

# K7 Endpoint Protection

## ADVANCED EDITION

Todos los días, las organizaciones enfrentan el desafío de defender sus redes contra intentos maliciosos de violar sus defensas cibernéticas. La ciberseguridad es una de las decisiones de compra de TI más importantes que toma una organización para garantizar operaciones comerciales exitosas y continuas. Los efectos de un ataque de malware dirigido pueden poner rápidamente de rodillas a una empresa, afectando negativamente la eficiencia de una organización e incurriendo en una pérdida de productividad de la fuerza laboral.

La protección de la propiedad intelectual de una empresa y la seguridad de los datos de los clientes son buenas prácticas comerciales; sin embargo, el costo de implementar, administrar y mantener la administración de TI comercial y los controles de seguridad pueden ser prohibitivos para cualquier empresa emergente. Las mejores soluciones anti-malware para endpoints y servidores implementadas dentro de la empresa deben lograr un equilibrio entre la detección proactiva de amenazas, la capacidad de administración, el rendimiento y el costo operativo.

### Anti-malware de clase empresarial

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 Standard y Advanced, Endpoint Security de K7 puede admitir múltiples modos de administración centralizada (en las instalaciones o en la nube) para simplificar la implementación, optimizar las operaciones de TI y cumplir con los requisitos de cumplimiento internos y externos.

### Seguridad de Endpoints con rendimiento optimizado

K7 lidera la industria en optimización del rendimiento y una huella de memoria significativamente pequeña, lo que ayuda a las organizaciones a reducir el impacto de la protección contra malware que consume muchos recursos en los sistemas existentes. La optimización del rendimiento y la memoria también pueden aplazar los costos futuros asociados con el reemplazo del sistema de gama baja o las actualizaciones de hardware a una fecha posterior.

### Integración con plataformas de gestión centralizadas

La plataforma de gestión centralizada de K7 Security ofrece a los administradores de TI visibilidad de toda la organización sobre las amenazas para proteger de forma proactiva los puntos finales vulnerables a malware y ataques maliciosos. La administración centralizada, administrada a través de la nube o implementada en las instalaciones, permite la instalación, configuración y generación de informes remotos de las soluciones de punto final K7 implementadas en toda la empresa.

### Las actualizaciones por hora minimizan la exposición y el riesgo

Con actualizaciones cada hora, K7 Security ayuda a las empresas a protegerse contra las últimas amenazas de malware las 24 horas del día, los 7 días de la semana, los 365 días del año. Las actualizaciones cada hora reducen la ventana de vulnerabilidad de una organización al minimizar el riesgo y el impacto comercial del malware de rápido movimiento o los brotes que rápidamente conducen al compromiso del sistema o la red.

### Protección contra amenazas múltiples

K7 Security desarrolla soluciones anti-malware proactivas y multiplataforma que detectan y detienen troyanos, virus, spyware, adware, ransomware y otras amenazas de malware que pueden comprometer la integridad de los puntos finales y, en última instancia, la red corporativa.

### Características Clave

- Protección y prevención de endpoints de alto rendimiento y bajo costo
- Detecte y mitigue las amenazas del mundo real, como virus, spyware, ransomware 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
- Rendimiento optimizado y la huella digital extienden la vida útil de los sistemas más antiguos
- Gestión centralizada y flexible en las instalaciones o basada en la nube
- Crear y hacer cumplir una política de seguridad coherente en escritorios y servidores.
- El filtrado web permite el control centralizado y la aplicación granular del acceso al sitio web en función de categorías predefinidas.
- Las políticas de control de aplicaciones centralizadas bloquean aplicaciones no deseadas o dañinas.
- Se pueden generar y extraer informes complejos sobre aplicaciones, dispositivos y amenazas para sus necesidades comerciales únicas.
- Enterprise Asset Management realiza un seguimiento de todos los activos de hardware en la red, genera informes y envía notificaciones sobre cambios.
- Compatibilidad con K7 Enterprise Security.
- Proceso de migración sin esfuerzo. Garantizando una transición sin problemas, K7 desinstalará cualquier producto existente y se instalará automáticamente.

