KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT

Potentes controles granulares y de terminales combinados con seguridad proactiva y administración para dispositivos móviles y datos

Control de aplicaciones, páginas web y dispositivos, incluidas las listas blancas dinámicas del laboratorio interno único de Kaspersky, que añaden una dimensión más profunda de seguridad a los terminales. Los dispositivos móviles de propiedad corporativa y del empleado (BYOD) también están seguros y las plataformas están unificadas para su administración mediante la consola de Kaspersky Security Center. La protección del servidor de archivos garantiza que la infección no se extienda a través de los datos almacenados hacia los endpoints protegidos.

CONTROLES PARA ENDPOINTS

Control de aplicaciones con lista blanca dinámica: el uso de reputaciones de archivo en tiempo real suministradas por la red de Kaspersky Security, permite que los administradores de TI bloqueen o regulen las aplicaciones, incluso si se opera en una situación de "negación predeterminada" en un escenario de lista blanca en un entorno en marcha o de prueba. El control de privilegios de aplicaciones y la detección de vulnerabilidades controlan las aplicaciones y restringen aquellas con comportamiento sospechoso.

Control web: se pueden crear políticas de exploración a partir de categorías preestablecidas o personalizables, asegurando una amplia función de supervisión y eficiencia administrativas.

Control de dispositivos: se pueden establecer, planificar y aplicar políticas de datos granulares que controlan la conexión de dispositivos de almacenamiento extraíbles y otros dispositivos periféricos, con el uso de máscaras para la implementación simultánea en múltiples dispositivos.

SEGURIDAD DE SERVIDOR DE ARCHIVOS

Se administra junto con la seguridad de terminales a través de Kaspersky Security Center.

SEGURIDAD MÓVIL:

Potente seguridad para dispositivos móviles: tecnologías avanzadas, proactivas y asistidas por nube que se combinan para ofrecer protección en tiempo real y de múltiples capas para terminales móviles.

Los componentes de protección web, antispam y antiphishing aumentan aún más la seguridad del dispositivo.

Antirrobo remoto: bloqueo, borrado, seguimiento de SIM, alarma, foto y borrado completo o selectivo, son funciones que evitan el acceso no autorizado a datos corporativos en caso de que un dispositivo se pierda o sea robado. La habilitación de administradores y usuarios finales, junto con la compatibilidad con Google Cloud Management , ofrece una rápida activación si es necesario.

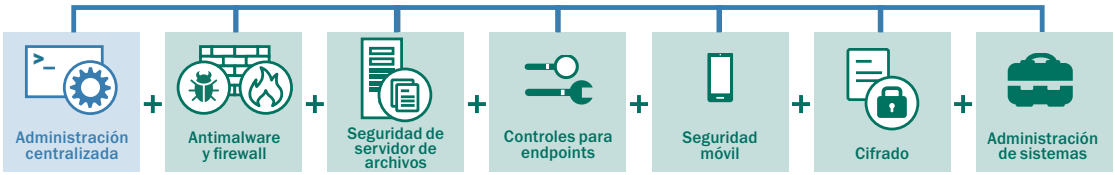
Administración de aplicaciones móviles (MAM): limita el acceso del usuario a ejecutar las aplicaciones de la lista blanca, evitando la implementación de software desconocido o no deseado. La "**envoltura de aplicaciones**" aísla los datos corporativos en los dispositivos que son propiedad de los empleados. La codificación adicional o el "borrado selectivo" se pueden aplicar remotamente.

Administración de dispositivos móviles (MDM): una interfaz unificada para dispositivos **Microsoft® Exchange ActiveSync** y **iOS MDM** con implementación de políticas OTA (por aire). También existe compatibilidad con dispositivos **Samsung KNOX** para Android™.

Portal de autoservicio: permite el registro de automático de los dispositivos de propiedad de empleados aprobados en la red, con instalación automática de todos los certificados y claves necesarios, y activación de emergencia de usuario/propietario de la funciones antirrobo, reduciendo la carga administrativa de TI.

Kaspersky Endpoint Security for Business – SELECT también incluye todos los componentes del nivel CORE.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED



Las herramientas de administración de sistemas optimizan la eficiencia y la seguridad de las TI, a la vez que el cifrado integrado protege los datos confidenciales

La administración automatizada de parches, la administración de imágenes del sistema operativo, la distribución remota de software y la integración SIEM; todo esto ayuda a optimizar la administración, a la vez que los inventarios de hardware y software y la administración de las licencias proporcionan visibilidad y control. La tecnología de cifrado integrada añade una potente capa de protección de datos.

ADMINISTRACIÓN DE SISTEMAS

Vulnerabilidad y administración de parches: detección y priorización automatizada de vulnerabilidades del sistema operativo, combinadas con la rápida distribución automatizada de parches y actualizaciones.

Implementación del sistema operativo: creación, almacenamiento e implementación sencilla de imágenes "golden" del sistema operativo desde una ubicación central, incluida compatibilidad con UEFI.

Distribución de software y solución de problemas: implementación remota de software, y actualización del sistema operativo y aplicaciones disponibles a petición o programadas, incluido soporte Wake-on-LAN. La óptima solución de problemas y la eficiente distribución de software remotos se realiza mediante tecnología Multicast.

Inventarios de hardware y software, y administración de licencias: la identificación, visibilidad y control (incluido el bloqueo), junto con la administración del uso de licencias, proporciona una visión de todo el software y hardware implementado en todo el entorno, incluidos los dispositivos extraíbles. También se encuentran disponibles la administración de licencias de software y hardware, la detección de dispositivos de invitados, el control de privilegios y la autorización de acceso.

