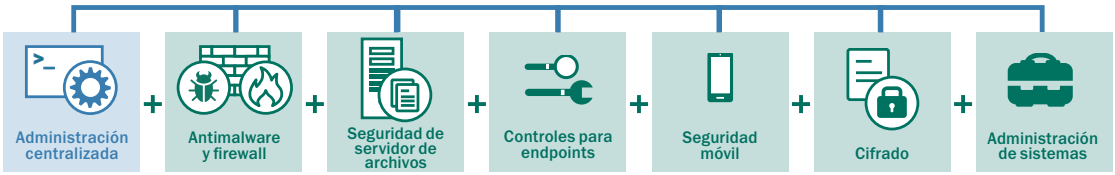
KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED



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.