Trend Micro™

APEX ONE™

Seguridad para endpoints todo-en-uno, automatizada y detallada

El entorno de las amenazas solía ser en blanco y negro: se tenía que mantener únicamente lo confiable dentro de las organizaciones. Actualmente, es más difícil distinguir lo malicioso de lo confiable y los métodos antivirus tradicionales basados en las firmas, por sí solos, son una débil defensa frente al ransomware y las amenazas desconocidas, que a menudo consiguen filtrarse. Las tecnologías de próxima generación ayudan con algunas amenazas, pero no son infalibles, y añadir varias herramientas antimalware en un solo endpoint da como resultado demasiados productos independientes que no funcionan bien juntos. Para complicar las cosas, sus usuarios acceden cada vez más a recursos corporativos procedentes de una gran variedad de ubicaciones y dispositivos, e incluso servicios en la nube. Por lo que necesita una seguridad para endpoints inteligente, optimizada e interconectada de un proveedor en el que pueda confiar.

Trend Micro™ Apex One™ utiliza una mezcla de técnicas avanzadas de protección frente amenazas para eliminar las brechas de seguridad en cualquier actividad del usuario y en cualquier endpoint. Esta solución aprende, se adapta y comparte continuamente inteligencia de forma automática en su entorno.

Esta mezcla de protección se ofrece a través de una arquitectura que utiliza recursos del endpoint de forma más eficaz y supera a la competencia en el uso de la red y CPU, ofreciendo:

- Detección automática de amenazas, así como protección contra amenazas emergentes, como el ransomware y el fileless.
- Funciones de investigación detallada y visibilidad centralizada en toda la red mediante un conjunto de herramientas avanzadas de EDR y MDR, integración SIEM y un conjunto de APIs abiertas.
- Un agente ligero todo-en-uno con implementación flexible a través del software como servicio (SaaS) y opciones de implementación en sitio.

Apex One™ es un componente fundamental de nuestras **Smart Protection Suites,** que ofrecen capacidades de protección de gateway y endpoint tales como Application Control, Intrusion Prevention (protección frente a vulnerabilidades), Data Loss Prevention™ (DLP), entre
otras, en un único paquete. Las soluciones adicionales de Trend Micro amplían las funciones de investigación con Endpoint Detection and Response (EDR) y Trend Micro™ Endpoint Encryption™. Su organización puede acceder fácilmente a toda esta moderna tecnología de seguridad frente a amenazas mediante la visibilidad, la gestión y la creación de informes de manera centralizada.

Puntos de protección

- Endpoints físicos
- Endpoints virtualizados (add-on)
- PC y servidores Windows
- Computadoras Mac
- Punto de venta (POS) y endpoints ATM

PUEDE TENERLO TODO

- **Protección avanzada frente a malware y ransomware:** Protege los endpoints, dentro o fuera de la red corporativa, frente a malware, troyanos, gusanos, spyware y ransomware; además, se adapta para brindar protección ante las nuevas variantes desconocidas y amenazas avanzadas, como el criptomalware y el malware fileless
- **Funciones de detección y respuesta:** Apex One™ incluye funciones de detección y respuesta avanzadas. Como herramienta de investigación adicional, Trend Micro Endpoint Sensor, y nuestro servicio de Managed Detection and Response (MDR), están disponibles como complementos.
- **El parcheo virtual más oportuno de la industria:** Apex One™ Vulnerability Protection™ aplica parches de forma virtual a vulnerabilidades conocidas y desconocidas, ofreciendo una protección instantánea antes de que el parche esté disponible o pueda implementarse.
- **Defensa interconectada frente a amenazas:** Apex One™ se puede integrar con otros productos de seguridad de forma local en su red o a través del sistema de inteligencia global de amenazas de Trend Micro en la nube, para proporcionar actualizaciones rápidas a través del sandbox de red a los endpoints cuando se detecte una nueva amenaza, permitiendo agilizar la protección y reducir la propagación de malware.
- **Visibilidad y control centralizados:** Cuando se implementa Trend Micro™ Apex Central™, se pueden gestionar varias capacidades a través de una única consola para tener una visibilidad y un control centralizados en todas las funciones.
- **Integración con Mobile Security:** Puede integrar Trend Micro™ Mobile Security™ y Apex One™ por medio de Apex Central™ para centralizar la gestión de la seguridad e implementación de políticas de seguridad en todos los endpoints. Mobile Security incluye la protección contra amenazas para dispositivos móviles, gestión de aplicaciones móviles, gestión de dispositivos móviles (MDM) y protección de datos.
- **Disponible on-premise o as a service:** Apex One™ se puede implementar on-premises o en modalidad SaaS, con una paridad de producto completa entre las dos opciones de implementación.