Integración SIEM: compatibilidad con sistemas IBM® QRadar y HP ArcSight SIEM.

Control de acceso basado en funciones (RBAC): se pueden asignar responsabilidades administrativas en redes complejas, con vistas de la consola personalizadas de acuerdo con las funciones y derechos asignados

CIFRADO

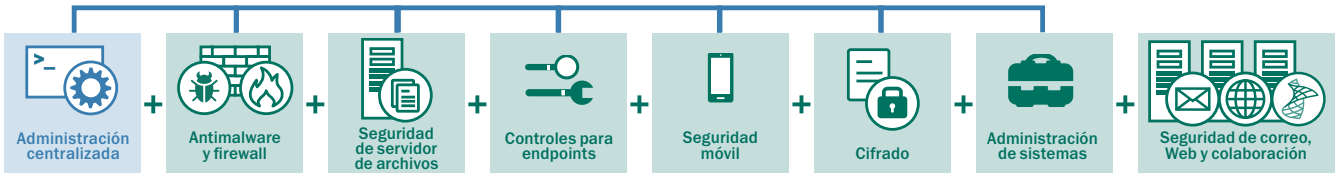
Potente protección de datos: en los terminales se puede aplicar cifrado de archivo/carpeta (FLE) y a todo el disco (FDE). La compatibilidad con el "modo portátil" asegura la administración del cifrado en todos los dispositivos que salen de los dominios administrativos.

Inicio de sesión de usuario flexible: la autenticación previa al arranque (PBA) para una mayor seguridad incluye "inicio de sesión único" opcional para transparencia del usuario. La autenticación basada en 2 factores o token también está disponible.

Creación de políticas integradas: la integración única del cifrado con la aplicación y los controles del dispositivo proporciona una capa adicional de seguridad mejorada y facilidad de administración.

Kaspersky Endpoint Security for Business – ADVANCED también incluye todos los componentes de los niveles SELECT y CORE.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Las organizaciones que requieren seguridad integral para todo su entorno de TI eligen Kaspersky Total Security for Business

Kaspersky Total Security for Business ofrece la más completa plataforma de protección y administración actual de la industria. Total Security for Business protege cada nivel de su red e incluye sólidas herramientas de configuración para garantizar que sus usuarios sean productivos y no reciban amenazas de malware, independientemente del dispositivo o de la ubicación.

SEGURIDAD PARA SERVIDORES DE CORREO ELECTRÓNICO

Previene con eficacia las amenazas de malware, los ataques de phishing y el spam de los correos electrónicos, mediante actualizaciones basadas en la nube y en tiempo real para velocidades de captura excepcionales y falsos positivos mínimos. También se incluye protección antimalware para IBM® Domino®. La funcionalidad DLP para Microsoft Exchange está disponible por separado.

SEGURIDAD PARA GATEWAYS DE INTERNET

Garantiza acceso seguro a Internet en toda la organización al eliminar automáticamente programas maliciosos y potencialmente hostiles en HTTP(S) / FTP / SMTP y tráfico POP3.

SEGURIDAD PARA LA COLABORACIÓN

Defiende los servidores y granjas de SharePoint® contra todas las formas de software malicioso. La funcionalidad DLP para Sharepoint, disponible por separado, otorga capacidades de filtro de contenido y archivos que identifican datos confidenciales y protegen contra la fuga de datos.

SEGURIDAD CON UNA DIFERENCIA

Kaspersky Lab ofrece el antimalware más potente del mercado gracias a que aprovecha la inteligencia de seguridad líder mundial, incorporada en nuestro ADN y que influye en todo lo que hacemos y en cómo lo hacemos.

- **Somos una empresa impulsada por la tecnología**, de arriba a abajo, empezando por nuestro director ejecutivo, Eugene Kaspersky.
- **Nuestro Equipo de Investigación y Análisis Global (GReAT)**, un grupo de élite de expertos en seguridad, ha sido pionero en descubrir muchas de las amenazas de malware y ataques dirigidos más peligrosos.
- **Muchas de las organizaciones de seguridad** y organismos encargados de hacer cumplir la ley más respetados en el mundo buscan activamente nuestra asistencia.
- Y puesto que Kaspersky Lab desarrolla y perfecciona sus propias tecnologías básicas internamente, nuestros productos son naturalmente más estables y más eficientes.
- **Cada año, Kaspersky Lab participa en más pruebas independientes que cualquier otro proveedor** y ocupamos el primer lugar en un porcentaje mucho más elevado de pruebas que cualquier otro proveedor.
- **Los analistas más ampliamente respetados de la industria,** incluidos Gartner, Inc, Forrester Research e International Data Corporation (IDC), nos califican como Líderes dentro de muchas categorías de TI clave.
- **Más de 130 OEM**, incluidos Microsoft, Cisco Meraki, Juniper Networks, Alcatel Lucent y más, utilizan nuestras tecnologías dentro de sus propios productos y servicios.

Esto es lo que marca la diferencia.

Para obtener más información acerca de Kaspersky Endpoint Security for Business, póngase en contacto con su distribuidor.

Kaspersky Endpoint Security for Business – SELECT también incluye todos los componentes del nivel CORE.

Kaspersky Endpoint Security for Business/15 feb/global

KASPERSKY lab