Avast Business

zaltor Software Distribution

Ficha técnica

Avast Ultimate Business Security

Avast Ultimate Business Security combina nuestro galardonado antivirus de última generación[1] con herramientas de privacidad en línea y software de automatización de la administración de parches para que sus dispositivos, datos y aplicaciones se mantengan actualizados y protegidos.

Ciberseguridad integral y automatización de parches para empresas en crecimiento

Administración remota

Administre los dispositivos y la seguridad a medida que crece

A medida que su empresa crece, también lo hacen sus necesidades de seguridad. Con nuestra plataforma de administración en línea, puede controlar todos los dispositivos, los servicios de seguridad de Avast y sus suscripciones de manera centralizada, en cualquier momento y lugar.

Protección del dispositivo

Proteja los dispositivos de su empresa contra los ciberataques

Los ordenadores y servidores son puntos de entrada clave para los datos empresariales. Refuerce su seguridad frente a amenazas como las infecciones de malware, las ralentizaciones que estas provocan y los usos indebidos de sus dispositivos, estén o no conectados. Consiga más tranquilidad con el antivirus de última generación de Avast, con seis escudos de protección y una red de detección de amenazas con tecnología de IA y protección de USB.

Protección de datos

Evite el ransomware y las filtraciones de datos, incluso desde dentro

Proteja los datos de su empresa y de sus clientes contra filtraciones, cifrados y tiempos de inactividad con cortafuegos y varios escudos protectores. Además, nuestra seguridad por capas se extiende a los dispositivos USB para evitar el robo y la filtración de datos confidenciales.

Seguridad y privacidad en línea

Evite el phishing, los sniffers, las estafas y otras amenazas en línea

Nunca se sabe a qué redes wifi y sitios web pueden acceder los empleados remotos. Limite sus actividades en línea para que sean seguras y privadas, sigan siendo productivos y trabajen con tranquilidad estén donde estén.

Administración de parches

Ahorre tiempo y elimine vulnerabilidades de software mediante la aplicación automática de parches

Los ciberdelincuentes aprovechan las vulnerabilidades sin parches en las aplicaciones y los sistemas operativos más utilizados (Java, Adobe, Google Chrome, Zoom, etc.) para lanzar ataques selectivos. Administración de parches corregirá de forma automática[2] las vulnerabilidades del sistema Windows y de las aplicaciones de terceros para mantener la seguridad de su empresa en línea.

[1]AV-TEST, «Evaluación del producto e informe de certificación: Protección de terminales corporativa aprobada para Windows» Avast Ultimate Business Security 22.12, enero-febrero de 2023.

[2]AV-Comparatives, Premio de Producto de seguridad aprobado para empresas para Avast Ultimate Business Security, diciembre de 2022.

Avast Business

Funciones

Protección del dispositivo

Escudo de archivos
Analiza en tiempo real los programas y archivos guardados en el PC en busca de amenazas perjudiciales antes de permitir que se abran, ejecuten, modifiquen o guarden. Si se detecta malware, el Escudo de archivos evita que el programa o el archivo infecten el PC.

Escudo Web
Se encarga de analizar en tiempo real los datos que se transfieren al navegar por Internet a fin de evitar que se descargue y se ejecute en el PC malware, como scripts maliciosos.

Escudo de correo electrónico
Analiza en tiempo real los mensajes de correo electrónico entrantes y salientes para detectar contenido malicioso como, por ejemplo, virus. El análisis solo se aplica a los mensajes enviados o recibidos mediante clientes de correo electrónico de escritorio, como Microsoft Outlook o Mozilla Thunderbird.

Escudo de comportamiento
Supervisa en tiempo real todos los procesos del PC en busca de comportamientos sospechosos que puedan indicar la presencia de código malicioso. Está diseñado para detectar y bloquear archivos sospechosos a partir de su similitud con otras amenazas conocidas, incluso si aún no se han añadido a la base de datos de definiciones de virus.

