COMODO CYBERSECURITY

Protección avanzada de Endpoints
Ficha de datos

Impenetrabilidad sin sacrificar la usabilidad

Veredictos al 100% el 100% del tiempo

Comodo Advanced Endpoint Protection (AEP) entrega una contención automática, en proceso de patentado, donde programas y ejecutables desconocidos, así como otros archivos que soliciten privilegios en tiempo de ejecución, son ejecutados de manera automática en un contenedor virtual que no tiene acceso a los recursos de sistema del ordenador anfitrión o a los datos de los usuarios. Estos son ejecutados de la misma forma que lo harían en el sistema anfitrión, por lo que para el usuario es transparente, pero no pueden dañar o infectar el sistema nativo.

Mientras son ejecutados en contención automática, los archivos desconocidos son cargados a la nube global de amenazas para un análisis en tiempo real, la cual entrega un veredicto en un tiempo máximo de 45 segundos para un 95% de los archivos enviados. El 5% restante de los casos son enviados a los investigadores para un análisis realizado por humanos quienes realizan el análisis y entregan los resultados dentro de los tiempos determinados por los acuerdos de niveles de servicio (SLA - Service Level Agreement). En resumen, Comodo AEP entrega el veredicto del 100% el 100% del tiempo. Y debido a que la nube global de amenazas está siendo alimentada por la comunidad, el conocimiento ganado sobre un archivo desconocido beneficia a toda la comunidad de usuarios de Comodo AEP. Usted se beneficia del efecto de estar en red con 85 millones de usuarios.

El cliente de Comodo es extremadamente ligero, no tiene dependencias de CPU y es completamente agnóstico de las aplicaciones.

Elimine el miedo a los desconocido

Los archivos buenos, pueden ser ejecutados de manera segura. Los archivos malos, pueden ser bloqueados. Pero, ¿cómo puede lidiar con los archivos desconocidos? Si los ejecuta y son malos, pueden poner su computadora en riesgo. Si los bloquea y son legítimos, eso provocaría que los usuarios no puedan hacer su trabajo.

"Comodo AEP ofrece el grupo más amplio de herramientas para identificar a los archivos buenos de los malos. Para todos los desconocidos, nuestra tecnología en proceso de patentado de contención automática y nuestro motor de decisión de veredictos entrega el veredicto - bueno o malo - cada vez, sin impacto alguno en la experiencia de usuario"

Características principales

Revisión antivirus: Verifica los puntos de salida contra una enorme lista de archivos conocidos buenos y malos compilados por años que constituyen la autoridad certificadoras más grande del mundo y recopilados de los 85 millones de puntos instalados alrededor del mundo.

Contención automática: Los ejecutables desconocidos y otros archivos que soliciten privilegios de ejecución, son ejecutados automáticamente en los contenedores virtuales patentados de Comodo, los cuáles no tienen acceso a los recursos de sistema del computador anfitrión, lo que, desde la perspectiva del usuario, es transparente; pero estos no pueden dañar o infectar el sistema.

Análisis de comportamiento VirusScope: Utiliza técnicas como la alteración de APIs (API Hooking), prevención de inyección de DLL y muchas más para identificar indicadores de peligro mientras se mantienen los endpoints a salvo sin afectar su usabilidad.

Motor de decisiones y veredictos Valkyrie: Mientras se ejecuta un archivo en contención automática, los archivos desconocidos son enviados a la nube global de amenazas para un análisis en tiempo real, regresando un veredicto en un tiempo máximo de 45 segundos para el 95% de los archivos enviados.

Análisis humano: En el 5% de los casos donde VirusScope y Valkyrie no puedan emitir un veredicto, el archivo puede ser enviado a los investigadores para un análisis humano, quienes emiten un resultado dentro de los tiempos del nivel de acuerdo de servicio.

Prevención de intrusión al servidor: El sistema de prevención de intrusión al servidor (HIPS), está basado en reglas que monitorean las actividades de la aplicación y de los procesos del sistema, bloqueando aquellos que son maliciosos mediante el bloqueo de acciones que podrían dañar los componentes críticos del sistema.

Cortafuegos personal de filtrado de paquetes: Permite una administración granular de las actividades entrantes y salientes de la red, oculta puertos de sistema contra escaneos y genera alertas cuando se detectan actividades sospechosas. Puede ser administrado de manera remota o por un administrador local.

Protección avanzada de Endpoints
Ficha de datos

Caracteristicas

- Contenerización automatizada
- Lista blanca basada en certificados
- Cortafuegos Comodo para el servidor
- Reputación de archivos
- Analizador de comportamiento VirusScope
- Antivírus Comodo (lista negra)
- IPS para el servidor
- Filtrado de URL
- Analizador dinámico y estático Valkyrie
- Protección contra secuestro de sistema
- Análisis humano integrado
- Protección contra malware sin archivos
- Análisis de línea de comando
- Detección de código incrustado.

Administración de dispositivos

- Perfil por defecto
- Funcionalidad de “encuentra-mi-dispositivo”
- Inscripción de dispositivos remotamente
- Políticas relacionadas con VPN
- Aislamiento de datos
- Borrado de datos remoto
- Impone políticas sólidas para dispositivos móviles
- Control de dispositivos externos
- Certificados móviles
- Funcionalidad antirrobo “Sneak Peek”
- Administración basada en políticas

Seguridad de aplicaciones

- Inventario de aplicaciones
- Cobertura integrada de dispositivos, aplicaciones y seguridad
- Lista negra de aplicaciones
- Aplicaciones Móviles Comodo
- Almacenamiento de lista blanca de aplicaciones
- Trae tu propio dispositivo (BYOD)

Sistemas Operativos Suportados

- Windows 10 (versiones 32-bit y 64-bit)
- Windows 8 (versoiones 32-bit y 64-bit)
- Windows 7 (versiones 32-bit y 64-bit)
- Windows Vista (versiones 32-bit y 64-bit)
- Windows XP (versiones 32-bit e 64-bit)
- Android: 4.x, 4.x (KNOX), 5.x, 5.x (KNOX), 6.x (KNOX), 7.x, 7.x (KNOX)
- iOS: 7.x, 8.x, 9.x, 10.x, 11.x

macOS: 10.11.x, 10.12.x, 10.13.x

- Windows server: Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016
- Linux: Ubuntu 16.04.2 LTS x64, Debian 8.8 x64, Red Hat Enterprise Linux Server 7 x64

Requerimientos mínimos de sistema

Windows 10, 8, 7, Vista

Memoria RAM disponible 384 MB

Disco duro disponible 210MB tanto para versiones de 32-bit y 64-bit

CPU con soporte de SSE2

Internet Explorer versión 5.1 o superior

Windows XP

Memoria RAM disponible 256MB

Disco duro disponible 210MB tanto para versiones de 32-bit y 64-bit

CPU con soporte de SSE2Internet Explorer

Internet Explorer versión 5.1 o superior

Administración y monitoreo remoto

- Acceso remoto con control total de dispositivos
- Administración remota
- Administración de parches