

Todos los días, se registran más de 350.000 nuevos programas maliciosos (malware) y aplicaciones potencialmente no deseadas (PUA).¹ Los hackers apuntan a los endpoints vulnerables, donde las empresas almacenan sus activos más valiosos. ¿Con qué fin? Como suele suceder, **el motivo es obtener beneficios económicos**.

Las empresas dependen cada vez más de nuevas tecnologías, por lo que **están expuestas** a nuevos tipos de malware que **ponen en peligro** su seguridad. Esto, por supuesto, requiere de enfoques de seguridad que **reduzcan la superficie de ataque**.

EVOLUCIÓN DE ENTORNOS DE TI EMPRESARIALES

En los últimos años, la evolución de la tecnología, junto con el uso extendido de Internet, los dispositivos móviles, y el almacenamiento y las aplicaciones basados en la nube, han producido una verdadera revolución del entorno corporativo. Esta revolución, sin embargo, conlleva algunos riesgos. A pesar de que estas ventajas son un estímulo para las empresas, los criminales cibernéticos las aprovechan para sus actividades delictivas.

El aumento del número de ataques cibernéticos coincide con el aumento del valor de los activos digitales que las empresas almacenan. Esto significa también que los criminales cibernéticos ven posibilidades para aumentar sus propios beneficios económicos. El malware y el ransomware se han convertido en una de las amenazas más comunes, aunque paradójicamente, los costos directos no son el problema principal, sino los momentos sin conectividad que provocan. Esto obliga a las empresas a tomar medidas para mejorar su postura en cuanto a la seguridad.

PROTEJA SU EMPRESA CONTRA EL MALWARE Y EL RANSOMWARE

Panda Endpoint Protection Plus es una completa solución de seguridad avanzada para computadoras de escritorio, computadoras portátiles y servidores. Administra la seguridad de los endpoints de manera centralizada, tanto dentro como fuera de la red corporativa.

Este servicio ofrece un conjunto de tecnologías de EPP para controlar el malware, el ransomware y las amenazas que se aprovechan de las vulnerabilidades desconocidas (día cero). No es necesario instalar o mantener nuevos recursos de hardware en la infraestructura de la empresa.

Además, el agente ligero no afecta el rendimiento de endpoints y es posible acceder a través de una consola web única, lo que simplifica el mantenimiento de seguridad y aumenta la eficiencia operativa.



Figura 1: Acceso web y panel de control de correo no deseado.

BENEFICIOS

Seguridad de Múltiples Plataformas

- Seguridad contra amenazas avanzadas desconocidas: detecta y bloquea malware, troyanos, suplantación de identidad y ransomware.
- Seguridad para todos los vectores de ataque: exploradores, correo electrónico, sistemas de archivos y dispositivos externos conectados a endpoints.
- Análisis y desinfección automáticos de computadoras. Análisis de comportamiento para detectar malware conocido y desconocido.
- Seguridad para sistemas Windows, Linux, macOS, Android y entornos virtuales (VMware, Virtual PC, MS Hyper-V, Citrix), y también para infraestructuras de virtualización (VDI) tanto persistente como no persistente.

Aumento de la Productividad

- Supervisa y filtra el tráfico web, lo que impide que los empleados se vean involucrados en comportamientos improductivos o que sean víctimas de amenazas de seguridad, como los bots o la suplantación de identidad.
- No se requiere infraestructura o mantenimiento específicos; el departamento de TI puede concentrarse en tareas más importantes.

Administración Simplificada

- Fácil de mantener: no se requiere infraestructura específica para hospedar la solución, por lo que el departamento de TI puede concentrarse en tareas más importantes.
- Fácil de proteger usuarios remotos: cada computadora protegida con Panda Endpoint Protection Plus se comunica con la nube, mientras que las oficinas y los usuarios remotos obtienen protección rápida y sencilla, sin necesidad de instalaciones adicionales.
- Fácil de implementar: varios métodos de implementación que incluyen desinstaladores automáticos para los productos de la competencia con el fin de facilitar una rápida migración de soluciones de terceros.

SEGURIDAD DE ENDPOINTS CENTRALIZADA

Incluye administración centralizada de actualizaciones de seguridad y productos para todas las estaciones de trabajo y los servidores de la red corporativa. Administra la protección de los dispositivos Windows, Linux, macOS y Android desde una consola de administración única basada en la web.

