avast business
powered by AVG and Avast

Soluciones Endpoint Protection

Protección integral para dispositivos, datos y personas

Las soluciones Endpoint Protection de Avast Business, integradas en la red de detección de amenazas de mayor tamaño y más extendida a escala internacional que existe, proporcionan una protección superior de nivel empresarial que mantiene a las pequeñas y medianas empresas a salvo de las amenazas actuales y futuras.

FOLLETO

En los números está la seguridad.

Nuestros más de 400 millones de usuarios activos proporcionan un flujo de datos continuo que nos ayuda a identificar y destruir rápidamente cualquier amenaza, así como a predecir las amenazas futuras. Nuestro inmenso motor de aprendizaje automático basado en la nube evoluciona y aprende en todo el planeta, tanto de día como de noche, para conseguir que nuestras soluciones sean más inteligentes y rápidas, además de más potentes que nunca.

INFORMACIÓN MÁS INTELIGENTE

Nuestra nube de seguridad comprueba más de 200 mil millones de URL y un millón de archivos ejecutables nuevos al día. Evitamos 3,5 mil millones de ataques de malware cada mes. Cada vez que alguien descarga un archivo, nosotros aprendemos, lo que nos otorga un conocimiento valioso sobre amenazas nuevas y emergentes.

INSPECCIÓN MÁS DETALLADA

Nuestro analizador inteligente en tiempo real pone en cuarentena de inmediato los archivos sospechosos con un comportamiento desconocido y se pone manos a la obra diseccionando el archivo para analizarlo con más detalle. Nuestra capacidad para aislar los archivos cuestionables nos permite evitar los ataques de día cero mejor que cualquier solución disponible en el mercado.

DETECCIÓN MÁS RÁPIDA

Están apareciendo nuevas variantes de malware a un ritmo alarmante, por lo que la detección rápida es vital. Nuestra tecnología puede identificar en pocos segundos variantes de malware y de ataques de día cero en un dispositivo y desarrollar actualizaciones para toda nuestra red inmediatamente.

Cómo funciona

Sistema de defensa formado por cuatro escudos

Estos componentes colaboran para analizar la información sospechosa que llega a los dispositivos y sale de ellos, además de bloquear los archivos maliciosos, los sitios web peligrosos, el comportamiento poco habitual, las conexiones no autorizadas y otras amenazas.

Escudo web | **Escudo de archivos** | **Escudo de correo electrónico** | **Escudo de comportamiento** | **CyberCapture**

CyberCapture

CyberCapture sube el listón considerablemente en lo que se refiere a protección frente a ataques de día cero. Es una defensa esencial frente a variantes de malware nuevas, desconocidas y poco habituales. Su funcionamiento consiste en incautar, o «capturar», todos los archivos que no se hayan visto anteriormente para realizar un análisis más detallado en un entorno seguro en la nube.

Bloquear • Aislar • Analizar

128 millones de ataques de ransomware bloqueados

Con más de 400 millones de usuarios en 45 países, identificamos amenazas nuevas cada 6 o 7 minutos y publicamos actualizaciones en nuestra red en tiempo real.

Soluciones Endpoint Protection

Antivirus

Avast Business Antivirus es una solución antivirus completa para pymes que mantiene todos los dispositivos del usuario final que estén conectados a la red a salvo de sofisticadas amenazas en línea, ya sea una variante de ransomware conocida o un ataque de día cero que no se haya visto nunca.

Antivirus Pro

Avast Business Antivirus Pro incluye todas las capacidades de Avast Business Antivirus y, además, actualizaciones de software automáticas, destrucción de datos para eliminar archivos permanentemente y seguridad adicional para los servidores.

Antivirus Pro Plus

Avast Business Antivirus Pro Plus cuenta con las capacidades de Antivirus y Antivirus Pro, pero, además, incluye una protección adicional de identidad y datos cuya función es proteger a los usuarios y las conexiones en redes públicas y abiertas.

Consola de Administración

La consola de gestión facilita la implementación de una protección antivirus en varios dispositivos, la administración de todos ellos desde un único lugar, la programación de análisis periódicos y la opción de añadir más dispositivos rápidamente.

Funciones

dispositivo

	Antivirus	Antivirus Pro	Antivirus Pro Plus CloudCare
Escudo de archivos Analiza todos los archivos que se abren o descargan para asegurarse de que no estén infectados con malware.	●	●	●
Escudo web Comprueba los certificados y las URL de los sitios web para cerciorarse de que sean seguros antes de que se establezca una conexión de red.	●	●	●
Escudo de correo electrónico Examina tanto los mensajes de correo electrónico entrantes como los salientes para asegurarse de que no contengan ningún tipo de malware.	●	●	●
Escudo de comportamiento Busca comportamientos sospechosos en programas instalados en los dispositivos que puedan indicar la presencia de código malicioso.	●	●	●
CyberCapture Detecta y analiza archivos sospechosos y poco habituales en un entorno virtual seguro.	●	●	●
Cortafuegos Supervisa todo el tráfico de la red entre el PC y el mundo exterior para evitar que se produzcan comunicaciones no autorizadas.	●	●	●
Antispam Impide que los correos electrónicos de phishing peligrosos y el molesto spam se acumulen en la bandeja de entrada y la pongan en peligro.	●	●	●
Análisis inteligente Busca todos esos resquicios que permiten que se cuele el malware: desde configuraciones y contraseñas no seguras hasta complementos sospechosos.	●	●	●

