

Prueba de Concepto – Servicio

CLIENTE

2025

**Trend Micro**



Contenido

[Introducción 4](#_Toc209800286)

[Trend Vision One™ 4](#_Toc209800287)

[Trend Micro Ciber Risk Exposure Management CREM 4](#_Toc209800288)

[Trend Micro XDR 5](#_Toc209800289)

[Trend Vision One Standard Endpoint Protection 5](#_Toc209800290)

[Trend Vision One Server and Workload Protection 6](#_Toc209800291)

[Trend Micro Cloud Email and Collaboration Protection 6](#_Toc209800292)

[Trend Micro Cloud Email Gateway Protection 7](#_Toc209800293)

[Trend Micro Identity Posture 7](#_Toc209800294)

[Trend Micro Virtual Network Sensor 7](#_Toc209800295)

[Trend Micro Deep Discovery Inspector 7](#_Toc209800296)

[Trend Micro Zero Trust Secure Access 8](#_Toc209800297)

[Trend Micro CREM for Cloud 8](#_Toc209800298)

[Requerimientos 9](#_Toc209800299)

[Consola de administración Trend Vision One 9](#_Toc209800300)

[Standard Endpoint Protection SEP y Server and Workload Protection SWP 9](#_Toc209800301)

[Requerimientos de sistema SEP-SWP 10](#_Toc209800302)

[Requerimientos de conectividad SEP-SWP 10](#_Toc209800303)

[Definición de alcance de la prueba SEP-SWP 11](#_Toc209800304)

[Requerimientos Cloud Email and Collaboration Protection 11](#_Toc209800305)

[Requerimientos Cloud Email Gateway Protection 14](#_Toc209800306)

[Requerimientos para conexión de directorio activo On-Premises 14](#_Toc209800307)

[Requerimientos para conexión de directorio activo Entra ID 15](#_Toc209800308)

[Requerimientos para despliegue Virtual Network Sensor 15](#_Toc209800309)

[Requerimientos de sistema 15](#_Toc209800310)

[Requerimientos de conectividad 15](#_Toc209800311)

[Proceso de despliegue 15](#_Toc209800312)

[Puertos y URL usadas por el Virtual Network Sensor 16](#_Toc209800313)

[Requerimientos para despliegue Deep Discovery Inspector (Virtual) 16](#_Toc209800314)

[Requerimientos de conectividad vDDI 17](#_Toc209800315)

[Arquitectura General de Referencia 17](#_Toc209800316)

[Arquitectura de tarjeta de red para el vDDI 17](#_Toc209800317)

[Requerimientos para despliegue ZTSA: Private Access. 18](#_Toc209800318)

[Arquitectura de referencia 18](#_Toc209800319)

[Integración con solución de identidades (IAM) vía SAML 2.0 19](#_Toc209800320)

[Requerimientos del sistema para el Private Access Connector (Virtual Appliance) 20](#_Toc209800321)

[Requerimientos de conectividad Zero Trust Secure Access 20](#_Toc209800322)

[Definición de aplicaciones corporativas para acceso seguro 20](#_Toc209800323)

[Requerimientos para el despliegue de Secure Access Module (SAM) 21](#_Toc209800324)

[Requerimientos para despliegue ZTSA: Internet Access. 21](#_Toc209800325)

[Arquitectura de referencia 21](#_Toc209800326)

[Listado de IP públicas 22](#_Toc209800327)

[Integración con solución de identidades (IAM) vía SAML 2.0 22](#_Toc209800328)

[Requerimientos para el despliegue de Secure Access Module (SAM) 22](#_Toc209800329)

[Requerimientos de conectividad Zero Trust Secure Access 22](#_Toc209800330)

[Requerimientos para conexión de nubes públicas con CREM for Cloud. 22](#_Toc209800331)

[Cuentas en Amazon Web Services 22](#_Toc209800332)

[Subscripciones de Azure 23](#_Toc209800333)

[Proyectos de Google Cloud Platform 23](#_Toc209800334)

# Introducción

## Trend Vision One™

Proporciona una visión centralizada del riesgo mediante un análisis de la superficie de ataque (ASM) y los procesos de detección extendida y respuesta (XDR), permitiendo de esta forma a los equipos de ciberseguridad a mejorar sus procesos y tener una visualización de su plataforma tecnológica gracias a la integración de su portafolio sumado al amplio sistema de integración con terceros mediante APIs, permitiendo de esta forma recibir y normalizar las actividades y telemetría dentro de los ambientes de sus usuarios.

## Trend Micro Ciber Risk Exposure Management CREM

La visibilidad como herramienta de reconocimiento de activos tecnológicos es fundamental para determinar las debilidades de estos activos en términos de seguridad, con esta perspectiva Trend Micro permite a las entidades a reconocer el riesgo desde una forma general-ejecutiva a cada punto particular-operativa, logrando:

• Identificar, categorizar y documentar los activos dentro de la organización bajo las siguientes categorías:

* Activos expuestos en internet.
* Dispositivos
* Cuentas
* Aplicaciones accedidas por los dispositivos
* Activos en nube

• Cubrimiento tanto para ambientes IT como OT.

• Visualización desde una consola unificada.

• Integración con soluciones de protección asociadas a Endpoint, Correo, Nubes públicas, Red, OT, XDR y Zero Trust desde una misma consola.

• Conexión con terceras partes tanto para obtener datos enriquecidos, como para compartir información de alertas.

• Análisis de la criticalidad de los activos basado en la medición de su riesgo, alineado a la información de vulnerabilidades, actividad de amenazas dentro del entorno y configuraciones de controles de seguridad.

• Brindar información de los activos descubiertos a nivel de dispositivos (ej: Endpoints, Servidores), mostrando además información de sistema operativo, nivel de riesgo, dirección IP, último usuario conectado, vulnerabilidades, fuente que lo detectó y cuándo se detectó dicho activo.

• Configuración de criticalidad del activo basado en la decisión del usuario.

• Posibilidad de detectar activos que no se manejan con sistemas de protección de Trend Micro, ya sea por medio de la lectura de estado de red, así como de las fuentes de terceros.

• Identificación de activos de identidad desde distintas fuentes de información, así como dominios y cuentas de servicio.