¹ AV-Test: <https://www.av-test.org/en/statistics/malware/>

PROTECCIÓN CONTRA MALWARE Y RANSOMWARE

Panda Endpoint Protection Plus analiza los comportamientos y las técnicas de los ataques informáticos para detectar y bloquear tanto el malware conocido como el desconocido, y también los ataques de ransomware, troyanos y suplantación de identidad. Además, la solución Malware Freezer congela el malware detectado durante siete días y, en caso de detectar un falso positivo, restablece de manera automática el archivo afectado al sistema.

DESINFECCIÓN AVANZADA

En el caso de que se produzca una vulnerabilidad de seguridad, Panda Endpoint Protection Plus permite a las empresas restaurar rápidamente el estado de las computadoras afectadas anterior a la infección, gracias a las herramientas avanzadas de desinfección y cuarentena, que almacenan los elementos sospechosos y eliminados. Además, permite a los administradores reiniciar de manera remota estaciones de trabajo y servidores para garantizar que queden instaladas las últimas actualizaciones de los productos.

SUPERVISIÓN Y FILTRADO WEB

Supervisión de seguridad de red detallada en tiempo real a través de paneles de control integrales y gráficos fáciles de interpretar.

El filtrado web aumenta la productividad de la empresa y supervisa la actividad para impedir el acceso a URL peligrosas o inproductivas.

CONTROL CENTRALIZADO DE DISPOSITIVOS

Detiene el malware y las filtraciones de información, ya que bloquea categorías completas de dispositivos (unidades flash, módems USB, cámaras web, DVD/CD, etc.), clasifica dispositivos en listas blancas o configura permisos de acceso de solo lectura, solo escritura y lectura, y escritura. Además, bloquea cualquier tipo de actividad que pueda considerarse riesgosa.

INSTALACIÓN RÁPIDA Y FLEXIBLE

Implemente la protección a través del correo electrónico con una URL de descarga o de manera silenciosa en endpoints seleccionados mediante el uso de la herramienta de distribución de la solución. Instalador de MSI compatible con herramientas de terceros (Active Directory, Tivoli, SMS, etc.).

COMPATIBLE CON ISO 27001 Y SAS 70, DISPONIBILIDAD GARANTIZADA LAS 24 HORAS, LOS 7 DÍAS A LA SEMANA

La solución se hospeda en Aether, la plataforma con garantía completa de protección de datos. Nuestros centros de datos tienen certificación de ISO 27001 y SAS 70, lo que permite a los clientes evitar costosas interrupciones de servicio e infecciones de malware.

PLATAFORMA DE ADMINISTRACIÓN EN LA NUBE

Plataforma Aether

La plataforma en la nube Aether y su consola de administración, que comparten todas las soluciones de endpoint de Panda Security, optimizan la administración de la seguridad avanzada adaptable, tanto dentro como fuera de la red. Está diseñada con mínima complejidad y máxima flexibilidad, granularidad y escalabilidad.

Logre Más en Menos Tiempo. Fácil Implementación

- Se implementa, instala y configura en minutos. Máximo valor desde el primer día.
- Agente único y ligero para todos los productos y todos los sistemas (Windows, macOS, Linux y Android).
- Detección automática de endpoints desprotegidos. Instalación remota.
- Tecnologías patentadas de proxy y de repositorio/caché. Comunicación optimizada, incluso con endpoints sin conexión a Internet.

Operaciones Simplificadas Que Se Adaptan a Su Organización

- Consola web intuitiva. Administración flexible y modular que reduce el costo total de propiedad.
- Usuarios con visibilidad y permisos completos o restringidos. Auditorías de actividades.
- Políticas de seguridad por endpoints y por grupos. Roles predefinidos o personalizados.
- Inventario de hardware y software, y registro de cambios.

Fácil Implementación de Capacidades de Seguridad y Administración con el Tiempo

- No se requiere nueva infraestructura para implementar módulos. Sin costos de implementación.
- Comunicación con endpoints en tiempo real desde una consola única de administración web.
- Reportes, paneles de control e indicadores detallados para cada módulo.

Soluciones compatibles en la plataforma Aether:

 Panda Endpoint Protection  Panda Endpoint Protection

Estaciones de trabajo y servidores de Windows:
<http://go.pandasecurity.com/endpoint-windows/requirements>

Dispositivos macOS:
<http://go.pandasecurity.com/endpoint-macos/requirements>

Estaciones de trabajo y servidores de Linux:
<http://go.pandasecurity.com/endpoint-linux/requirements>

Dispositivos móviles de Android:
<http://go.pandasecurity.com/endpoint-android/requirements>