PRINCIPALES DESAFÍOS DE NEGOCIO

* Hay demasiadas amenazas como el malware y ransomware que alcanzan su objetivo, las amenazas avanzadas evaden la detección previa a la ejecución.

* Se necesita una solución que proteja frente a todas las amenazas conocidas y desconocidas en los endpoints de PC, Mac y VDI.

* Dificultad para correlacionar y priorizar todas las alertas que llegan

* Los usuarios necesitan más automatización y conocimientos cuando se enfrentan a amenazas potenciales

* Las soluciones de seguridad de endpoints que no se comunican entre sí retrasan el tiempo de respuesta de protección y aumentan la carga de gestión.

* Existe el riesgo de que los usuarios trabajen de manera remota y que compartan información de nuevas formas a través de la nube, redes, etc.

* Aplicar parches a endpoints de manera rápida y meticulosa es una tarea compleja que puede generar vulnerabilidades.

Puntos de Protección

- Endpoints físicos
- Endpoints virtualizados (add-on)
- PC y servidores Windows
- Computadoras Mac
- Punto de venta (POS) y endpoints ATM

Capacidades de detección de amenazas

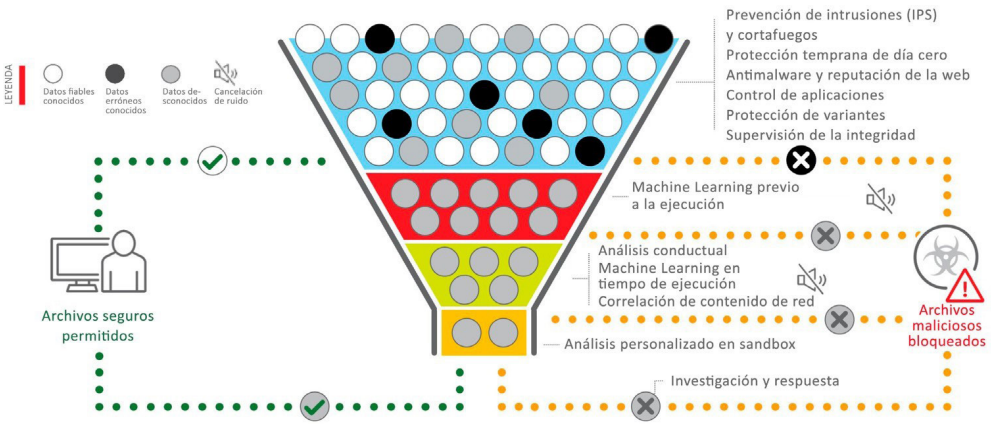
- High-fidelity Machine learning (ejecución previa y tiempo de ejecución)
- Análisis de comportamiento (frente a scripts, inyección de código, ransomware, y ataques a navegadores y memoria)
- Reputación de archivos
- Protección frente a variantes
- Census check
- Reputación Web
- Prevención de exploits (host firewall, protección ante exploits)
- Bloqueo de comando y control (C&C)
- Prevención de pérdida de datos
- Control de dispositivos
- Comprobación de archivos fiables
- Integración con sandbox y detección de brechas
- Detección y respuesta
- Endpoint Encryption (requiere un agente adicional)
- Protección contra vulnerabilidades

Descubra cómo destacamos

https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html

Máxima Seguridad XGen™

- Aplica high-fidelity machine learning con otras técnicas de detección avanzadas para ofrecer la más amplia protección frente al ransomware y los ataques avanzados..



- Filtra progresivamente amenazas mediante la técnica más eficiente para lograr una máxima detección sin falsos positivos.
- Utiliza técnicas sin firmas, incluidos el high-fidelity machine learning, el análisis de comportamiento, la protección de variantes, la comprobación CENSUS, el control de aplicaciones, la prevención de la exploits y la comprobación de archivos confiables con otras técnicas, como la reputación de archivos, la reputación de la web y el bloqueo de Comando y Control (C&C).
- Trend Micro es el primero en usar high-fidelity machine learning que analiza los archivos de forma única, no solo antes de la ejecución, sino también durante el tiempo de ejecución para obtener una detección más precisa.
- Las técnicas de cancelación de ruido, como la comprobación del censo y whitelist en cada capa, permite reducir los falsos positivos.
- Comparte información al instante sobre la actividad sospechosa en la red, así como archivos con otras capas de seguridad para detener posibles ataques posteriores.
- La protección avanzada contra el ransomware supervisa las actividades sospechosas de cifrado de archivos en el endpoint, detiene actividades maliciosas e incluso recupera archivos perdidos si es necesario.

