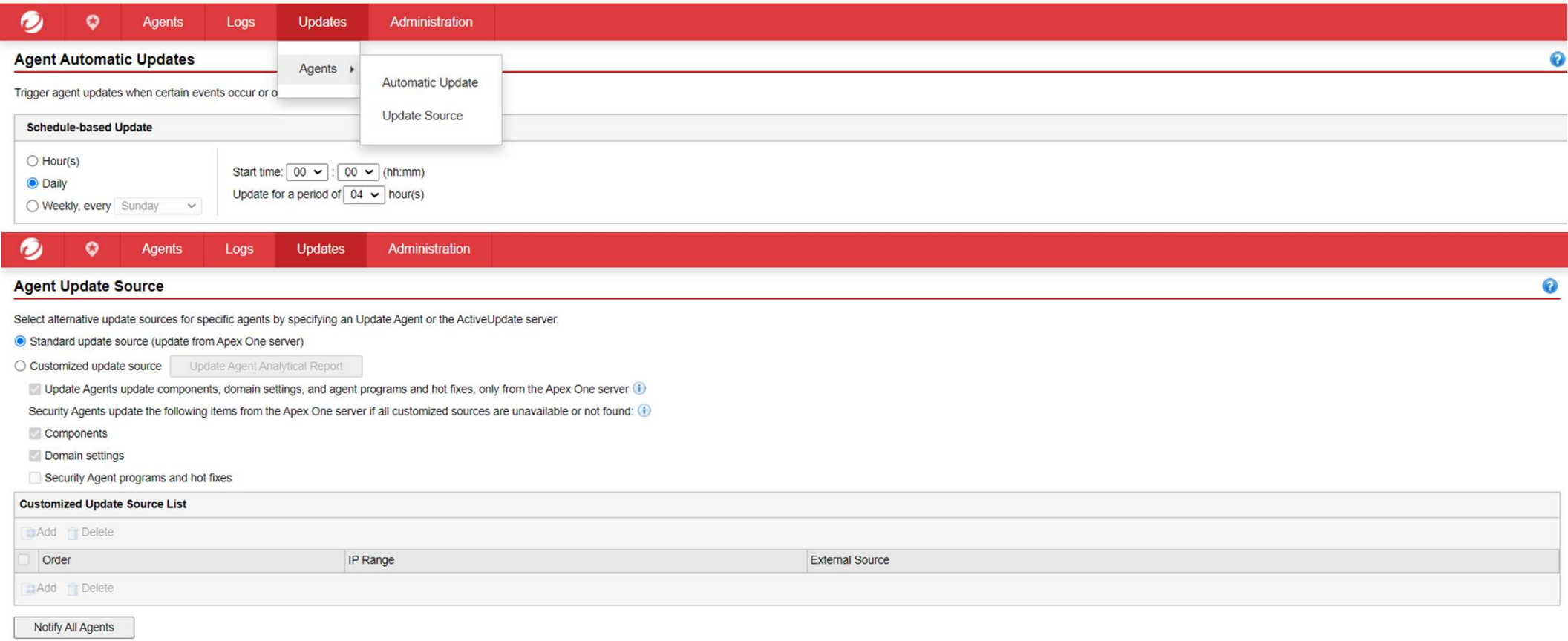
# Cortafuegos – Perfiles



# Logs

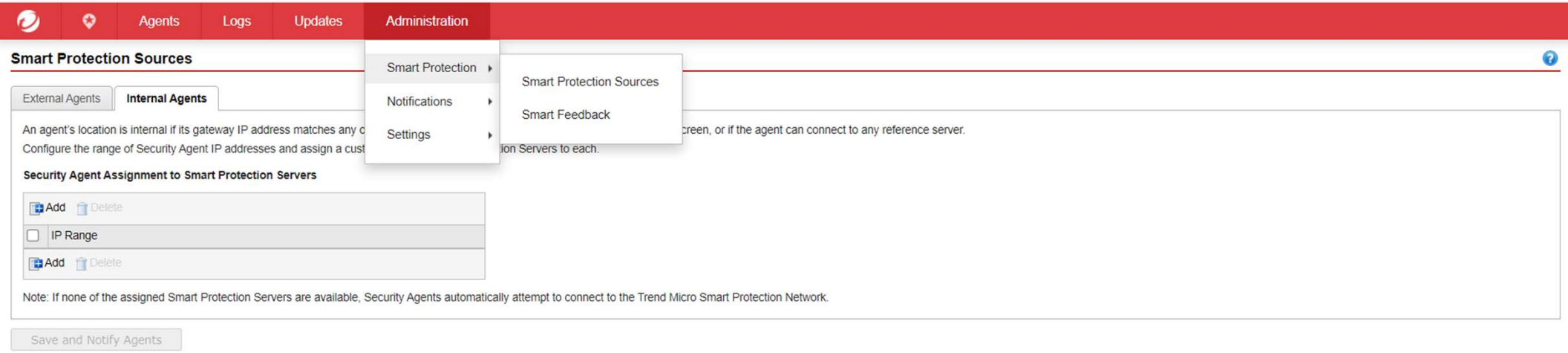

Agents
Logs
Updates
Administration
Central Quarantine Restore
Agents
System Events
Central Quarantine Restore
Central Quarantine Restore Logs
Last restore: 8/9/2024 17:24:33
Export to CSV
0 - 0 of 0
Page 0 of 0
Date/Time
File Name
Total Endpoints
Successful
Unsuccessful
Pending
Updated Domain Exclusion Lists
Export to CSV
0 - 0 of 0
Page 0 of 0
Results per page: 10

