Kaspersky® Endpoint Security for Business

Advanced

Kaspersky Endpoint Security for Business Advanced combina seguridad a varios niveles con herramientas de control ampliadas herramientas para ofrecer una solución de seguridad eficaz que se adapta rápidamente para proteger contra las nuevas amenazas. Los niveles adicionales de defensa ayudan a las empresas a eliminar vulnerabilidades y hacen aún más para proteger los datos confidenciales. Y todas las funciones se controlan mediante una única consola de gestión fácil de utilizar.

Las funciones de protección y gestión que necesita

Kaspersky Lab ha incorporado potentes funciones empresariales en los niveles progresivos de nuestros productos. Nos hemos asegurado de que el uso de la tecnología es sencillo e idóneo para empresas de cualquier tamaño.

¿Qué nivel de protección es el más adecuado para usted?

- SELECT
- **ADVANCED**
- TOTAL

Varias capas de protección para

- Windows, Linux y Mac
- Servidores de Windows y Linux
- Contenedores de Windows Server
- Android y otros dispositivos móviles
- Medios de almacenamiento extraíbles

Seguridad inigualable contra

- Exploits de software
- Ransomware
- Malware móvil
- Amenazas avanzadas
- Amenazas sin archivos
- Ataques de PowerShell y basados en scripts
- Amenazas web

Funciones incluidas

- Antimalware mejora
- Gestión de vulnerabilidades
- Aprendizaje mecánico dinámico novedad
- Aislamiento de procesos
- Firewall
- Gestión de firewalls del sistema operativo novedad
- Protección con asistencia en la nube
- Agente de EDR integrado novedad
- Control de aplicaciones mejora
- Listas blancas dinámicas
- Control web
- Control de dispositivos mejora
- Protección del servidor mejora
- Protección para servidores terminales mejora
- Gestión de la movilidad empresarial mejora
- Seguridad de endpoints móviles mejora
- Cifrado
- Gestión del cifrado del sistema operativo mejora
- Configuración e implementación del sistema mejora
- Gestión de parches mejora
- Generación de informes mejora

Seguridad mejorada con gestión ampliada y protección de datos

Una consola de gestión

Desde la consola de gestión o "panel de control", los administradores pueden ver y gestionar todo el panorama de seguridad y aplicar las políticas de seguridad que haya elegido a cada endpoint de su empresa. La implementación de soluciones de seguridad es rápida y entraña mínimas interrupciones y complicaciones gracias a nuestra amplia gama de casos preconfigurados.

Seguridad eficaz

El producto está diseñado para poder utilizarse en cualquier entorno de IT. Emplea una pila completa de tecnologías probadas y de última generación. Los sensores integrados y la integración con Endpoint Detection and Response (EDR) permiten la captura y el análisis de grandes volúmenes de datos para detectar incluso los ciberataques más oscuros y sofisticados.

Un único producto, sin costes ocultos

Con varias tecnologías de seguridad integradas en un solo producto, no hay costes ocultos. Un producto significa una licencia, y todo lo que necesita para proteger su entorno de IT.

Un líder reconocido

Solo en 2017, los productos de seguridad de Kaspersky Lab participaron en 86 análisis independientes, lograron 72 primeros puestos y quedaron 78 veces entre los tres primeros. Los principales analistas mundiales reconocen el liderazgo de nuestra solución para endpoints.

Características principales

Controles de endpoints compatibles con la nube

Control de aplicaciones mejorado
Reduce su exposición a los ataques en servidores, dispositivos móviles y equipos, proporcionando así un control total del software que se puede ejecutar y cuándo, con las funciones de marcado dinámico en lista blanca de nuestro laboratorio interno. Los escenarios de permisos predeterminados y denegaciones predeterminadas son compatibles.

Prevención de intrusiones en el host
Regula el acceso a los datos confidenciales y los dispositivos de registro mediante el uso de la base de datos de reputación en el entorno local y la nube (Kaspersky Security Network) sin influir en el rendimiento de las aplicaciones autorizadas.

Control de dispositivos, control web, etc.

Cifrado y protección de datos

Cifrado exhaustivo
Los equipos de seguridad pueden aplicar de manera centralizada la función de cifrado certificada según el estándar FIPS 140-2 en el nivel de archivo, disco o dispositivo, y gestionar las herramientas de cifrado nativo como Microsoft BitLocker y macOS FileVault.

Creación de políticas integradas y exclusivas
La integración exclusiva del cifrado con controles de aplicaciones y dispositivos proporciona un nivel adicional de seguridad y una mayor facilidad administrativa.

Protección contra amenazas orientada al futuro

Detección del comportamiento y restauración automática
Identifica y protege contra amenazas avanzadas, incluidos ransomware, ataques sin archivos y apropiaciones de cuentas administrativas. La detección del comportamiento bloquea los ataques, mientras que la restauración automática revierte los cambios ya realizados.

Protección contra cifrado para carpetas compartidas
Un exclusivo componente anticifrado que puede bloquear el cifrado de archivos en los recursos compartidos del proceso malicioso que se ejecuta en otra máquina de la misma red.

Protección para contenedores y servidores de terminal
Protege los contenedores de Windows Server y una amplia variedad de entornos de acceso remoto, incluidos Microsoft Terminal Services y Citrix XenApp/Xen Desktop. El componente Seguridad del tráfico proporciona protección para el tráfico web y de correo electrónico en el servidor de terminal.

Prevención de exploits, tecnología Anti-Rootkit, etc.

Funciones de seguridad móvil

Innovadoras tecnologías antimalware
La combinación de tecnologías de detección basadas en el aprendizaje automático, proactivas y con asistencia en la nube proporciona protección en tiempo real. Mayor seguridad gracias a una navegación segura y análisis a petición y programados.

Implementación con tecnología de abastecimiento inalámbrica (OTA), etc.

Gestión de sistemas, vulnerabilidades y parches

gestión de parches
Análisis exhaustivo avanzado de vulnerabilidades combinado con la distribución automatizada de parches.

Ahorro de tiempo de implementación de sistema operativo y software
Cree, almacene e implemente imágenes del sistema desde una ubicación central. Esta posibilidad es ideal para la migración a Microsoft Windows 10, por ejemplo, o la implementación de 150 aplicaciones populares identificadas por Kaspersky Security Network.

Gestión de hardware, software y licencias
Los informes de inventario de hardware y software contribuyen a mantener el control de las obligaciones de licencia de software. Así podrá ahorrar costes gracias al abastecimiento central de derechos de software.

Mantenimiento y asistencia

Con operaciones en más de 200 países y 35 oficinas en todo el mundo, nuestros equipos de Professional Services están preparados para asegurarse de que pueda sacar el máximo provecho de su instalación de seguridad de Kaspersky Lab.

Prueba gratuita

Descubra por qué solo True Cybersecurity combina la facilidad de uso con la inteligencia de **HuMachine™** para proteger su empresa frente a todo tipo de amenazas. Visite la página y obtenga una prueba gratuita de 30 días de la versión completa de **Kaspersky Endpoint Security for Business**.

Kaspersky Lab Iberia
Encuentre un partner próximo: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
Noticias de seguridad de IT: **business.kaspersky.com/**
Nuestro enfoque exclusivo:
https://www.kaspersky.es/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.es