POWERED BY XGen™ SECURITY

La solución Trend Micro User Protection con tecnología XGen™ es un método de seguridad inteligente, optimizado e interconectado.

Minim Impacto

Reduzca el impacto en el usuario y los costos de gestión.

- Apex One™ as a Service (opción disponible únicamente con Smart Protection Suites) le permite implementar y gestionar Apex One™ desde nuestro servicio basado en la nube y ofrece la misma funcionalidad que la opción on-premise.
- Este agente ligero y optimizado utiliza la técnica de detección adecuada en el momento adecuado para garantizar un mínimo impacto sobre dispositivos y redes.
- La visión centralizada del estado de los endpoints le permite tener rápidamente visibilidad de los riesgos de seguridad.
- El uso compartido automático del sistema de inteligencia sobre amenazas entre capas de seguridad permite la protección frente a amenazas emergentes en toda la organización.
- Habilite el cumplimiento y la protección fuera de las instalaciones con Edge Relay, que permite a los empleados trabajar fuera de la red corporativa y seguir conectándose a Apex One™ sin necesidad de VPN.
- Consolas personalizables para adaptarse a las diferentes responsabilidades de administración.
- Soporte 24/7 significa que, si surge un problema, Trend Micro lo resuelve rápidamente.

Partner de seguridad confiable

Trend Micro tiene una historia de constante innovación para ofrecer las tecnologías de seguridad más eficaces y eficientes. Siempre miramos al futuro para desarrollar la tecnología necesaria para luchar contra las amenazas en constante evolución del mañana.

- Más de treinta años de innovación en seguridad.
- Protegiendo más de 155 millones de endpoints.
- Contamos con la confianza de 45 de las 50 principales corporaciones mundiales.
- Trend Micro se ha posicionado como uno de los tres únicos líderes en un campo de 21 proveedores en el Cuadrante Mágico de Gartner 2018 en las Plataformas de Protección de Endpoints.

Haga clic aquí para más información

PERSONALICE LA PROTECCIÓN DE SUS ENDPOINTS

Apex One™ le ofrece la libertad de añadir capacidades adicionales de seguridad e investigación para ampliar la protección de sus endpoints. Elija entre una amplia gama de funciones avanzadas diseñadas para adaptarse a las necesidades de seguridad exclusivas de su organización.

> "Con una red como la nuestra podemos abarcar todo el país y, de este modo, ser capaces de proteger los dispositivos móviles y de escritorio con una sola plataforma para simplificar la seguridad de nuestra red y aumentar la productividad de nuestro equipo."

Greg Bell,
Director de TI en DCI Donor Servicess

PROTECCIÓN FRENTE A VULNERABILIDADES

Respaldado por una investigación de vulnerabilidades de clase mundial, la aplicación de parches virtuales de seguridad de Apex One™ ofrece la protección contra vulnerabilidades más inmediata de la industria en una gran variedad de endpoints, incluidos los dispositivos de punto de venta (POS) y de "Internet de las cosas" (IoT), así como dispositivos con sistemas operativos en fin de soporte (EOS).

Detiene inmediatamente las amenazas de día-cero en los dispositivos móviles y escritorios virtuales, dentro y fuera de la red. Trend Micro™ Vulnerability Protection, junto con las capacidades de defensa de endpoints de Trend Micro, amplía la protección a las plataformas críticas, incluidos los sistemas operativos heredados.

Protege contra amenazas avanzadas

- Bloquea los exploits que pueden aprovechar vulnerabilidades conocidas o desconocidas antes de que se implementen los parches.
- Protege a los sistemas operativos heredados y sin soporte para los que nunca se van a proporcionar parches.
- De forma automática, evalúa y recomienda parches virtuales necesarios para su entorno específico.
- Ajusta dinámicamente la configuración de seguridad en función de la ubicación de un endpoint.
- Protege los endpoints con un mínimo impacto en el funcionamiento de la red, el rendimiento o la productividad de los usuarios.
- Blinda los endpoints contra el tráfico de red no deseado con múltiples capas de protección.
- Protege los sistemas que contienen información confidencial y que son críticos para el cumplimento normativo y de las políticas empresariales.