-  **K7 Sentry - Análisis en tiempo real /bajo demanda** - La tecnología de escaneo en acceso y bajo demanda identifica y bloquea los objetos de malware conocidos y desconocidos antes de que impacten en 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 forma proactiva el malware desconocido además de los zero-day exploit.
-  **Protección contra ransomware** - La 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.
-  **Cortafuegos K7 (HIDS / HIPS): bloquea las amenazas de forma proactiva** - El firewall basado en host con un sistema integrado de detección de intrusiones en el host (HIDS) y el sistema de prevención de intrusiones en el host (HIPS) protegen contra ataques directos a nivel de aplicaciones y sistemas.
-  **K7 SafeSurf: navegación segura en línea** - Proteja los endpoints de las infecciones de malware basadas en Internet y los ataques drive-by-download mediante el análisis de URL heurístico y los servicios de reputación de sitios web basados en la nube, antes de que se puedan implementar las cargas útiles.
-  **Control de dispositivos K7: Proteja medio de almacenamiento y USB** - Bloquee el acceso a dispositivos de almacenamiento USB desconocidos y no autorizados que puedan contener una carga útil de malware. Establezca políticas a nivel de host para hacer cumplir la contraseña del dispositivo, la ejecución de archivos y las configuraciones de escaneo automático o bajo demanda.
-  **Control de aplicaciones K7: bloquear aplicaciones no autorizadas** - Implemente una política centralizada para controlar las aplicaciones no deseadas instaladas en los sistemas de punto final. Se puede bloquear la ejecución, el acceso a la red o la denegación total del acceso a Internet a los mensajeros instantáneos, los clientes Bit-torrent u otras aplicaciones de uso intensivo del ancho de banda.
-  **Filtrado web K7: bloquear contenido no autorizado** - Definición de políticas centralizadas y aplicación del acceso al sitio web de punto final 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.

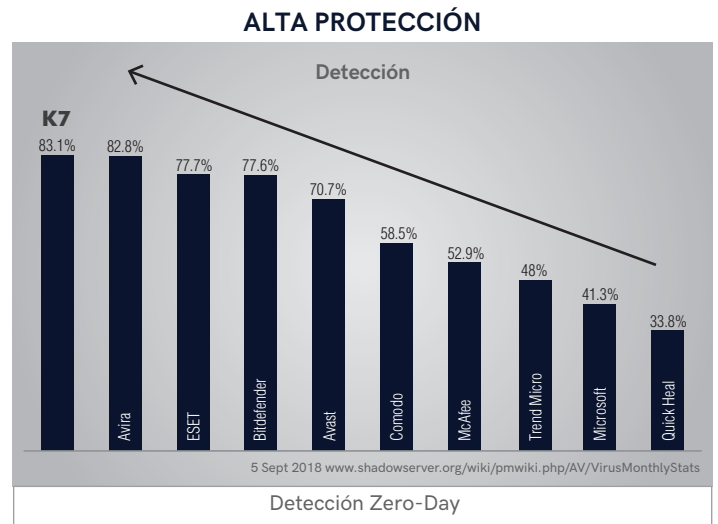
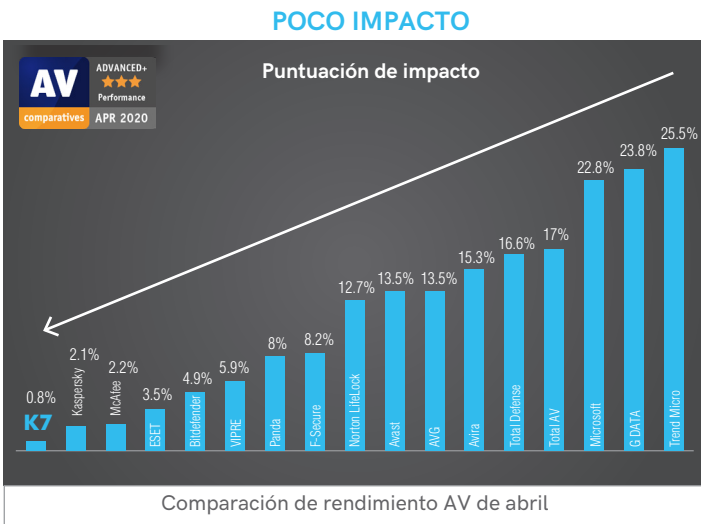
**Plataforma de soporte K7 Security:**

**Endpoint**  
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

**Server Console**  
Arq.de 32 y 64 bits

- Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2016, Windows Server 2019



**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 (On-premise / Cloud)	✓	✓
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.