• Visualización gráfica de cómo el activo depende o relaciona con otros activos dentro de la organización.

• Correlación de identidades, dispositivos y aplicaciones usadas por los mismos con el fin de determinar riesgos en dichas relaciones, esto basado en el uso discriminado a nivel de usuario y dispositivo.

• Brindar información detallada del por qué una aplicación presenta riesgo en su uso, basado en información como cabeceras de seguridad, compliance, características de seguridad y brechas de datos.

• Identificación de las vulnerabilidades con mayor riesgo dentro de los activos, brindando información relevante sobre las mismas con el fin de apoyar al equipo operativo en su gestión.

• Posibilidad de establecer planes de acción con el fin de disminuir el riesgo basado en metas establecidas por la entidad.

• Habilidad de mostrar a nivel ejecutivo un dashboard que permitirá entender a alto nivel el estado actual de la situación de ciberseguridad dentro de la organización.

## Trend Micro XDR

Por medio de sensores dispuestos en las tecnologías, Trend Vision One permite a las entidades reconocer actividades anómalas que salen del alcance de los sistemas de protección convencionales, por lo que por medio de sistemas de Detección y Respuesta eXtendida es posible encontrar amenazas dentro de las instituciones, para ello Trend Micro se apalanca de características como:

* Lago de datos con telemetría de distintas tecnologías (Endpoints, servidores, servicios de correo electrónico, directorio activo, red, escáner de vulnerabilidades, etc)
* Análisis de posibles técnicas observadas de ataque bajo las técnicas, tácticas y procedimientos definidos por MITRE ATT&CK
* Análisis particular sobre telemetría basado en modelos de detección de actividades anómalas.
* Reportes de inteligencia de distintos tipos de entidades como:
  + Investigadores de seguridad
  + Agencias gubernamentales
  + Organizaciones analistas.
  + Fabricantes de productos de ciberseguridad
* Creación y gestión de indicadores de compromiso.
* Barrido de indicadores de compromiso propios y de reportes en tecnologías Trend Micro.

## Trend Vision One Standard Endpoint Protection

Solución de protección de Endpoints de Trend Micro y reconocida en Gartner Peer Insights Customers' Choice, así como líder en Gartner Magic Quadrant para EPP, aprovecha una combinación de técnicas de amenazas intergeneracionales para brindar la protección más amplia contra todo tipo de amenazas y gestión de Endpoints con las siguientes capacidades:

* Antimalware de próxima generación
* Mitigación avanzada de Ransomware y todo tipo de amenazas
* Data Loss Prevention
* Protección de vulnerabilidades de red
* Control de Dispositivos y Aplicaciones
* Reputación Web

## Trend Vision One Server and Workload Protection

Proporciona una detección y protección en una única solución diseñada específicamente para servidor, nube y entornos de contenedores. Esta protección permite una seguridad constante, independientemente de la carga de trabajo También proporcionan un amplio conjunto de interfaces de programación de aplicaciones (API) para que la seguridad se puede automatizar y no afectará a sus equipos.

La POC de Trend Micro Vision One Server & Workload Protection está enfocada en la protección de los servidores tiene como objetivo mostrar los niveles de protección avanzados que nuestros clientes pueden tener en sus servidores para optimizar la postura de seguridad. Para esto se la solución permite la implementación de las siguientes características.

* Escaneo de Recomendaciones
* Blindaje de Vulnerabilidades (virtual patch), tanto de sistema operativo como de aplicaciones)
* Firewall de host
* Integrity Monitoring
* Log Inspection
* Control de aplicaciones
* Antimalware
* Reputación Web

## Trend Micro Cloud Email and Collaboration Protection

El uso de servicios como Microsoft 365 y Google Workspace se ha vuelto una constante en las distintas entidades, ya que se pueden encontrar herramientas de trabajo colaborativo para correo, manejo de archivos, chats, comunicación de equipos, etc. Con Trend Micro Cloud Email and Collaboration Protection las entidades pueden analizar dentro de sus activos amenazas mediante características como:

* Advanced Spam Protection.
* Malware Scanning.
* File Blocking.
* Web Reputation.
* Virtual Analyzer.
* Correlated Intelligence.
* Business Email Compromise.
* Data Loss Prevention.

## Trend Micro Cloud Email Gateway Protection

Dado la importancia del correo electrónico en el día a día de las operaciones de las distintas entidades, y cómo es uno de los vectores de ataque más comunes en la actualidad, Trend Micro Cloud Email Gateway Protection permite mediante el direccionamiento del flujo de correo, establecer un punto de análisis previo a la llegada el buzón de los correos anómalos, para ello cuenta con características como:

* Connection Filtering
* Domain-based authentication
* Advanced Spam Protection.
* Malware Scanning.
* Content filtering
* Virtual Analyzer.
* Correlated Intelligence.
* Business Email Compromise.
* Data Loss Prevention.

## Trend Micro Identity Posture

En la actualidad se reconoce la identidad como un nuevo perímetro, ya que los ataques dirigidos a cada uno de los integrantes de cada entidad se convierten en foco principal de los atacantes, por esta razón se requiere entender completamente cuál es el inventario de usuarios existentes, ya sean activos o no, y bajo los mismos determinar los riesgos existentes, para ello Trend Micro define esta solución a nivel de:

* [Identity Inventory](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-for-mea-identity-inventory#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-qiw63n).
* [Identity Posture](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-for-mea-__identity-posture-2#GUID-ddca03c9-4beb-4312-8cc0-466872e01da2-2).

Para este fin se requiere conexiones particulares para el directorio activo, ya sea en nube (Entra ID) u On-Premises.

## Trend Micro Virtual Network Sensor

En términos de actividades de detección y respuesta a nivel de red, Trend Micro cuenta con el Virtual Network Sensor, dispositivo virtualizado que permite analizar el tráfico con el fin de detectar entre otros los siguientes elementos:

* Descubrir activos dentro de la infraestructura.
* Evaluar el riesgo en los activos encontrados.
* Analizar el ciclo de vida de un ataque.
* Extracción de IoC con el fin de conectar con terceros

## Trend Micro Deep Discovery Inspector

Mediante el análisis del tráfico de su red, Deep Discovery Inspector proporciona una visibilidad de 360° supervisando todos los puertos de red en más de 105 distintos protocolos gracias a sus capacidades de IDS, correlacionando eventos de amenazas avanzados con el fin de priorizar su respuesta, de esta forma no sólo se supervisa el tráfico este-oeste, sino además norte-sur, detectando características importantes como movimientos laterales.