Elimina los datos maliciosos del tráfico crítico empresarial

- Aplica filtros de control que alertan o bloquean el tráfico específico como la mensajería instantánea o transferencia de contenido multimedia.
- Utiliza la inspección profunda de paquetes para identificar contenido que puede dañar la capa de aplicaciones.
- Filtra el tráfico de red no permitido y garantiza el paso del tráfico permitido a través de la inspección de estado.

Proporciona protección temprana

- Proporciona protección antes de que se implementen los parches y, a menudo, antes incluso de que estén disponibles.
- Blinda al sistema operativo y a las aplicaciones comunes de ataques conocidos y desconocidos.
- Detecta el tráfico malicioso que se oculta usando protocolos permitidos sobre puertos que no son estándar.
- Bloquea el tráfico que puede dañar ciertos componentes en riesgo mediante la inspección de vulnerabilidades en la red.
- Impide que los backdoors en la red puedan dar acceso a la red corporativa.
- Bloquea todos los exploits conocidos con firmas de prevención de intrusiones.
- Protege las aplicaciones personalizadas y heredadas mediante el uso de filtros que bloquean parámetros definidos por el usuario..

Se implementa y gestiona desde su infraestructura existente

- Aumenta la comodidad de implementar un control granular con un dashboard simplificado y una visibilidad basada en el usuario con la consola de gestión.
- Organiza las evaluaciones de vulnerabilidades de acuerdo a los números de los boletines de seguridad de Microsoft, números de CVE u otra información importante.
- Ofrece integración de registro con las herramientas de SIEM más populares.
- Simplifica la implementación y la gestión mediante el uso de un único agente de Apex One™, con visibilidad y control centralizados

Software

Puntos de Protección

- Endpoints

Protección frente a Amenazas

- Exploits de vulnerabilidades
- Ataques de denegación de servicio
- Tráfico de red ilegítimo
- Amenazas web

Características y ventajas

- Elimina la exposición a riesgos debido a la falta de parches.
- Amplía la vida útil de los sistemas operativos heredados y sin soporte.
- Reduce el tiempo de recuperación gracias a la protección incremental contra los ataques de día-cero.
- Permite la aplicación de parches según sus propias condiciones y planificaciones de tiempo
- Reduce posibles conflictos legales al mejorar el cumplimiento de políticas de seguridad
- Mejora la protección del firewall para endpoints empresariales remotos y móviles

ENDPOINT APPLICATION CONTROL

Trend Micro Apex One™ Application Control™ le permite mejorar la protección frente al malware y los ataques dirigidos al impedir que aplicaciones no deseadas y desconocidas se ejecuten en los endpoints corporativos. Con una combinación de políticas flexibles y dinámicas, funciones de whitelisting y blacklisting, así como un amplio catálogo de aplicaciones, esta solución es fácil de manejar y reduce significativamente su exposición a ataques de endpoints. Para proporcionar más información sobre las amenazas, la visibilidad basada en el usuario y la gestión de políticas están disponibles en la consola Apex Central™ con gestión centralizada. Apex Central™ también amplía la visibilidad y el control de todos los modelos de implementación, ya sean on-premises, en la nube o híbridos. Acceda a información procesable sobre amenazas con Connected Threat Defense de Trend Micro desde un sandbox local o desde Trend Micro™ Smart Protection Network™, que utiliza información sobre amenazas de ámbito mundial para ofrecer seguridad en tiempo real desde la nube, bloqueando las amenazas antes de que lleguen a su destino.

CARACTERÍSTICAS Y VENTAJAS

Protección mejorada contra malware, ataques dirigidos y amenazas de día-cero

- Previene el daño potencial de las aplicaciones no deseadas o desconocidas (ejecutables, DLL, aplicaciones de la tienda de Windows, controladores de dispositivos, paneles de control y otros archivos ejecutables portátiles (PE).
- Proporciona información global y local sobre amenazas en tiempo real basada en los datos de buena reputación de archivos correlacionados a través de una red global.
- Se interconecta con capas adicionales de seguridad para correlacionar mejor los datos de las amenazas y detener más amenazas, más a menudo.
- Aprovecha los datos de las aplicaciones analizadas y correlacionados a partir de más de 1,000 millones de registros de archivos adecuados (Trend Micro Smart Protection Network).
- Complementa la seguridad, con herramientas como el antivirus, la prevención de intrusiones de host, la prevención de pérdida de datos y la protección móvil.