	Antivirus	Antivirus Pro	Antivirus Pro Plus
Sandbox Aísla archivos sospechosos en un entorno virtualizado seguro para que tanto usted como el Laboratorio de virus de Avast puedan analizarlos más a fondo.	●	●	●
Inspector de Wi-Fi Analiza las redes en busca de vulnerabilidades, comprueba la configuración de las redes, los dispositivos y el router e identifica amenazas.	●	●	●
Sitio web legítimo Protege frente al secuestro de DNS (sistema de nombres de dominio) para garantizar que acceda al sitio web que desea visitar.	●	●	●
Disco de rescate Permite arrancar un PC infectado por malware mediante un USB que contiene una versión limpia del sistema.	●	●	●
Extensión de seguridad del navegador Analiza los sitios web para comprobar su reputación y autenticidad, bloquea anuncios y le ofrece una protección aún más segura cuando realiza operaciones bancarias en Internet.	●	●	●
datos			
Actualizador de software Mantiene actualizado el software más usado de otros fabricantes para eliminar posibles riesgos de seguridad.	○	●	●
Destructor de datos Sobrescribe archivos varias veces para eliminar permanentemente información confidencial de forma que no se pueda recuperar.	○	●	●
Protección de servidores Exchange Analiza y filtra los correos electrónicos en el servidor Exchange para detener posibles ataques antes de que se propaguen por la red.	○	●	●
Protección de servidores SharePoint Analiza todos los archivos cargados en el espacio compartido de almacenamiento para garantizar que ningún malware ponga en peligro sus datos.	○	●	●
identidad			
Passwords Protege los datos de inicio de sesión de los empleados con una contraseña principal segura. Incluye un complemento para el navegador que rellena datos de forma automática y segura.	○	○	●
SecureLine VPN Cifra los datos y protege la conexión al usar redes wi-fi públicas, como las de cafeterías o aeropuertos.	○	○	●
Limpieza del navegador Analiza los navegadores en busca de complementos de baja reputación y elimina las cookies que contienen información personal.	○	○	●
Escudo de webcam Impide que las aplicaciones y el malware accedan a la webcam del equipo sin su consentimiento.	○	○	●

Requisitos del sistema

PC: Windows 10, 8.1,8,7, Vista, or XP SP3*
Servidor: Windows Server 2016, 2012 R2, or 2008 R2**
Procesador: Intel Pentium 4/AMD Athlon 64 CPU que admita las instrucciones de SSE2
Memoria: Al menos 256 MB de RAM y 2 GB de espacio en el disco duro
Resolución de pantalla: No inferior a 800 x 600 píxeles

MacOS: 10.9 (Mavericks) o versiones posteriores con al menos 500 MB de espacio en disco
Resolución de pantalla: No inferior a 800 x 600 píxeles

Consola de gestión

Consola en la nube

La consola de gestión de Avast Business es compatible con Internet Explorer 11, Microsoft Edge y con todas las ramas de mantenimiento actualmente compatibles de Windows 10.

Local

Consola de versiones de Windows

Sistema operativo:
Windows 10 Windows 8.x (escritorio)
Windows 7 SP1
Windows Server 2008 R2 SP1
Windows Server 2012 y 2012 R2
Windows Server 2016, cualquier edición con SP

Requisitos de hardware:
RAM: 2 GB (se recomiendan 4 GB)
Espacio en disco: 6 GB
Procesador: 2 GHz, como mínimo

Consola de versiones de Docker

Requisitos de software:
Cualquier sistema operativo que ejecute Docker (Linux, Mac OS, Windows)
Docker Engine 1.10.0 o versiones posteriores
Docker Compose 1.6.0 o versiones posteriores

Requisitos de hardware:
RAM: 2 GB (se recomiendan 4 GB)
Espacio en disco: 6 GB
Procesador: 2 GHz, como mínimo

Acerca de Avast Business

Avast Business ofrece soluciones de seguridad integradas y de nivel empresarial de terminales y redes para pymes y proveedores de servicios de TI. Con la cartera de productos de seguridad de Avast Business, avalada por la red de detección de amenazas de mayor tamaño y más extendida a escala internacional, es muy fácil y asequible proteger, administrar y supervisar entornos tecnológicos complejos. El resultado es una protección superior en la que las empresas pueden confiar.

Para obtener más información sobre nuestros servicios gestionados y nuestras soluciones de ciberseguridad, visite **www.avast.com/business/endpoint-protection.**

avast business

BR-EPP-18-10