## Trend Micro Zero Trust Secure Access

Zero Trust es un enfoque de arquitectura para la seguridad de las redes que asume que cada transacción, entidad e identidad no es de confianza hasta que esta sea establecida y mantenida a lo largo del tiempo. Las estrategias ZT contrastan con la idea antigua de que una red es segura a menos de que los sistemas de seguridad identifiquen una brecha, teniendo esto en cuenta Trend Micro Zero Trust Secure Access permite la evaluación de acceso desde tres enfoques:

* Zero Trust Private Access: Los recursos corporativos privados y el acceso a los mismos es de suma importancia en las organizaciones, mediante esta metodología es posible controlar que dispositivos y usuarios (administrados o no) podrán tener acceso a dichas aplicaciones.
* Zero Trust Internet Access: Implementar control de accesos en la navegación de internet de los equipos dentro de las compañías permite analizar qué tipo de procesos se están realizando, y de esta forma controlar el procesamiento de información.
* Zero Trust AI Service Access: Permite controlar el uso de servicios de IA de forma general o incluso inspeccionando los prompts para evitar brechas potenciales de datos.

## Trend Micro CREM for Cloud

El uso de la nube pública aumenta considerablemente en los últimos tiempos, principalmente debido a la diversidad de servicios que la misma presta a las instituciones, así como la presencia en distintas zonas del mundo que facilitan la creación de infraestructura a un clic, sin embargo, la creación de recursos en las nubes implica el seguimiento de un Modelo de Responsabilidad Compartida entre el proveedor de nube y el usuario de la misma, dejando allí fallos de seguridad que pueden afectar a las compañías, por medio de Trend Micro CREM for Cloud, es posible hacer un análisis de las configuraciones con el fin de detectar:

* Fallos de seguridad.
* Mejoras de rendimiento.
* Reconocimiento de activos.
* Análisis de posibles caminos de ataque.
* Identidades.

# Requerimientos

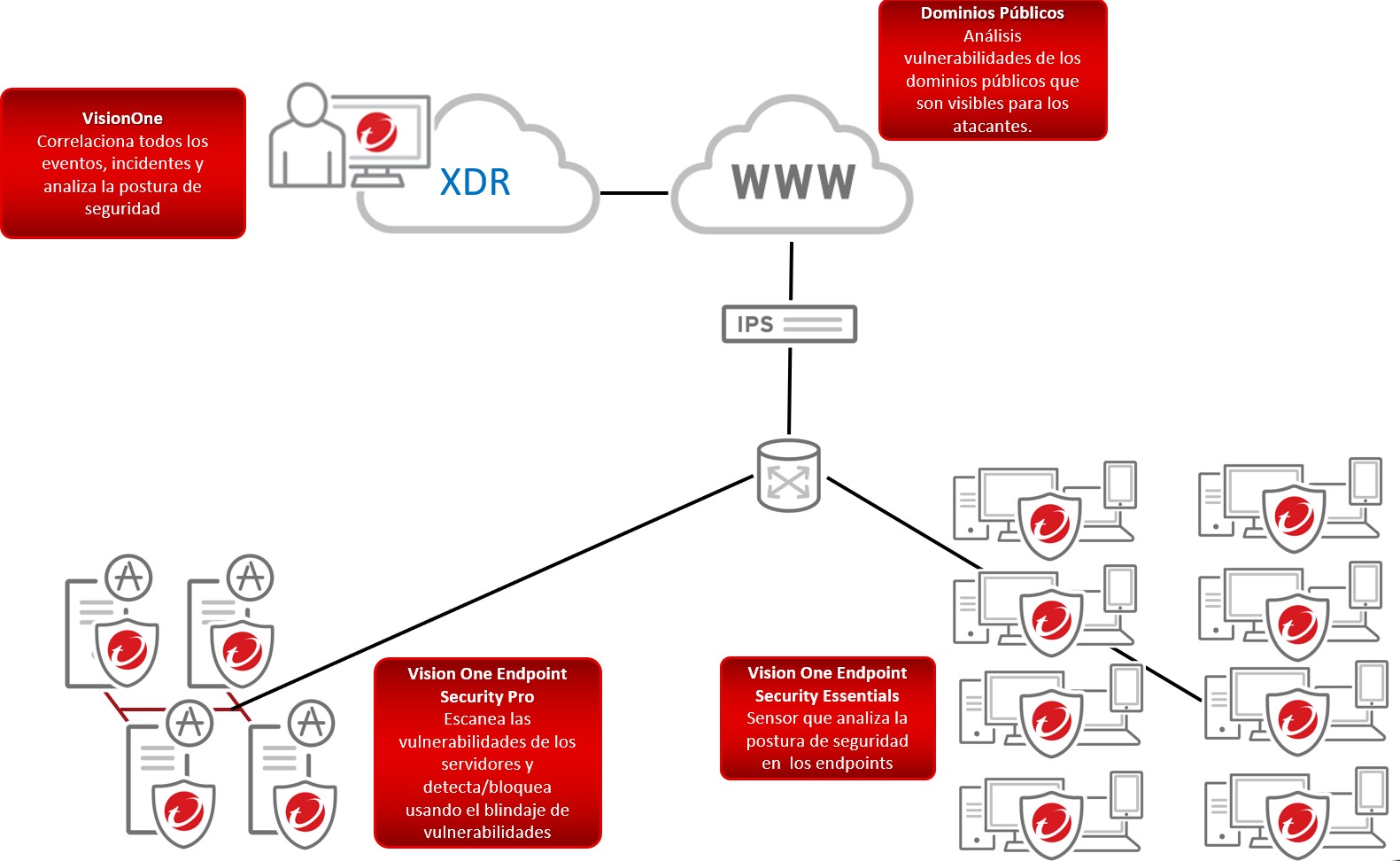
# Consola de administración Trend Vision One