Protección de velocidades de gestión simplificada

- Aumenta la comodidad de implementar un control granular con un dashboard personalizable y una consola de gestión.
- Usa políticas inteligentes y dinámicas que permiten a los usuarios instalar aplicaciones válidas basadas en las variables de reputación como la prevalencia, el uso regional y la madurez de la aplicación.
- Proporciona más información sobre las epidemias de amenazas con visibilidad basada en el usuario, la gestión de políticas y la agregación de registros. Permite la creación de informes en múltiples capas de soluciones de seguridad de Trend Micro a través de Apex Central™.
- Categoriza las aplicaciones y proporciona actualizaciones periódicas para simplificar la administración mediante el servicio de software seguro certificado de Trend Micro

Whitelisting y blacklisting exhaustivos bloquean aplicaciones desconocidas y no deseadas

- Utiliza el nombre de la aplicación, la ruta de acceso, la expresión regular o el certificado para crear listas blancas o negras de aplicaciones básicas.
- Contiene una amplia lista de aplicaciones previamente categorizadas que se pueden seleccionar fácilmente en el catálogo de aplicaciones de Trend Micro (con actualizaciones periódicas).
- Se asegura de que se puedan instalar los parches y las actualizaciones asociados con aplicaciones en una whitelist, además de permitir que los programas de actualización puedan instalar nuevos parches y actualizaciones, con fuentes confiables.
- Permite la creación de Whitelists y blacklists de aplicaciones in-house que no aparecen en las listas.
- Ofrece una cantidad insuperable de aplicaciones y datos de archivos de confianza.

El cumplimiento con las políticas de TI internas ayuda a reducir la responsabilidad legal y financiera

- Limita el uso de aplicaciones a una lista específica de aplicaciones compatible con productos de prevención de pérdida de datos (DLP) para usuarios o endpoints específicos.
- Recopila y limita el uso de aplicaciones para el cumplimiento con las licencias de software.
- Incluye un bloqueo del sistema que refuerza los sistemas de usuario final al impedir que se puedan ejecutar nuevas aplicaciones.

> “Mi primer objetivo era deshacerme de la pesada carga administrativa que la anterior solución de seguridad de endpoints suponía para nuestros sistemas, y el segundo, incorporar un sistema de seguridad que funcionara de verdad. Desde que sustituimos la solución anterior, hemos visto que Trend Micro ha detenido los ataques por virus.”
>
> .
>
> **Bruce Jamieson**
> Gerente de Sistemas de Red de A&W Food Services de Canadá

DATA LOSS PREVENTION (DLP)

Trend Micro™ Apex One™ Data Loss Prevention™ (DLP) minimiza la complejidad y los costos de la seguridad de los datos gracias a la integración de la función DLP directamente en la solución de endpoint de Trend Micro existente. Puede obtener visibilidad y control de los datos confidenciales de forma rápida y sencilla, así como evitar la pérdida de datos a través de USB, correo electrónico, aplicaciones de software-como-servicio, web, dispositivos móviles y almacenamiento en la nube. Aproveche las plantillas regionales y específicas que tiene integradas para simplificar la implementación y cumplir con las normativas y directrices locales. Apex One™ DLP™ le permite implementar la seguridad de datos por una fracción del costo y el tiempo de las soluciones DLP empresariales tradicionales.

CARACTERÍSTICAS Y VENTAJAS

Refuerza la protección y el control de los datos

- Permite al personal de TI restringir el uso de unidades USB, dispositivos móviles conectados a USB, grabadoras de CD/DVD, almacenamiento en la nube y otros medios extraíbles mediante políticas de DLP y control granular de dispositivos.
- Permite el almacenamiento en la nube con la aplicación de DLP del cifrado de archivos, así como el uso de aplicaciones de SaaS con DLP para Microsoft® Office 365®.
- Detecta y reacciona ante el uso incorrecto de datos basado en atributos de archivo, palabras clave y expresiones regulares.
- Forma a los empleados sobre las políticas de uso de datos corporativos a través de alertas, bloqueo o bloqueo suave y presentación de informes.

