Visión general

Comodo Endpoint Security Manager

Con tecnología de contención Auto-Sandbox

La tecnología de contención de amenazas de Comodo asegura previniendo que ninguno de los virus y malware infecte su computadora.

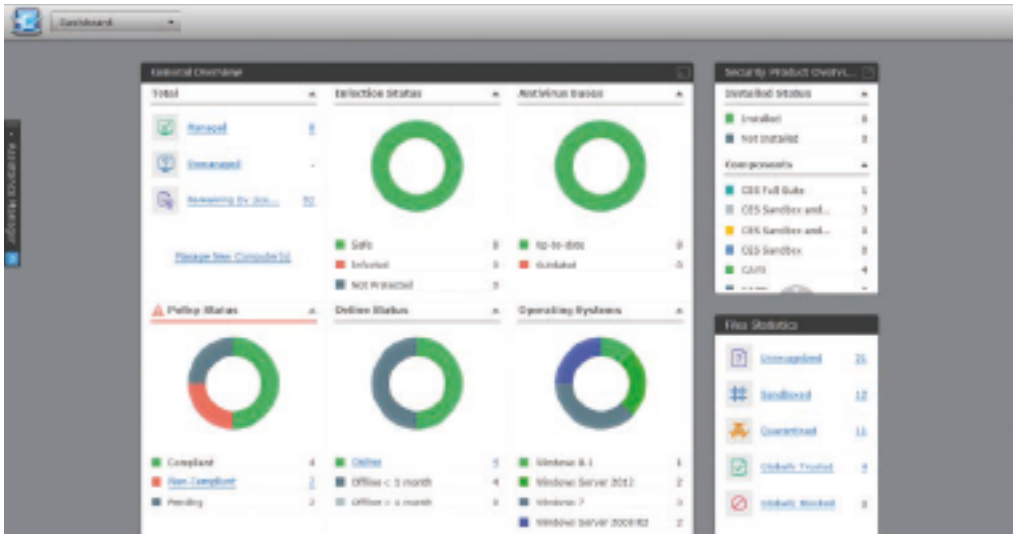
COMODO
Creating Trust Online®

Comodo Endpoint Security Manager (ESM) protege contra virus y malware enfocándose en prevención, no solo en detección. Nuestra tecnología de prevención de amenazas crea un escudo impenetrable que identifica archivos seguros, inseguros y cuestionables (reconocidos como archivos buenos, malos y desconocidos).

Comodo Endpoint Security Manager proporciona una gestión centralizada de las 7 capas de seguridad de Comodo que protege de forma proactiva los usuarios finales y sus aplicaciones contra Malware y amenazas avanzadas

Siguiente Generación, protección de 7 capas para usuarios finales.

Contención - Las soluciones tradicionales de seguridad para usuarios finales dependen de una detección por medio de una lista negra y una lista blanca.
La tecnología de contención de Comodo rompe con este enfoque tradicional añadiendo una capa preventiva que aísla automáticamente **(auto-sandbox)** los archivos que tienen que ser aún reportados. Estos archivos desconocidos pero que son amenazas potenciales están contenidos en un ambiente virtual dentro del sistema con muy poco uso de recursos hasta que su comportamiento sea analizado.



Filtrado de WEB URL - Con la potente interfaz de configuración de reglas, puede crear reglas generales o independientes como lo requieras, incluso por cada usuario.

Comodo Firewall - Un paquete de Firewall altamente configurable que constantemente defiende tu sistema de ataques que entran o salen de internet.

Comodo Antivirus - Un motor de Antivirus proactivo que automáticamente detecta y elimina virus, gusanos y otro malware. Los usuarios pueden arrastrar y soltar elementos automáticamente en la pantalla principal para ejecutar un análisis de virus instantáneo.

File Lookup Services - Una búsqueda de archivos basada en el servicio de la nube (FLS, File Lookup Service) comprueba la reputación de los archivos en su computadora cotejándola con las listas maestras blanca y negra de Comodo.

Host Intrusion Protection System (HIPS) - Como parte del enfoque de defensa multi-capa de Comodo, (HIPS) es un sistema de prevención de intrusiones basado en reglas que supervisan las actividades de todas las aplicaciones y procesos en nuestra computadora. (HIPS) bloquea las actividades de los programas maliciosos y detiene cualquier acción que pueda causar daños a su sistema operativo o memoria del sistema registrando claves de acceso o datos personales.