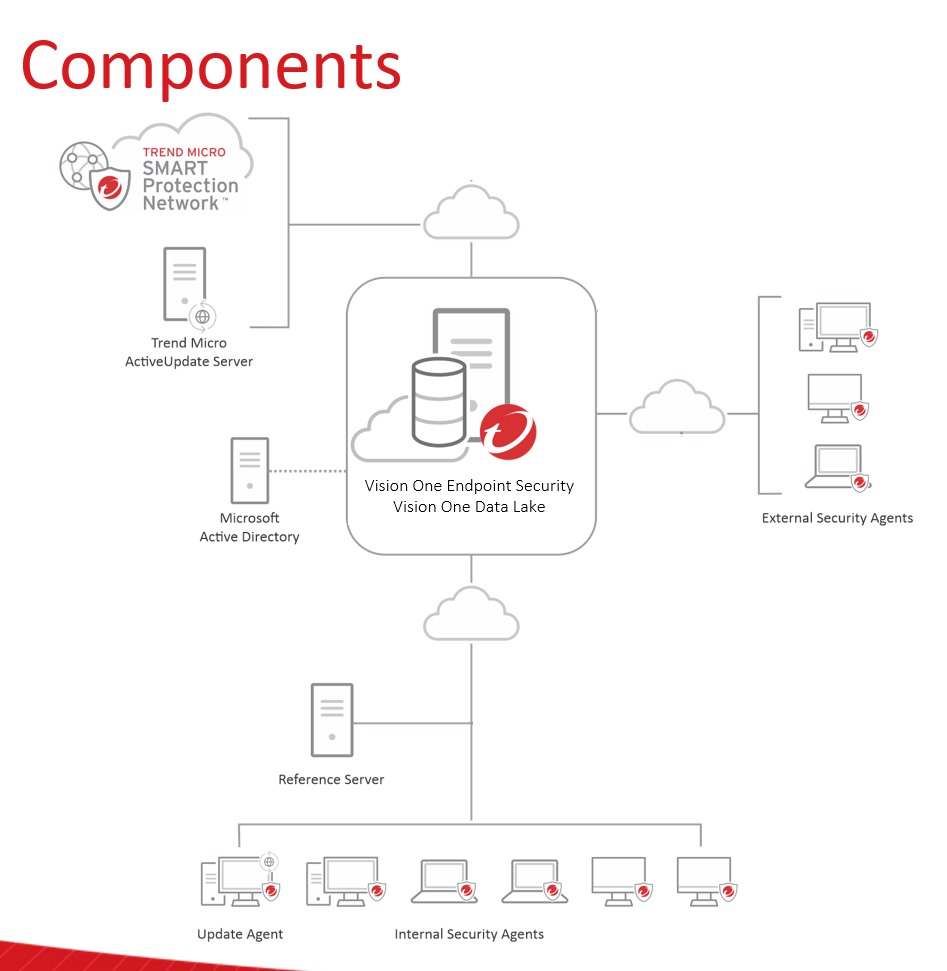
Con el fin de administrar, configurar y analizar los servicios de Trend Micro se requiere la creación de una consola denominada Vision One, para esta se requiere un usuario administrador enlazado a una cuenta de correo de la institución, sumado a ello.

Por otra parte, para poder acceder a estos servicios se recomienda el uso de un navegador web actualizado (Chrome, Firefox, Opera, Edge) y permitir excepción de conexión a los puntos recomendados en la [guía](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-firewall-americas-all-exceptions#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-7jodxo), especialmente la sección de Trend Vision One Authentication,

# Standard Endpoint Protection SEP y Server and Workload Protection SWP

Los sistemas de protección de endpoint y servidores se administran desde un mismo punto en la consola Trend Vision One, un esquema de arquitectura tendría las siguientes características:





## Requerimientos de sistema SEP-SWP

**Server Protection**: <https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-es-agent-sys-reqs>

**Kernels soportados para sistemas UNIX:** <https://files.trendmicro.com/documentation/guides/deep_security/Kernel%20Support/20.0/Deep_Security_20_0_kernels_EN.html#intro>

**Endpoint Protection**: <https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-central-patch-6-officescan-agent-ins>

**Endpoint Detection and response**: <https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-es-agent-sys-reqs>

## Requerimientos de conectividad SEP-SWP

Con el fin de garantizar un óptimo funcionamiento tanto de los sistemas de protección y su comunicación con la plataforma de administración se recomienda seguir las recomendaciones definidas en éste [enlace](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-firewall-americas-all-exceptions#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-7jodxo), específicamente para las secciones de:

* Endpoint Sensor Agents
* Standard Endpoint Protection Agents
* Server & Workload Protection Agents

El método recomendado de inclusión en la lista segura es por nombre DNS. Vision One Protection como servicio reside en la infraestructura Azure Cloud de Microsoft. Como tal, no hay un conjunto de IP o IP en las que opere el servidor Vision One. Al aprobar el nombre DNS, no será necesario aprobar una gran cantidad de subredes IP, ya que la IP se puede aprobar dinámicamente en función del DNS.

***Nota 1****: Se recomienda permitir* ***\*.trendmicro.com*** *lo cual cubre todas las urls requeridas para el funcionamiento de Vision One Endpoint and Workload Protection. Si no es posible adicionar esta única url se deben adicionar las url mencionadas en la documentación, permitiendo tráfico tanto http como https.*

***Nota 2:*** *Importante que el agente actual de la solución no esté instalado en las estaciones de trabajo, ya que ambos módulos antimalware pueden ocasionar lentitud en los procesos del equipo.*



## Definición de alcance de la prueba SEP-SWP

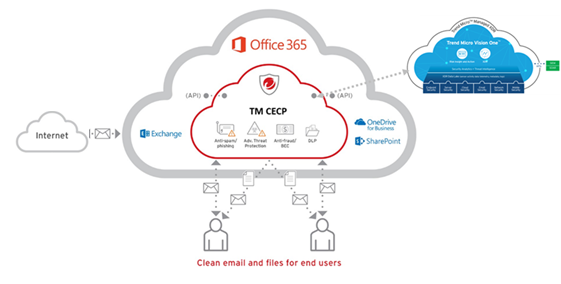
Para la instalación de los agentes de Trend Micro Vision One Endpoint en estaciones de trabajo y/o Servidores se requiere diligenciar el siguiente cuadro:

|  |  |  |
| --- | --- | --- |
| Hostname | SO | Versión/Kernel (Linux) |
| Ej: SRV\_QA\_APP | Windows Server 2012 |  |
| Ej: SRV\_Dev | Redhat 8 | 4.18.0-147.8.1.el8.x86\_64 |