Favorece el cumplimiento

- Simplifica el cumplimiento normativo con plantillas de cumplimiento.
- Acelera las auditorías y el cumplimiento con captura de datos y creación de informes en tiempo real.
- Proporciona opciones de protección de datos y plantillas específicas regionales, que ayudan a los clientes a cumplir con las directrices para la protección de datos como el Reglamento General de Protección de Datos (GDPR), PCI/DSS, HIPAA, GLBA, SB-1386 y US PII.

Optimiza la administración y reduce los costos

- Mejora la visibilidad y el control con una solución completamente integrada y de gestión centralizada
- Reduce el impacto del rendimiento y la demanda de recursos con un solo agente para endpoint security, el control de dispositivos y DLP del contenido..

Punto centralizado de visibilidad y control

- Integrado con Trend Micro™ Apex Central™ para ofrecer una cómoda consola de gestión centralizada de la seguridad que consolida la política, los eventos y la creación de informes entre varias soluciones de DLP integrada.

Protección de los datos en reposo, en uso y en tránsito

- Puntos de control de los datos en reposo: Reconoce y procesa más de 300 tipos de archivos, incluyendo la mayoría de aplicaciones de correo electrónico y de productividad de oficina, lenguajes de programación, gráficos, archivos de ingeniería y archivos comprimidos o almacenados. Las funciones de descubrimiento exploran el endpoint, el servidor de archivos, el almacenamiento de correo, el repositorio de Microsoft© SharePoint© Portal Server, incluyendo las aplicaciones de SaaS y el almacenamiento en la nube para ver dónde se ubican los datos de cumplimiento.
- Puntos de control de los datos en movimiento: Proporciona visibilidad y control de los datos en movimiento, ya sea en el correo electrónico, el correo web, la mensajería instantánea (IM), las aplicaciones de SaaS y la mayoría de protocolos de red como FTP, HTTP/HTTPS y SMTP.
- Puntos de control de los datos en uso: Proporciona visibilidad y control de los datos que se utilizan en puertos USB, CD, DVD, puertos COM y LPT, discos extraíbles, dispositivos infrarrojos y de creación de imágenes, PCMCIA y módems. También se puede configurar para supervisar las funciones de copiar y pegar y de impresión de pantalla

Vista granular de datos por medio de identificadores

- Además de las plantillas, Apex One™ DLP™ incluye una lista granular de identificadores verdaderamente internacionales para identificar datos específicos por patrones, fórmulas, posicionamiento y más. Los identificadores también pueden crearse desde cero.

Ventajas de Apex One™ DLP™

Puntos de protección

- Proteja sus datos, hoy
- Implemente DLP inmediatamente y recupere la visibilidad y el control de sus datos con rapidez

Reduzca los costos de DLP

- Ahorre en costos de mantenimiento e implementación en comparación con DLP tradicional

Proteja la privacidad

- Identifique, supervise e impida la pérdida de datos, dentro y fuera de la red
- Cumpla con las normativas
- Aplique controles de protección, visibilidad y aplicación

Forme a los usuarios

- Notifique a los empleados sobre conductas de riesgo o aplique controles de usuarios, si es necesario

ENDPOINT SENSOR

Proporciona un sistema de investigación y respuesta para endpoints (EDR) sensible al contexto que registra y genera informes detallados de las actividades a nivel del sistema para permitir que los analistas de amenazas valoren con rapidez la naturaleza y el alcance de un ataque. La detección, el sistema de inteligencia y los controles personalizados le permiten:Record detailed system-level activities

- Realizar registros detallados de las actividades a nivel de sistema
- Realizar búsquedas multicapa en todos los endpoints con múltiples criterios de búsqueda como OpenIOC, Yara y objetos sospechosos.
- Detectar y analizar indicadores de amenazas avanzadas, como los ataques fileless.
- Responder rápidamente antes de que se pierda información confidencial.

ENDPOINT ENCRYPTION

Garantiza la privacidad de la información mediante el cifrado de los datos almacenados en los endpoints, incluidos PC, Mac, DVD y unidades USB, que se pueden robar o extraviar con facilidad. Trend Micro™ Endpoint Encryption le proporciona la seguridad de datos que necesita con cifrado de disco completo, cifrado de carpetas y archivos y cifrado de soportes extraíbles.

- Automatiza la gestión de los datos con unidades de disco duro con cifrado automático.
- Cifra los datos en archivos específicos, carpetas compartidas y soportes extraíbles.
- Define políticas detalladas para el control de los dispositivos y la gestión de datos.
- Gestiona Microsoft Bitlocker y Apple FileVault.