Viruscope (Análisis por Comportamiento) - Viruscope monitorea el comportamiento de los procesos que se ejecutan en la computadora y le avisa si se toman acciones que podrían poner en peligro su privacidad y / o seguridad. Tiene la habilidad de revertir acciones potencialmente indeseables de software sin necesidad de bloquearlo totalmente, dándole un control más preciso del software de otro modo legítimo.

CARACTERÍSTICAS PRINCIPALES

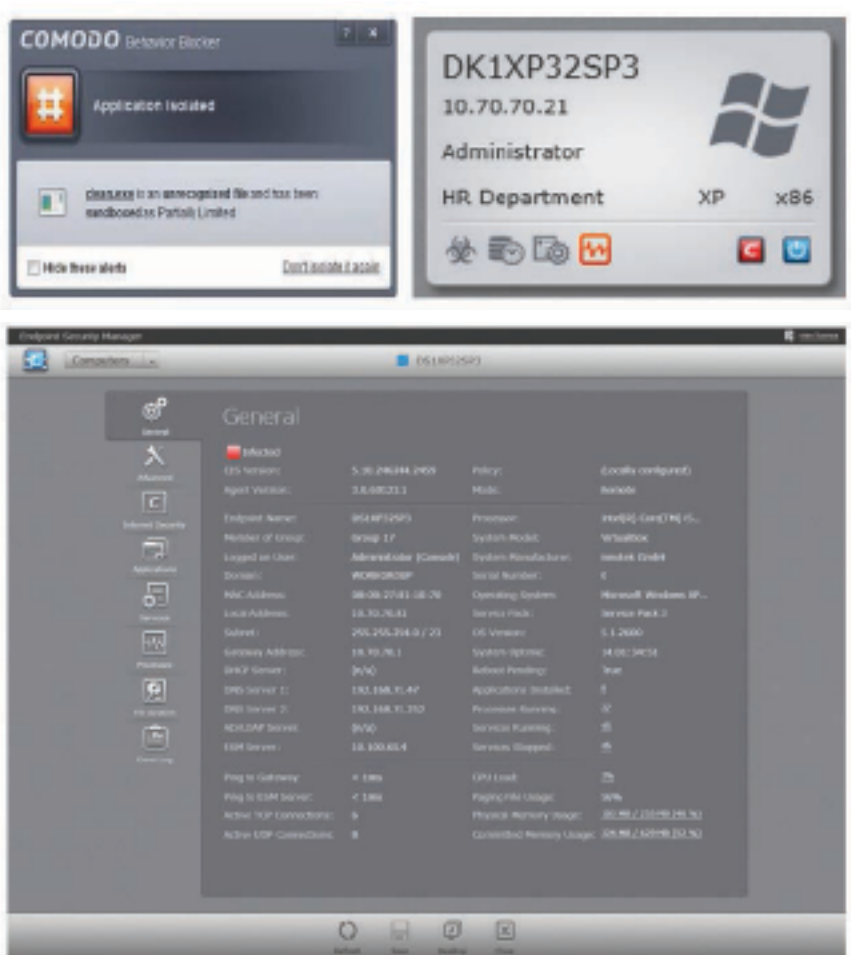
- Capa de seguridad preventiva única, con la contención de **Comodo** que de inmediato aísla automáticamente (auto sandbox) amenazas de día cero y amenazas persistentes avanzadas **(APTs)** en un ambiente virtual dentro del sistema existente y requieren los mínimos recursos del sistema.
- La tecnología de contención puede ser desplegada de forma independiente junto con otras soluciones existentes de anti-virus para incrementar la seguridad del usuario final contra archivos desconocidos hasta haber realizado una prueba de conducta.
- Permite la gestión centralizada de servidores, estaciones de trabajo y computadoras portátiles de usuario final, generando un detallado informe de la configuración e información del usuario final.
- La integración de las 7 capas de seguridad para usuario final ofrece: **Filtrado de WEB URL, Comodo Firewall, Comodo Antivirus, File Lookup Services, Host Intrusion Protection System (HIPS), Contención con Auto-Sandbox y Viruscope (Análisis de Comportamiento).**
- La consola proporciona una visión panorámica para controlar todos los aspectos de protección y gestión de usuarios finales.
- Administra los procesos de usuario final, servicios, aplicaciones instaladas, uso de recursos, dispositivos extraíbles y el uso de energía.
- La implementación jerárquica de los servidores CESM permite la gestión local o remota de usuarios finales que no estén en la red local.
- Reportes administrativos para tener un mayor detalle en actualizaciones, escaneos y base de datos de antivirus.
- Inmediata funcionalidad y compatibilidad para Windows 10.
- Garantía única en la industria *libre de virus contra infección de $5,000 USD.