*Nota: se pueden colocar la cantidad de servidores/estaciones de trabajo que se requieren en la prueba. Luego del análisis de las versiones de S.O se confirmará por parte de Trend Micro la compatibilidad de estos.*

# Requerimientos Cloud Email and Collaboration Protection

El esquema general de protección por medio de esta solución es el siguiente:



Como se observa en la imagen, el flujo de correo no es alterado, en vez de ello Trend Micro Cloud Email and Collaboration Protection existe como aplicación permitida dentro de Google Workspace y Office 365 para que, por medio de API el sistema pueda ejecutar las acciones dentro de los módulos de protección avanzada de amenazas, para esto se requiere el uso de una [cuenta de servicio](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-for-mea-authorized-account) asociada a un administrador de la plataforma, esta cuenta proveerá los permisos necesarios bajo cada servicio.

[Servicios de Microsoft 365](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-for-mea-granting-access-office-365-services).

[Box, DropBox y Google Drive](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-for-mea-access-dropbox-google-drive).

[Gmail](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-for-mea-granting-access-gmail).

En términos de Microsoft 365, se debe contar con alguno de los planes descritos a continuación:

|  |  |
| --- | --- |
| Microsoft 365 business plan | Microsoft 365 Apps for business (previously Office 365 Business) |
| Microsoft 365 Business Basic (previously Office 365 Business Essentials) |
| Microsoft 365 Business Standard (previously Office 365 Business Premium) |
| Microsoft 365 Business Premium (previously Microsoft 365 Business) |
| [For details, see https://www.microsoft.com/en-us/microsoft-365/business.](https://www.microsoft.com/en-us/microsoft-365/business) |
|  | |
| Microsoft 365 enterprise plan | Microsoft 365 E3 |
| Microsoft 365 E5 |
| [For details, see https://www.microsoft.com/en-us/microsoft-365/compare-microsoft-365-enterprise-plans.](https://www.microsoft.com/en-us/microsoft-365/compare-microsoft-365-enterprise-plans) |
|  | |
| Microsoft 365 education plan | Microsoft 365 A3 |
| Microsoft 365 A5 |
| [For details, see https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-education.](https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-education) |
|  | |
| Office 365 enterprise plan | Office 365 Enterprise E1 |
| Office 365 Enterprise E3 |
| Office 365 Enterprise E5 |
| Microsoft 365 Apps for enterprise (previously Office 365 ProPlus) |
| [For details, see https://products.office.com/en-us/business/compare-more-office-365-for-business-plans.](https://products.office.com/en-us/business/compare-more-office-365-for-business-plans) |
|  | |
| Office 365 standalone plan | [Exchange Online Plan 1, Plan 2, and Kiosk](https://products.office.com/en-us/exchange/compare-microsoft-exchange-online-plans) |
| [OneDrive for Business Plan 1 and 2](https://products.office.com/en/onedrive-for-business/compare-onedrive-for-business-plans) |
| [SharePoint Online Plan 1 and 2](https://products.office.com/en-us/sharepoint/compare-sharepoint-plans) |
|  | |
| Office 365 firstline worker plan | [Office 365 F3](https://www.microsoft.com/en-us/microsoft-365/business/office-365-f3) |
|  | |
| Office 365 education plan | Office 365 Education A1 |
| Office 365 Education A3 |
| Office 365 Education A5 |
| [For details, see https://www.microsoft.com/en-us/microsoft-365/academic/compare-office-365-education-plans.](https://www.microsoft.com/en-us/microsoft-365/academic/compare-office-365-education-plans) |
|  | |
| Office 365 nonprofit plan | The following Office 365 Nonprofit plans are supported: |
| Office 365 Nonprofit Business Premium |
| Office 365 Nonprofit E3 |
| Office 365 Nonprofit E5 |
| [For details, see https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing.](https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing) |
|  | |
| Office 365 government plan | [For details, see https://products.office.com/en-us/government/compare-office-365-government-plans.](https://products.office.com/en-us/government/compare-office-365-government-plans) |

Por otra parte, para el caso de Google Workspace los planes son los siguientes:

|  |  |
| --- | --- |
| **G Suite Basic** | Cloud App Security supports Gmail and Google Drive only. |
| Note: Cloud App Security supports only manual scan for Google Drive. |
| **G Suite Business** | Cloud App Security supports Gmail and Google Drive only. |
| **Google Workspace Business editions** | Business Starter |
| Business Standard |
| Business Plus |
| [For details, see https://gsuite.google.com/intl/en/pricing.html.](https://gsuite.google.com/intl/en/pricing.html) |
| Cloud App Security supports Gmail and Google Drive only. |
| Note: For Business Starter, Cloud App Security supports only manual scan for Google Drive. |
| **Google Workspace Enterprise editions (including the previously G Suite Enterprise)** | [For details, see https://gsuite.google.com/intl/en/pricing.html.](https://gsuite.google.com/intl/en/pricing.html) |
| Note: Cloud App Security supports Google Drive and Gmail only. |
| **G Suite editions for education** | G Suite for Education |
| G Suite Enterprise for Education |
| [For details, see https://edu.google.com/products/gsuite-for-education.](https://edu.google.com/products/gsuite-for-education) |
| Note: Cloud App Security supports Google Drive and Gmail only. |

# Requerimientos Cloud Email Gateway Protection

Tanto para sistemas de correo OnPremises como los reconocidos servicios de correo y servicios colaborativos como son Microsoft Office 365 y Google Workspace esta solución requiere que el tráfico se direccione por nuestro Gateway, la arquitectura es la siguiente:

Diagrama

El contenido generado por IA puede ser incorrecto.

Para este propósito se requiere:

1. Verificar propiedad del dominio a proteger, por lo que a nivel de DNS se requiere la creación de un registro TXT que permita dicha validación.
2. Cambiar a nivel de DNS los registros MX de forma tal que el direccionamiento apunte a la tecnología de protección Trend Vision One Cloud Email Gateway Protection.
3. A nivel de correos de entrada y salida, se requiere realizar cambios con respecto al punto de donde se recibirán y enviaran correos dejando a Trend Micro como Gateway, esto depende de la suite de correo que se usa, mayor detalle del proceso se puede observar a continuación:
   1. [Google Workspace](https://success.trendmicro.com/en-US/solution/KA-0010473).
   2. [Microsoft Office 365](https://success.trendmicro.com/en-US/solution/KA-0010474).