TREND MICRO APEX CENTRAL

Esta consola de gestión de seguridad centralizada garantiza una gestión coherente de la seguridad, además de una visibilidad completa y funciones de creación de informes en las diferentes capas de seguridad interconectada de Trend Micro. También amplía la visibilidad y el control de todos los modelos de implementación, ya sean in situ, en la nube o híbridos.

La gestión centralizada se combina con la visibilidad basada en el usuario, lo que mejora la protección, reduce la complejidad y elimina las tareas redundantes y repetitivas de la administración de seguridad. Apex Central™ también proporciona acceso al sistema de inteligencia sobre amenazas procesable desde Trend Micro Smart Protection Network, que utiliza el sistema de inteligencia mundial sobre amenazas para ofrecer seguridad en tiempo real desde la nube, bloqueando las amenazas antes de que lleguen a su destino.

SECURITY FOR MAC

- Añade una capa de protección para los clientes Apple Mac de la red al impedir que accedan a sitios maliciosos y que distribuyan malware, incluso si el malware no está diseñado para atacar sistemas Mac OS X.
- Reduce la exposición a las amenazas web, incluido el malware de propagación rápida creado específicamente para Mac.
- Cumple los estándares de aspecto y sensación de funcionamiento del Mac OS X para ofrecer una experiencia de usuario positiva.
- Ahorra tiempo y esfuerzos gracias a la gestión centralizada de endpoints, incluyendo Macs.

Puntos de Protección

- Endpoints
- Servidores
- Dispositivos incrustados y de punto de venta (POS)

Protección frente a Amenazas

- Exploits de vulnerabilidades
- Aplicaciones maliciosas (ejecutables, DLL, controladores de dispositivos, tienda de aplicaciones de Windows®, etc.)
- Identifica, supervisa e impide la pérdida de datos, dentro y fuera de la red
- Cumpla con las normativas
- Aplique controles de protección, visibilidad y normativa

Forme a los usuarios

- Notifique a los empleados sobre conductas de riesgo o aplique controles de usuarios, si es necesario

REQUISITOS MÍNIMOS RECOMENDADOS PARA EL AGENTE

REQUISITOS MÍNIMOS RECOMENDADOS PARA EL AGENTE:

- Windows 7 (6.1)
- Windows 8/8.1 (6.2/6.3)
- Windows 10 (10.0)
- Windows Server 2008 R2 (6.1)
- Windows Server 2012 (6.2)
- Windows Server 2012 R2 (6.3)
- Windows Server 2016 R2 (10)
- Windows Server 2019
- macOS® Mojave 10.14
- macOS High Sierra 10.13
- macOS Sierra 10.12
- OS X® El Capitan 10.11
- OS X Yosemite 10.10 o posterior
- OS X Mavericks 10.9 o posterior

PLATAFORMA DEL AGENTE:

- Procesador: Intel® Pentium® a 300 MHz o equivalente (familia Windows 7, 8.1, 10) y procesador Intel® Core™ para Mac
- Intel Pentium a 1.0 GHz como mínimo (se recomiendan 2.0 GHz) o equivalente (Windows Embedded POSReady7)
- Intel Pentium a 1.4 GHz como mínimo (se recomiendan 2.0 GHz) o equivalente (Windows 2008 R2, familia Windows 2016, familia Windows 2019)

Memoria:

- 512 MB como mínimo (se recomiendan 2.0 GB) con al menos 100 MB exclusivamente para Apex One™ (familia Windows 2008 R2, 2012)
- 1.0 GB como mínimo (se recomiendan 2.0 GB) con al menos 100 MB exclusivamente para Apex One™ (familia Windows 7 (x86), 8.1 (x86), Windows Embedded POSReady 7, 10 (x64))
- 2.0 GB como mínimo (se recomiendan 4.0 GB) con al menos 100 MB exclusivamente para Apex One™ (familia Windows 7 (x64), 8.1 (x64), 10 (x64))
- 512 MB como mínimo para Apex One™ en Mac

Espacio en Disco:

- 1.5 GB como mínimo (se recomiendan 3GB para todos los productos) para Windows, 300MB como mínimo para Mac
- Endpoint Sensor requiere mínimo 2GB para plataforma Windows, 300MB para Mac.

Puede consultar online los requisitos detallados en **docs.trendmicro.com**

TREND MICRO™

Securing Your Connected World