# Updates

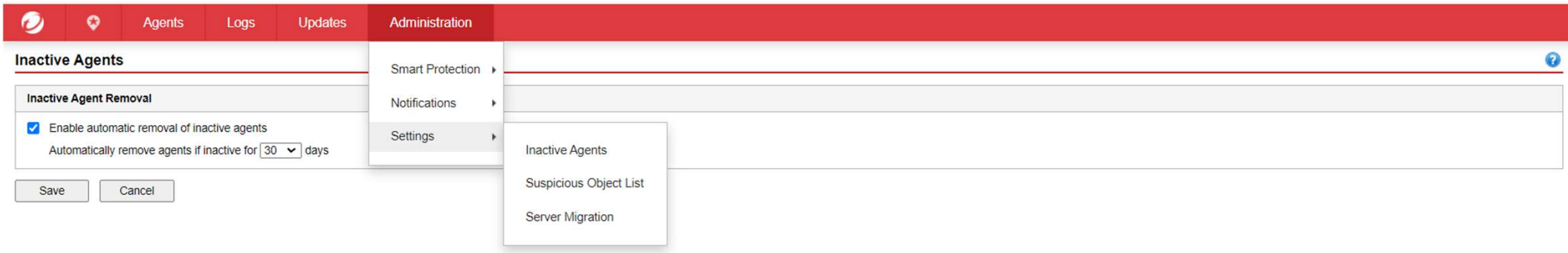

Agents
Logs
Updates
Administration
Agent Automatic Updates
Agents
Automatic Update
Update Source
Trigger agent updates when certain events occur or o
Schedule-based Update
Hour(s)
Daily
Weekly, every Sunday
Start time: 00 : 00 (hh:mm)
Update for a period of 04 hour(s)


Agents
Logs
Updates
Administration
Agent Update Source
Select alternative update sources for specific agents by specifying an Update Agent or the ActiveUpdate server.
Standard update source (update from Apex One server)
Customized update source
Update Agent Analytical Report
Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server
Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found:
Components
Domain settings
Security Agent programs and hot fixes
Customized Update Source List
Add
Delete
Order
IP Range
External Source
Add
Delete
Notify All Agents

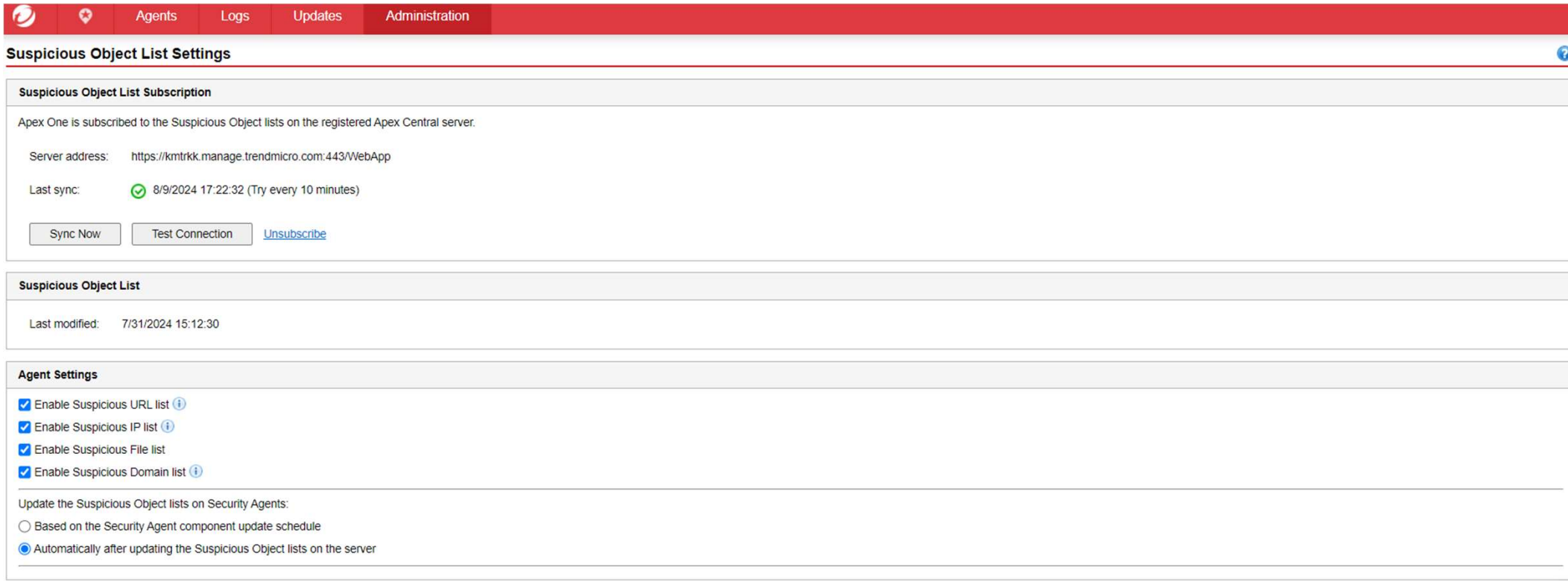
# Administration – Smart Protection Sources



