

ADVANCED EDITION

Las empresas están bajo amenazas cibernéticas constantes, ya que los delincuentes recurren al robo de datos, el espionaje industrial, el sabotaje y las demandas de rescate para monetizar sus ataques cibernéticos. Una fuerza laboral móvil y los empleados que trabajan desde casa aumentan el desafío de la ciberseguridad, ya que las instalaciones comerciales ya no definen el perímetro de TI. Cloud Deployed Endpoint Security de K7 es la protección integral y rentable, que no está restringida por el tiempo o el lugar, en la que puede confiar.

Consola en la nube

A diferencia de los productos de ciberseguridad convencionales que requieren un servidor local dedicado para ejecutar la consola de administración, Cloud Deployed Endpoint Security tiene su consola de administración en la nube, lo que evita el costo de hardware adicional y medidas de redundancia de hardware.

Implementación remota

La implementación en la nube permite una implementación 100% remota, donde ni los empleados ni el personal de K7 necesitan visitar las oficinas de la empresa para instalar la ciberseguridad de K7. La implementación rápida y sin complicaciones garantiza una protección rápida de toda la organización.

Control en cualquier momento y lugar

Los ciberataques no están restringidos por horas de trabajo, zonas horarias o regiones; Las ciberdefensas deben ser igualmente irrestrictas para ser efectivas. Con solo un navegador web, los administradores de TI pueden acceder a la consola en la nube de K7 en cualquier momento y desde cualquier lugar, con un control instantáneo, centralizado y completo sobre la ciberseguridad de la empresa.

Protección Enterprise contra malware

Mejorada con inteligencia artificial, la protección de K7 Security para terminales y servidores ayuda a las pequeñas, medianas y grandes empresas a proteger los datos, proteger los dispositivos, tranquilizar a los clientes y cumplir con los requisitos contractuales y reglamentarios.

Alto rendimiento, bajo impacto en recursos

Los productos de K7 están diseñados para proporcionar potentes defensas anti-malware sin sobrecargar los recursos del sistema. La baja huella de memoria y los escaneos increíblemente rápidos sobre un hardware modesto permiten a las empresas ahorrar costos al aplazar las actualizaciones de hardware sin comprometer la ciberseguridad.

Actualizaciones diarias

Constantemente surgen nuevas ciberamenazas y la ciberseguridad debe actualizarse con frecuencia para contrarrestarlas. K7 Labs analiza miles de muestras de malware todos los días y distribuye varias actualizaciones de definiciones de malware a diario para garantizar que las empresas siempre estén protegidas contra las últimas ciberamenazas.

Protección completa contra amenazas

Los productos K7 Security brindan una protección integral contra virus, malware, ransomware, troyanos, phishing, spyware, ataques de día cero, ingeniería social y muchas otras ciberamenazas. La protección contra amenazas incluye tanto la detección basada en firmas como el análisis heurístico, con una deconstrucción segura para identificar y derrotar los intentos de ofuscación.

Características clave

- Administración a través de un navegador web en cualquier momento y lugar
- Instalación remota 100%
- Sin necesidad de máquinas dedicadas en las instalaciones
- Protección de endpoints de bajo costo y alto rendimiento
- Detecte y mitigue las amenazas del mundo real, como virus, spyware, ransomware, intrusiones de piratas informáticos y ataques de phishing.
- Firewall granular con HIDS integrado para bloquear ataques dirigidos a nivel del sistema
- Protección de acceso al dispositivo contra amenazas de malware propagadas por USB
- El rendimiento optimizado y la pequeña huella de memoria extienden la vida útil de los sistemas más antiguos
- Cree y aplique una política de seguridad de punto final coherente en equipos de escritorio y servidores
- Control centralizado y aplicación granular del acceso al sitio web en función de categorías predefinidas, que incluyen juegos de apuestas, contenido relacionado con adultos, herramientas de piratería y más
- Las políticas de control de aplicaciones centralizadas bloquean aplicaciones no deseadas o dañinas
- Se pueden generar y extraer informes detallados sobre aplicaciones, dispositivos y amenazas en formatos Excel y PDF
- Enterprise Asset Management rastrea todos los activos de hardware de endpoint en la red, genera informes y envía notificaciones sobre cambios
- Proceso de migración sin esfuerzo. K7 desinstalará cualquier producto existente y se instalará automáticamente