Comodo EndPoint Security (CES) ofrece protección en tiempo real contra todo tipo de amenazas de malware. Otros productos de antivirus dependen solamente de una actualización de firmas, pero la tecnología de contención y aislamiento automático de Comodo lo protege de las amenazas desconocidas. Por lo tanto permite a Comodo ser el único proveedor que ofrece una *garantía libre de virus por $5000 USD por costos de reparación, si un Endpoint en su empresa es infectado por un virus o malware y no logramos restaurar sus condiciones de trabajo nosotros mismos.

El futuro en la administración de Endpoints

Comodo ESM no solo proporciona una protección inigualable en contra de amenazas inmediatas, también proporciona al administrador total visibilidad y control sobre el software, hardware y servicios en todas las maquinas. Comodo ESM está totalmente integrado con Comodo Endpoint Security que proporciona administración centralizada de estado del antivirus y el estado del sistema.

La consola centralizada de Comodo ESM permite al administrador ver cada métrica importante inmediatamente. La utilización única despliegue panorámico (patente pendiente). Una consola de administración basada en la web (nube) que presenta a cada Endpoint en una ventana que contiene 14 puntos críticos que facilitan una alerta inmediata y solución de problemas que requieren del mínimo esfuerzo del administrador.



- Estado de la infección
- Estado de la definición de base de datos
- Cumplimiento de políticas de seguridad
- Estado del sistema
- Solicitudes de asistencia del usuario
- Estado de la suite de seguridad
- Estado en línea

La pantalla de propiedades del equipo ofrece información precisa sobre cada usuario final, incluyendo versión del sistema operativo, service packs, aplicaciones instaladas, si se requiere un reinicio, estadísticas de las redes y CPU, métricas de uso de RAM y disco duro. Con un solo clic el administrador es capaz de ver y detener servicios y procesos así como examinar y desinstalar aplicaciones basadas en MSI (Instalador de Microsoft).

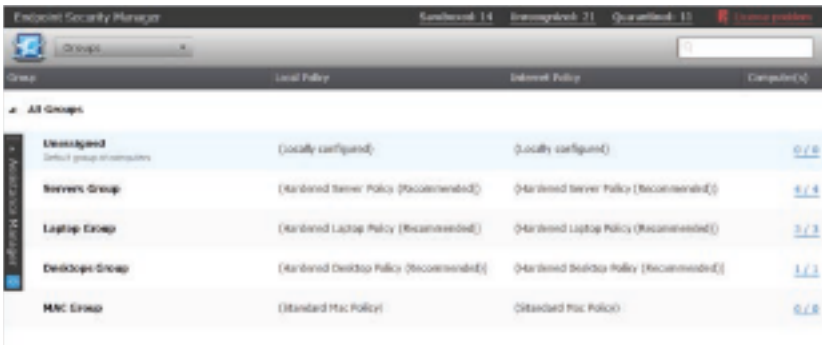
Armado con esta información el administrador puede tomar decisiones rápidas y precisas para proteger la infraestructura y asegura una suave y eficiente continuidad para los usuarios de los requerimientos computacionales.

La administración proactiva está disponible a través de la configuración de políticas o plantillas que dictan el comportamiento del Endpoint. Controlando todo desde el programa de actualización de la base de datos de definiciones, programación de actualizaciones y su fuente, manipulación granular de las configuraciones de seguridad críticas, hasta las listas blancas de archivos y fabricantes de dispositivos removibles, control y administración de la energía, y creación de políticas mediante wizards que generan y refuerzan las configuraciones de los administradores en minutos.