# Requerimientos para conexión de directorio activo On-Premises

Dado que el alcance de Trend Micro a nivel de detección y respuesta permite analizar además de las estaciones de trabajo y servidores las identidades correspondientes a los usuarios, se sugiere el despliegue de esta conexión, sin embargo, puesto que el AD se encuentra On Premises, se hace necesario un punto intermedio de conexión denominado Service Gateway, las características de este son:

* [Requerimientos del sistema](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sg-sys-requirements) (verificar sección “*On-premises directory connection*”)
* [Puertos requeridos](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sg-ports-used)

Una vez el Service Gateway se encuentra disponible, la integración con el directorio activo tiene las siguientes características:

* [Permisos](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-active-directory-permissions)
* [Integración](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-ad-premises-integration#GUID-0bdbf0d8-391e-41ec-b9d2-e51584859b66)
* [Envío de eventos de seguridad mediante herramienta](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-security-event-forwarding#GUID-d8519d0b-0c27-4c54-b934-b1ba0fc25104)
* [Información obtenida desde el Active Directory y usada por parte de Vision One](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-ad-data-usage-associated-apps)

# Requerimientos para conexión de directorio activo Entra ID

La conexión del directorio activo en nube requiere que un usuario con permisos administrativos dentro del Microsoft Entra ID, un detalle de estos pueden verse en [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-access-permissions-data#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-sc3g4v) enlace.

Por otra parte, la información adquirida será utilizada en distintas capas, como son: Inventario de correos, simulación de phishing, Ciber Risk Exposure Management, Identity Detection and Response, Zero Trust Secure Access, etc, si se desea reconocer esta información, puede observarse en [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-usage-associated-apps#GUID-09957805-70E7-401F-A691-F587FCE2CB8B-5fumt1) enlace.

# Requerimientos para despliegue Virtual Network Sensor

## Requerimientos de sistema

A screenshot of a computer

Description automatically generated

## Requerimientos de conectividad

Con el fin de garantizar un óptimo funcionamiento tanto de los sistemas de protección y su comunicación con la plataforma de administración se recomienda seguir las recomendaciones definidas en éste [enlace](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-firewall-americas-all-exceptions#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-7jodxo), específicamente para las secciones relacionadas a Virtual Network Sensor.

## Proceso de despliegue

Este proceso depende de dónde se vaya a desplegar, en la siguiente [documentación](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-network-sensors-deploy-guides#GUID-BED80320-70E5-47C4-9530-CC26073D469D-7mgryb) se observa la capacidad para:

* Hyper-V
* KVM
* VMWare ESXi
* VMWare vCenter
* Nutanix AHV
* AWS
* Azure
* Google Cloud

## Puertos y URL usadas por el Virtual Network Sensor

Con el fin de que el Virtual Network Sensor envíe data a Network Security en Vision One, se deben configurar los puertos y URL descritos en [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-ports-urls-used-network-sensor#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-8bmfqs) enlace.

# Requerimientos para despliegue Deep Discovery Inspector (Virtual)

Este proceso se realiza mediante la instalación de un *virtual appliance*, los ambientes soportados son:

* VMWare ESXi 7.0 u 8.0
* Microsoft Hyper-V en Windows Server 2019 o 2022
* RHEL 9.2 KVM

Teniendo en cuenta el tráfico a analizar (throughput) los requerimientos mínimos de la máquina virtual son los siguientes.

Tabla

El contenido generado por IA puede ser incorrecto.

*Tomado de* [*DDI Installation and Deployment Guide (p. 101)*](https://docs.trendmicro.com/o-help/manual/96515cfe-aa03-464c-acd9-3f132e7ff962/ddi_6.7_idg.pdf)

Adicionalmente, se debe tener en cuenta que, para la conexión es necesario que se realicen las configuraciones de Virtual Switch y Port Group. (configuración en el ESXi). Documentación: [*DDI Installation and Deployment Guide (p. 103)*](https://docs.trendmicro.com/o-help/manual/96515cfe-aa03-464c-acd9-3f132e7ff962/ddi_6.7_idg.pdf)

Puerto espejo (spam, mirror) configurado en el switch core (Switch Físico) que concentre el tráfico tanto Vertical como Horizontal, es decir que pueda ver todas las VLAN’s, DMZ y de ser necesario servicios como MPLS u otro tráfico de redes de interés. En este puerto se conectará el puerto de datos del DDI para realizar el análisis de tráfico. Tener en cuenta el throughput del dispositivo Deep Discovery Inspector

*Nota: En el caso del Virtual DDI, el ESXi (host) en donde se realizará la instalación requiere tener un puerto físico libre, para mapear el puerto de datos del DDI a ese puerto físico y a su vez conectar este puerto del ESXi al port mirror en el Switch Core (ver Arquitectura General de Referencia)*

Puerto para administración: Puerto al cual se conectará la interfaz de administración del DDI.

Direccionamiento de red: Una dirección IP de administración que será configurada en el DDI (asociado al puerto de administración). Mascara de red, default Gateway, dirección IP del DNS, dirección IP del Proxy si se requiere (usuario/contraseña).

## Requerimientos de conectividad vDDI

Con el fin de garantizar un óptimo funcionamiento tanto de los sistemas de protección y su comunicación con la plataforma de administración se recomienda seguir las recomendaciones definidas en éste [enlace](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-firewall-americas-all-exceptions#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-7jodxo), específicamente para las secciones relacionadas a Deep Discovery Inspector (La versión dependerá de aquella que sea instalada)

## Arquitectura General de Referencia

A continuación, se podrá observar cómo sería una referencia del proceso:

Diagrama

Descripción generada automáticamente

## Arquitectura de tarjeta de red para el vDDI

Se requiere que físicamente desde el Core de la red se le envée el tráfico al nodo de virtualización por medio del Span Port. Físicamente puede ser una conexión en Cobre y/o fibra óptica, dependiendo del medio de comunicación disponible.