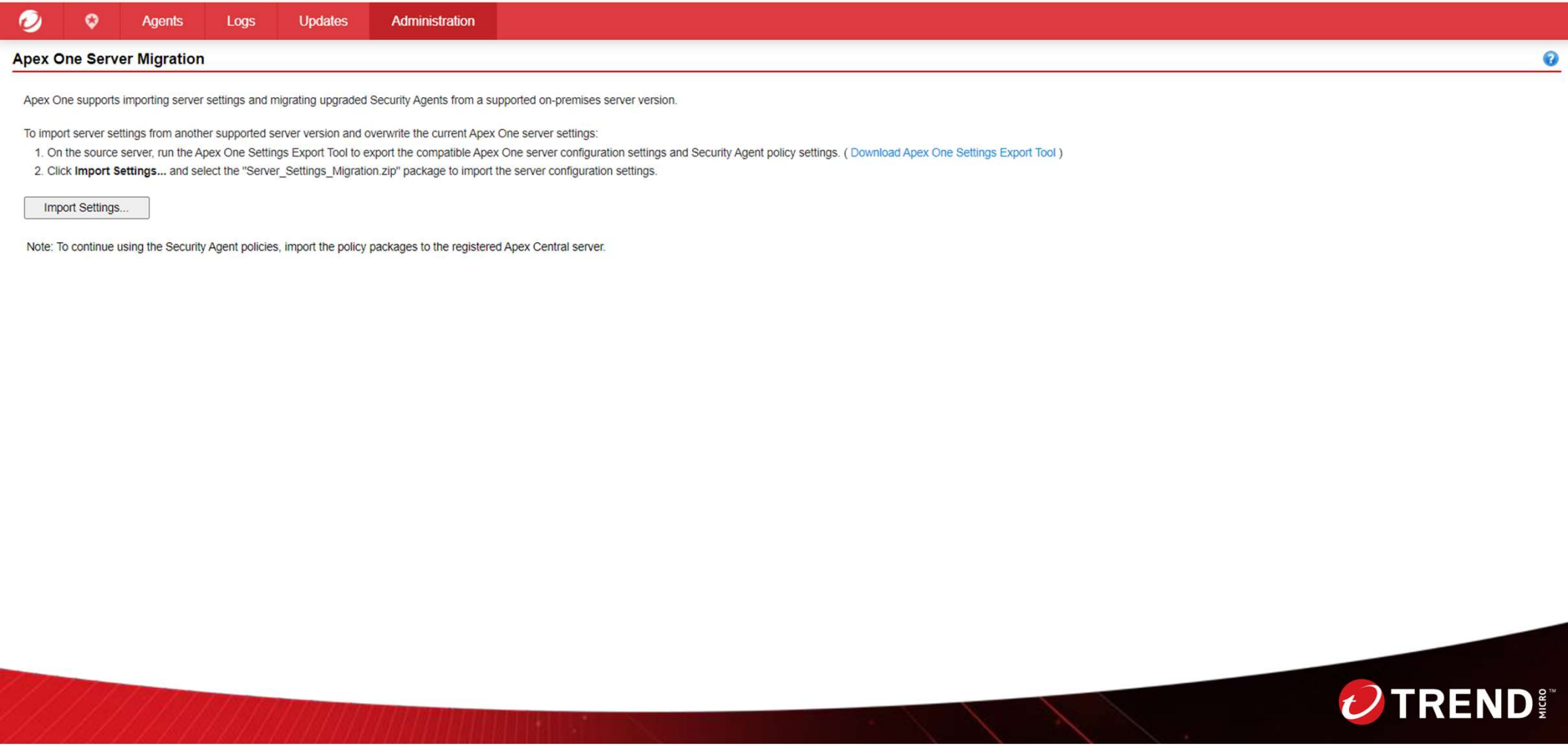
# Administration – Settings Inactive Agents



# Administration – Settings Suspicious Object List Subcription



# Administration – Settings Server Migration






©2024 Trend Micro Inc.