Una gestión más eficiente, eficaz y sencilla

Los perfiles y configuraciones intuitivas ahorran a los administradores miles de horas hombre al año. Para facilitar el proceso de incorporación, los administradores pueden configurar los perfiles predeterminados para todos o por grupos para desplegar y gestionar de forma centralizada las políticas de seguridad.

El tiempo del administrador que se perdería en la configuración repetitiva y problemas de interoperabilidad con el proveedor pueden ser re direccionados hacia una mayor productividad y rentabilidad de los intereses empresariales básicos. Además que las políticas del CESM se pueden implementar inmediatamente a través de todos los nodos protegidos, los administradores pueden responder más rápidamente a proteger a toda una red en contra de las últimas amenazas del día a día, la interface intuitiva del CESM proporciona acceso al alcance de su mano para tareas intuitivas importantes de la red y datos así como recursos de apoyo.



Una solución total para ambos, PyMEs y Grandes Empresas.

- **Más control, menos preocupaciones:** La tecnología única de contención de Comodo que aíslan automáticamente (auto sandbox) el malware desconocido en un ambiente virtual dentro del sistema y requieren los mínimos recursos del sistema.
- **Administre con Facilidad:** Administre Centralmente sus servidores, estaciones de trabajo, laptops, netbooks y sus aplicaciones.
- **Participar en las mejores prácticas:** Nuestra plataforma de seguridad de 7 capas asegura que cada usuario final este protegido con una combinación de filtrado de web URL, firewall, antivirus, file lookup, HIP's, contención con auto-sandbox y viruscope (análisis de comportamiento).
- **Aumente los Detalles:** Una robusta consola administrativa que presenta una vista panorámica de 14 métricas críticas para usuario final.
- **Ahorre tiempo**: Vea y modifique los procesos de los Endpoints, servicios y aplicaciones instaladas con poderosas capacidades de administración de sistema.
- **Administración simplificada:** Use “push” para desplegar a través de Active Directory®, grupos de trabajo y direcciones IP y “pull” para desplegar a través de una directiva de grupo o un script de inicio de sesión.
- **Interactuar de forma remota:** Interactúe remotamente con usuarios y Endpoints remotos con nuestro módulo de asistencia remota.
- **Disminuya sus tiempos de respuesta:** Notificaciones en tiempo real que reducen los tiempos de respuesta en emergencias de amenazas emergentes.
- **Profundizar el entendimiento:** Las políticas de conocimiento de ubicación permiten una definición granular de configuraciones de seguridad para usuarios finales dentro y fuera de la VPN.
- **Piense en verde:** Dispositivos habilitados con Wake-on-LAN avanzados que permiten una administración integral de energía.
- **Mantenga bajos requisitos de sistema:** Requisitos mínimos del sistema permiten la instalación en computadoras no dedicadas y servidores Windows.

Acerca de Comodo.

La organización Comodo es un innovador mundial y desarrollador de soluciones en seguridad cibernética, fundada en la creencia de que cada transacción merece y requiere una capa única de seguridad y confianza. Basándose en su profunda historia de los certificados SSL y liderazgo en antivirus y seguridad Endpoint y la verdadera tecnología de contención, las personas y las empresas confían en las soluciones probadas de Comodo para autenticar, validar y asegurar su información más crítica. Con la protección de datos cubriendo a los Endpoint, la seguridad de la red y móvil, además de la identidad y gestión de acceso, las tecnologías patentadas de Comodo ayudan a resolver los retos de malware, ciber ataques y los desafíos de hoy. Asegurando las transacciones en línea de miles de negocios y con más de 85 millones de instalaciones de software de seguridad de escritorio, Comodo está creando confianza en línea. Con su sede central en Clifton New Jersey, la organización Comodo tiene oficinas en China, India, Filipinas, Rumania, Turquía, Ucrania y el Reino Unido, para más información visite: www.enterprise.comodo.com

* El plan de protección de Comodo se incluye con Comodo Endpoint Security y está disponible por uno (1) año a partir de la fecha de registro e instalación del software siempre y cuando usted haya pagado la póliza de certificación y seguro. Por favor consulte Comodo Endpoint Security Manager Acuerdo de suscriptor de usuario final (http://www.comodo.com/repository/eula/EULA-CESM-v2013.pdf) para detalles completos. Las pruebas de Comodo Endpoint Security están excluidas del Comodo Protection Plan.

**Solo sistema.