Sandbox
Permite navegar por Internet o ejecutar una aplicación en un entorno totalmente aislado y seguro. Cuando una aplicación se ejecuta en Sandbox, la actividad y el contenido web quedan «encerrados», lo que impide daños en el PC. Esto es útil cuando queremos ejecutar aplicaciones sospechosas o que no son de confianza sin correr riesgos.

CyberCapture
Detecta y analiza archivos raros y sospechosos. Si intenta ejecutar un archivo de ese tipo, CyberCapture lo bloquea en el PC y lo envía al Laboratorio de virus de Avast para que se analice en un entorno virtual seguro.

Análisis inteligente
Lleva a cabo análisis en busca de malware, aplicaciones no actualizadas, configuraciones poco seguras y complementos sospechosos.

Disco de rescate
Permite analizar sus PC antes de que arranque el sistema. Este método aumenta de forma significativa las posibilidades de detectar y eliminar el malware, ya que de esta forma no puede contraatacar. Si sospecha que el PC tiene una infección de malware y ninguno de los otros análisis de antivirus ha podido resolver el problema, puede usar el Disco de rescate.

Avast Business

Protección de datos y redes

Cortafuegos avanzado
Supervise el tráfico de red entre los dispositivos de sus empleados e Internet. Mejore el bloqueo de transmisiones de datos peligrosas o innecesarias para proteger mejor su empresa contra la manipulación malintencionada de datos.

Escudo de ransomware
Refuerce la protección de sus datos confidenciales y otros documentos críticos para que los ataques de ransomware no puedan alterarlos, eliminarlos ni cifrarlos. Elija qué aplicaciones tienen permiso para acceder a sus carpetas protegidas y bloquee el resto.

Escudo de acceso remoto
Evite exploits del Protocolo de escritorio remoto (RDP) y ataques de fuerza bruta. Le permite establecer quién tiene acceso remoto a los terminales y bloquear conexiones no autorizadas.

Inspector de red
Protege la red para evitar que los atacantes accedan a ella y hagan un uso indebido de sus datos. Comprueba el estado de su red, los dispositivos conectados a ella y la configuración del router para identificar posibles problemas de seguridad que puedan dejar paso a amenazas.

Destructor de datos
Permite borrar de forma definitiva los archivos o las unidades para que nadie pueda restaurarlos y hacer un uso indebido de los datos.

Protección de SharePoint Server
Comprueba todos los archivos cargados en el almacenamiento compartido para evitar que el malware ponga en peligro sus datos.

Protección de Exchange Server
Analiza y filtra los correos electrónicos en el servidor Exchange para detener posibles ataques antes de que se propaguen por la red.

Protección de USB[1]
Evite que los trabajadores utilicen dispositivos de almacenamiento extraíbles no autorizados, como unidades flash, unidades externas, tarjetas de memoria, etc. Bloquee, controle y supervise los puertos USB para evitar el robo de datos y las infecciones de malware.

Avast Business

Online Security & Privacy

Sitio web legítimo
Sus trabajadores pueden navegar y realizar operaciones bancarias con mayor seguridad evitando sitios web falsos creados para robar datos confidenciales, como nombres de usuario, contraseñas y datos de tarjetas de crédito. Se ha diseñado para proteger a los usuarios contra el secuestro de DNS (sistema de nombres de dominio).

Extensión de navegador de seguridad
Analiza la reputación y autenticidad de los sitios web, bloquea los anuncios y pone los dispositivos en un «modo superseguro» para una mayor privacidad.

Limpieza del navegador
Analiza los navegadores en busca de complementos de baja reputación y elimina las cookies que contienen información personal.

Protección de contraseñas
Protege la información de inicio de sesión de sus trabajadores almacenada en los navegadores web contra el robo y el uso indebido. Se ha diseñado para evitar que las aplicaciones y el malware manipulen las contraseñas que se guardan en los navegadores Google Chrome, Mozilla Firefox, Microsoft Edge y Avast Secure Browser.