Protección multicapa

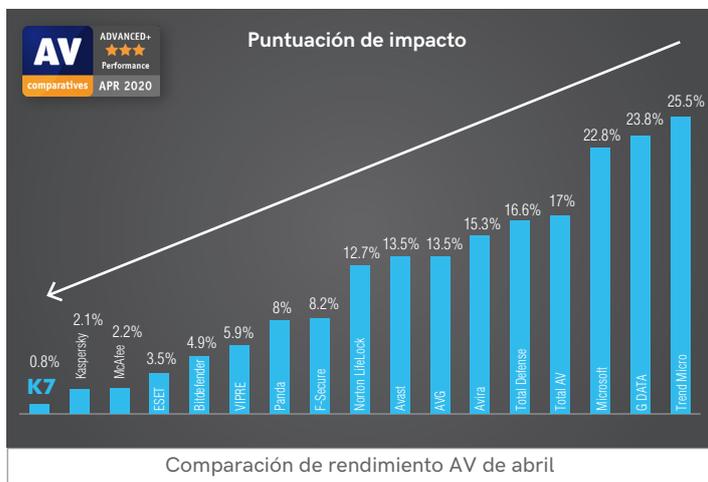
- K7 Sentry – Análisis en tiempo real /Bajo demanda – La tecnología de análisis en tiempo real y bajo demanda identifica y bloquea objetos de malware conocidos y desconocidos antes de que afecten a los sistemas
- Tecnología de detección heurística de malware – Como complemento de la detección tradicional, la detección heurística utiliza análisis de comportamiento para identificar y bloquear de manera proactiva el malware desconocido.
- Protección contra Ransomware – Monitorea el comportamiento de procesos potencialmente sospechosos, especialmente cualquier proceso que escribe en ciertos tipos de archivos de destino y bloquea los intentos de cambiarlos.
- K7 Firewall (HIDS/HIPS) – Bloquee las amenazas de forma proactiva – el firewall basado en el host con un sistema de detección de intrusiones en el host (HIDS) y un sistema de prevención de intrusiones en el host (HIPS) integrados protege contra ataques directos a nivel de aplicaciones y sistemas.
- K7 Safe Surf - Navegación segura en línea - Protege los puntos finales de infecciones de malware basadas en Internet y ataques drive-by-download mediante el uso de análisis de URL heurísticos y servicios de reputación de sitios web basados en la nube
- Control de dispositivos K7: elimine las infecciones de medios de almacenamiento y USB: bloquee el acceso a dispositivos de almacenamiento USB desconocidos y no autorizados que pueden contener malware. Establezca políticas a nivel de host para hacer cumplir las configuraciones de escaneo automático o bajo demanda, la ejecución de archivos y el acceso con contraseña
- Control de aplicaciones K7: bloquee aplicaciones no autorizadas: implemente una política centralizada para controlar las aplicaciones no deseadas instaladas en los endpoints. Los mensajeros instantáneos, los clientes de BitTorrent u otras aplicaciones que requieren un uso intensivo del ancho de banda pueden bloquearse para que no se ejecuten, accedan a la red o bloqueo completo del acceso a Internet.
- Filtrado web K7 - Bloquear contenido no autorizado - Definición de políticas centralizada y aplicación de restricciones de acceso a contenido no autorizado o inapropiado. El filtrado web cubre miles de sitios web predefinidos agrupados por categoría y bloqueados continuamente o en horarios programados.

Plataforma de soporte K7 Security

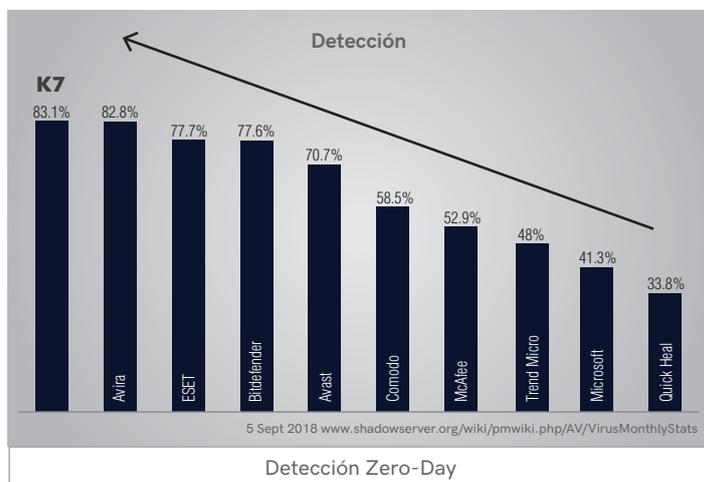
Arq. de 32 y 64 bits, excepto XP

- Microsoft Windows XP (SP2 o posterior) [32 bits], Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003 (SP1 o posterior), Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019

POCO IMPACTO



ALTA PROTECCIÓN



Comparación de características

	Standard Edition	Advanced Edition
Detecte virus, spyware y ataques de phishing	✓	✓
Detección de rootkits y ransomware	✓	✓
Navegación segura (escaneo de URL)	✓	✓
Protección de correo electrónico	✓	✓
Cortafuegos inteligente con HIDS / HIPS integrados	✓	✓
Control centralizado de aplicaciones	✗	✓
Protección de acceso a dispositivos USB / vacunación USB	✗	✓
Filtrado web (bloqueo de sitios web / filtrado por categoría)	✗	✓
Gestión centralizada	✓	✓
Varias actualizaciones diarias	✓	✓

Sobre K7 Security

K7 Security desarrolla soluciones anti-malware para terminales y servidores para empresas pequeñas, medianas y empresariales que ofrecen una amplia gama de características y capacidades para enfrentar las amenazas más ardientes de la actualidad. Disponible en las ediciones estándar y avanzada, Endpoint Security de K7 puede admitir múltiples modos de administración centralizados para simplificar la implementación, optimizar las operaciones de TI y cumplir con los requisitos de cumplimiento internos y externos.