En el nodo de virtualización de la red, se requiere garantizar un puerto físico para conectar directamente con el switch core para que así reciba el tráfico.

Como se muestra en las siguientes imágenes, en el nodo de virtualización se requiere que se realice un “bridge” de conexión entre la interfaz física y virtual switch para que así se pueda “enlazar” el tráfico proveniente del span port, y pueda ser asignado a la interfaz virtual del Network Sensor y/o el vDDI, aplica la misma configuración para ambos escenarios.

**A diagram of a server

Description automatically generated**

A diagram of a computer hardware

Description automatically generated

# Requerimientos para despliegue ZTSA: Private Access.

Trend Micro Vision One Zero Trust Secure Access - Private Access (ZTSA-PA) es una aplicación de la plataforma Vision One que proporciona capacidades de acceso a redes de confianza cero (ZTNA). ZTSA Private Access aplica los principios del mínimo privilegio para ofrecer a los usuarios una conectividad segura y directa a las aplicaciones privadas, al tiempo que elimina el acceso no autorizado y reduce significativamente el riesgo asociado a movimientos laterales.

## Arquitectura de referencia

En el siguiente diagrama general se muestran los componentes que interactúan para poder ofrecer los controles de Acceso Seguro Privado:

Diagrama

El contenido generado por IA puede ser incorrecto.

1. Cliente ZT Secure Access: es un software instalado en el endpoint. Dispone de una interfaz de usuario interactiva con la que el usuario final puede iniciar sesión en ZTSA Private Access con una contraseña de usuario o MFA. También es capaz de detectar la postura del endpoint e informar de ella hacia los servicios de nube de Vision One, lo que permite un control de acceso basado en el contexto. Además, tiene la función de redirigir el tráfico destinado a la red corporativa al túnel seguro entre el módulo y el conector ZTSA Private Access.
2. Cloud Service Private Access: los servicios dentro de Vision One dedicados al acceso privado se pueden dividir en dos partes, plano de control (controller) y plano de datos (relay service).

El plano de control se encarga de la autenticación de usuarios/dispositivos y de la autorización de acceso. También actúa como coordinador para conectar al usuario final con la aplicación corporativa. Para cada acceso se comprobará la identidad del usuario, el horario, la geolocalización y la aplicación con las reglas de acceso definidas por el administrador. El plan de datos es una colección de servidores relay. Cada servidor puede establecer conexiones tanto con el conector de acceso privado como con el agente ZT Secure Access mediante la creación de un túnel seguro virtual.

1. Private Access Connector: dispositivo virtual desplegado en la red corporativa (centros de datos locales o en nubes públicas). Su función principal es exponer de forma segura los recursos corporativos al servicio de retransmisión ZTSA Private Access haciéndolos invisibles en Internet. Utiliza únicamente conexiones inside-out con los servicios en la nube, por lo que no hay necesidad de configurar el firewall para permitir el tráfico entrante a la red corporativa.

## Integración con solución de identidades (IAM) vía SAML 2.0

Se deben otorgar ciertos permisos dentro de su sistema IAM para habilitar Zero Trust Secure Access para monitorear los intentos de inicio de sesión de los usuarios, acceder a los datos de los usuarios y realizar acciones en las cuentas de los usuarios. Para habilitar la autenticación del usuario, se debe configurar el inicio de sesión único (SSO) basado en SAML para su sistema IAM.

Esta integración soporta el protocolo SAML 2.0 definido por la organización OASIS. Cualquier proveedor de IDP que admita SAML 2.0 debería trabajar con Trend Vision One; sin embargo, Trend Micro solo puede garantizar la compatibilidad con los proveedores de IDP probados. El alcance de sistemas de IAM soportados, los permisos se definen en [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-iam-systems-required-permissions) enlace.

## Requerimientos del sistema para el Private Access Connector (Virtual Appliance)

El conector que tendrá conexión con los recursos privados puede ser desplegado en distintas metodologías, actualmente se soportan las siguientes

* VMWare ESXi
* Microsoft Azure
* Amazon Web Services
* Google Cloud Platform
* Microsoft Hyper-V

En cuanto a las recomendaciones en términos de las capacidades del servidor puede observarse en [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-pa-connector-system-reqs#GUID-09957805-70E7-401F-A691-F587FCE2CB8B-cktws6) enlace.

*Nota:La disponibilidad puede cambiar a través del tiempo, agregando nuevas plataformas disponibles, para determinar las actuales el mismo enlace será actualizado.*

## Requerimientos de conectividad Zero Trust Secure Access

Con el fin de garantizar un óptimo funcionamiento de los sistemas y su comunicación con la plataforma de administración se recomienda seguir las recomendaciones definidas en éste [enlace](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-firewall-americas-all-exceptions#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-7jodxo), específicamente para las siguientes secciones

* Zero Trust Secure Access Exceptions: Access Module.
* Zero Trust Secure Access Exceptions: Authentication.
* Zero Trust Secure Access Exceptions: Private Access Connector.

## Definición de aplicaciones corporativas para acceso seguro

Agregar las aplicaciones corporativas a Vision One permite gestionar y aplicar controles de acceso seguro mediante la aplicación de ZTSA Private Access. Se deberán de definir las aplicaciones sobre las que se desea controlar el acceso para asociarlas al grupo de Private Access Connector que se encuentre dentro del mismo ambiente.

El acceso a las aplicaciones por parte de los usuarios se puede ofrecer mediante 2 formas: Acceso por el cliente ZT Secure Access o por el navegador a través del portal web de usuarios generado por Trend Micro. Para dar de alta las aplicaciones a continuación se detallan los parámetros requeridos por cada tipo de acceso:

* Acceso por cliente ZTSA:
  + Protocolo (TCP/UDP, DNS, HTTP, HTTPS, FTP, FTPS, RDP, SSH, SFTP, TELNET, VNC).
  + Dominio interno de la aplicación.
  + Direcciones IP internas de la aplicación.
  + Puertos TCP UDP.
* Acceso por navegador (browser):
  + Protocolo (HTTP, HTTPS, Web-based RDP, Web-based SSH).
  + HTTP, HTTPS
    - URL interna: FQDN/dirección IP y puerto requerido que utiliza la red interna para conectarse a la aplicación.
    - URL Externa: FQDN/dirección IP y puerto requerido del dominio externo al que acceden los usuarios finales para conectarse a la aplicación interna.
  + Web-based RDP: FQDN/dirección IP y puerto requerido del escritorio remoto para conectarse a la aplicación.
  + Web-based SSH: FQDN/dirección IP y puerto requerido del servidor remoto para conectarse a la aplicación interna.

