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.