Escudo de webcam
Evita que las aplicaciones y el malware accedan a la webcam del PC sin el consentimiento del usuario. El Escudo de webcam permite impedir que aplicaciones que no son de confianza capturen imágenes o vídeos y pongan en riesgo la privacidad de los usuarios.

Monitor de actividad en línea
Cree un entorno empresarial más seguro y productivo para usted y sus trabajadores controlando su acceso a sitios web potencialmente peligrosos o no relacionados con el trabajo mediante el filtrado de contenidos y dominios web.[1]

VPN
La VPN personal sin límite de datos cifra el tráfico de datos en Internet para proteger los datos de sus trabajadores. También protege la privacidad cuando se utilizan redes wifi públicas como las de las cafeterías y los aeropuertos.

Funciones de Administración de parches[2]

Programación flexible de implementaciones
Programe e implemente los parches a la hora que desee, o bien hágalo manualmente en grupos de dispositivos o en dispositivos individuales.

Panel centralizado
Administre todos los parches de software y consulte resúmenes gráficos de los instalados, los que faltan y los que presenten errores en cualquier dispositivo.

[1] *Se requiere Avast Business Hub, una plataforma de administración en línea.*

Avast Business

Parches personalizables
Elija los parches que desea buscar e instalar en función del proveedor de software, el producto o la gravedad del parche. Cree fácilmente exclusiones para determinadas aplicaciones.

Miles de parches
Implemente parches para sistemas operativos Windows y miles de aplicaciones de software de terceros para disfrutar de protección integral y mantener al día sus dispositivos.

Funcionalidades de agentes maestros
Descargue todos los parches que faltan en un agente maestro que los distribuirá sin interrupciones entre todos los dispositivos gestionados de la red.

Informes exhaustivos
Determine el estado y la seguridad del software de un dispositivo gracias a una gran variedad de informes que se pueden configurar.

Análisis automáticos
Programe análisis de parches para que se ejecuten cada 24 horas y seleccione los parches que quiera implementar de forma automática en el día y la hora que prefiera. Esta configuración predeterminada se puede personalizar en cualquier momento.

[2]Actualmente, Administración de Parches solo está disponible para Windows. Para utilizar Administración de Parches se requiere Avast Business Hub, una plataforma de administración en línea.

Disponible con Avast Business Hub, nuestra plataforma de administración en línea

Detecte ciberamenazas en tiempo real, acceda a informes completos y use funciones administrativas directamente desde su navegador web. Nuestra consola en la nube le permite administrar de forma centralizada sus servicios de seguridad de Avast Business y sus suscripciones.

Gestión en las instalaciones locales no disponible.

Funciones de Avast Business Hub (plataforma de administración en línea):

- Panel de control intuitivo
- Informes exhaustivos
- Administración de dispositivos y políticas
- Alertas y notificaciones centralizadas
- Comandos en tiempo real
- Detección de redes e implementación remota
- Acceso remoto básico y herramienta de soporte
- Asistencia multiinquilino

Servicios integrados (disponibles como complementos en Business Hub)

- Control remoto Premium
- Copia de seguridad en la nube

Avast Business

Acerca de Avast Business

Avast ofrece soluciones de ciberseguridad fáciles de usar, asequibles y galardonadas para empresas pequeñas y en crecimiento. Avast proporciona servicios de seguridad integrados para proteger sus dispositivos, datos, aplicaciones y redes. Respaldados por 30 años de innovación, contamos con una de las redes de detección de amenazas más grandes y distribuidas por todo el mundo. Nuestras soluciones proporcionan la máxima protección para que las ciberamenazas le preocupen menos y pueda centrarse en el crecimiento de su empresa. Para obtener más información sobre nuestras soluciones de ciberseguridad, visite **www.avast.com/business**.