Se deberán considerar también los flujos de comunicación entre el Private Access Connector y las aplicaciones corporativas contempladas.

## Requerimientos para el despliegue de Secure Access Module (SAM)

En [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sam-sys-requirements#GUID-09957805-70E7-401F-A691-F587FCE2CB8B-fotgj2) enlace se presentan los distintos sistemas operativos y características de procesamiento sobre los cuales se podrá hacer despliegue del SAM.

# Requerimientos para despliegue ZTSA: Internet Access.

Trend Micro Vision One Zero Trust Secure Access - Internet Access (ZTSA-IA) es una aplicación de la plataforma Vision One que proporciona capacidades de acceso a internet de forma tal que sea posible ejecutar controles de navegación a los dispositivos/usuarios administrados por las compañías, para ello se realizan evaluaciones de usuarios, postura de dispositivos, localización geográfica, red y tiempo, con el fin de determinar si se habilitan accesos a los recursos necesarios.

## Arquitectura de referencia

El diagrama de componentes que permiten ejecutar el control de acceso seguro a internet es el siguiente:

Diagrama

El contenido generado por IA puede ser incorrecto.

Dentro del diagrama se contempla el escenario híbrido en donde se combinan la inspección con el servicio on-premise (On-premise Gateway) y el gateway que se encuentra en la nube (Internet Access Cloud Gateway). De lado del usuario aparecen las opciones de los equipos considerados como administrados, los cuales son aquellos donde se les puede instalar el cliente o módulo de Acceso Seguro (Secure Access Module) y los no administrados (PAC File).

Para poder habilitar los servicios de protección se deben de contemplar y ejecutar los siguientes requerimientos. En este caso se están considerando los requerimientos para proveer la protección mediante el Gateway que se encuentra en la nube.

## Listado de IP públicas

Se solicita las direcciones IP públicas con las cuales los usuarios salen a internet cuando se encuentran dentro de la organización o en una oficina en particular. Esta información se dará de alta dentro de la plataforma, lo que nos permitirá la aplicación de reglas de acceso específicas tomando como criterio la ubicación del dispositivos o usuario, no importando si se encuentra dentro o fuera de la organización.

## Integración con solución de identidades (IAM) vía SAML 2.0

Se deben otorgar ciertos permisos dentro de su sistema IAM para habilitar Zero Trust Secure Access para monitorear los intentos de inicio de sesión de los usuarios, acceder a los datos de los usuarios y realizar acciones en las cuentas de los usuarios. Para habilitar la autenticación del usuario, se debe configurar el inicio de sesión único (SSO) basado en SAML para su sistema IAM.

Esta integración soporta el protocolo SAML 2.0 definido por la organización OASIS. Cualquier proveedor de IDP que admita SAML 2.0 debería trabajar con Trend Vision One; sin embargo, Trend Micro solo puede garantizar la compatibilidad con los proveedores de IDP probados. El alcance de sistemas de IAM soportados, los permisos se definen en [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-iam-systems-required-permissions) enlace.

## Requerimientos para el despliegue de Secure Access Module (SAM)

En [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sam-sys-requirements#GUID-09957805-70E7-401F-A691-F587FCE2CB8B-fotgj2) enlace se presentan los distintos sistemas operativos y características de procesamiento sobre los cuales se podrá hacer despliegue del SAM.

## Requerimientos de conectividad Zero Trust Secure Access

Con el fin de garantizar un óptimo funcionamiento de los sistemas y su comunicación con la plataforma de administración se recomienda seguir las recomendaciones definidas en éste [enlace](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-firewall-americas-all-exceptions#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-7jodxo), específicamente para las siguientes secciones

* Zero Trust Secure Access Exceptions: Access Module.
* Zero Trust Secure Access Exceptions: Authentication.
* Zero Trust Secure Access Exceptions: Internet Access Service.
* Zero Trust Secure Access Exceptions: Internet Access Cloud Gateway.
* Zero Trust Secure Access Exceptions: Internet Access On-Premises Gateway.

## 

## Requerimientos para conexión de nubes públicas con CREM for Cloud.

Con el fin de realizar el proceso de escaneo de recursos y configuraciones, Trend Vision One se adapta a cada nube y sus metodologías de trabajo, teniendo en cuenta esto para las distintas nubes se requiere:

## Cuentas en Amazon Web Services

Cloudformation es un servicio de AWS que permite la creación recursos mediante el uso de una plantilla, este proceso es conocido como Infrastructure as a Service, mediante el mismo se despliegan recursos dentro de la cuenta de AWS que tendrán los privilegios necesarios para hacer el análisis, para esto se requiere acompañamiento del equipo administrador con una cuenta que tenga:

* Permisos de creación y ejecución de CloudFormation.
* Permisos para creación de roles y políticas dentro de la cuenta.

Cabe resaltar que la herramienta permite [integrar](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-add-cloudtrail-control-tower#GUID-F8FAF1DF-7A1E-4C0A-ADA3-6F6FC6CAD49D-ha1ebi) de forma masiva cuentas bajo un esquema de Organizations siempre y cuando usen Control Tower.

El soporte a las distintas regiones puede verse en [este](https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-aws-supported-regions-limitations#GUID-09957805-70E7-401F-A691-F587FCE2CB8B-owgk5e) enlace.

## Subscripciones de Azure

Con el fin de realizar la conexión, se requiere apoyo de un administrador de la nube con el fin de crear:

* App Registration
* Federated Credential
* Applicatons
* Role y Role Assignments para un Service Pricipal.
* Crear permisos de Azure Active Directory Graph
* Crear permisos de Microsoft Graph

## Proyectos de Google Cloud Platform

El enlace de proyectos de GCP requiere el apoyo de un usuario con permisos para:

* Creación de Service Account
* Workload Identity Pool Provider
* IAM
* Tag Keys
* Habilitación de API.