PROTECCIÓN DE PUNTO FINAL SIN COMPROMISO

El panorama de la amenaza cibernética ha evolucionado y también lo ha hecho la protección del punto final. Diferentes soluciones utilizan diferentes enfoques y antes de tomar una decisión para su organización, debe comprender las opciones y las ventajas y desventajas.

Contención

La contención es similar al concepto de sandboxing, pero aborda el problema de usabilidad al hacerlo virtualmente invisible desde la perspectiva del usuario final. Con este enfoque, un contenedor agonístico de procesador y sistema operativo se ejecuta justo en el punto final para analizar el archivo sin permitir el acceso al sistema subyacente. Si se determina que el archivo es malicioso, está bloqueado. Si el veredicto es que es seguro, la próxima vez que se ejecute el archivo, se ejecutará fuera del contenedor.

Sandboxing

El espacio aislado surgió como una forma de evaluar los archivos como "malos" o "buenos" antes de que ingresen a la red aislándolos en un estrictamente controlado entorno virtual en un servidor, y solo aquellos que pasan son luego liberados al punto final. Esto proporciona una forma segura de probar programas no verificados que podría contener código malicioso. En algunos casos, el sandboxing pone en cuarentena el archivo y solo lo libera al usuario cuando se considera seguro. Esto ofrece un alto nivel de seguridad, pero puede tener un impacto significativo en la experiencia del usuario y la productividad del negocio. En otros casos, mientras se analiza el archivo en la zona de pruebas, el archivo original permanece en el punto final. Esto aborda los problemas de usabilidad y productividad, pero el usuario ahora es vulnerable a un código malicioso.

"Las herramientas de detección basadas en la firma y el comportamiento utilizan un enfoque de "permitir por defecto" para la seguridad del punto final. Ellas dejan entrar todo y luego determinan si se está ejecutando algún código malicioso. Por el contrario, el espacio aislado y la contención toma una postura de "denegación predeterminada", impidiendo que se ejecute nada hasta que se considere seguro. Si bien esto ofrece una seguridad mucho más estricta ¿Qué sucede entre el momento en que el archivo ingresa al sistema y cuando se realiza un archivo seguro se borra y pasa de nuevo al usuario final? La seguridad es crítica, pero no puede hacerse a expensas de la productividad de los negocios. Comodo Advanced Endpoint Protection (AEP) resuelve este problema"

Detección basada en la firma

En los primeros días, las compañías antivirus documentaban las "firmas" de malware conocido. Cualquier archivo que coincida con las firmas se marcará como malicioso. El problema con este enfoque es que solo funciona para malware conocido. Pero todo el malware comienza como un software desconocido, por lo que cuando se desencadena una nueva pieza de código malicioso, las empresas son vulnerables hasta que se descubre la amenaza y se captura su firma (conocida como "día cero"). Es el equivalente cibernético de cerrar la puerta del establo solo después de que el caballo se ha ido. Cuando los atacantes comenzaron a usar técnicas para encriptar o mutar el código, el enfoque simplista de la detección basada en firmas, aunque valioso, simplemente no podía mantenerse al día.

Detección basada en el comportamiento

Una nueva ola de soluciones buscó resolver el problema al enfocarse no en las firmas de archivos maliciosos sino en el comportamiento del tráfico de la red. Los sistemas basados en el comportamiento entienden qué aspecto tiene "normal" y luego identifican un comportamiento anormal que podría representar un ataque. Este enfoque ayuda a resolver el problema del día cero al alertar a la TI sobre posibles ataques en cuestión de segundos, pero viene con sus propios desafíos. Puede haber un alto número de falsos positivos, por lo que la administración del sistema consume tiempo.

Y las herramientas basadas en el comportamiento pueden agregar tráfico significativo en la red, por lo que las organizaciones deben asegurarse de que sus sistemas puedan soportar las demandas adicionales de ancho de banda. Si bien este enfoque está mucho mejor equipado que las firmas para mantener el ritmo del malware sofisticado de hoy en día, el hecho es que no importa cuán rápido identifique el comportamiento malicioso en la red, solo puede identificarlo una vez que ya está dentro.

Características claves

Agente liviano

Con tan solo 10 MB, el cliente Comodo proporciona la más robusta protección en el mercado sin sacrificar usabilidad o tamaño

Filtrado de sitios webs

Establezca reglas específicas, que pueden ser específicas del usuario y dependientes del tiempo para bloquear el acceso a sitios web específicos

Prevención de intrusión de host

IPS basado en reglas que supervisan las actividades de las aplicaciones y los procesos del sistema, bloqueando comportamientos maliciosos al detener acciones que podrían dañar los componentes críticos del sistema.".

Firewall filtrador de paquetes personales

Se puede administrar localmente o de forma remota y proporciona administración granular de entrada y la actividad de la red saliente, oculta los puertos del sistema de los escaneos y proporciona advertencias cuando se detectan actividades sospechosas.

Servicio de búsqueda de archivos

Proporciona un sistema de clasificación de archivos basado en la nube para determinar rápidamente el estado de un archivo si aparece en la lista de archivos, la lista de proveedores de software de confianza o la propia lista de seguridad de Comodo. Estos archivos de confianza se excluyen de la supervisión adicional, lo que reduce el consumo de recursos del sistema

Interoperabilidad

Una sólida estrategia de seguridad de defensa en profundidad requiere que las empresas implementen un conjunto de herramientas de seguridad diverso utilizando tecnologías de una variedad de proveedores. En un entorno heterogéneo por diseño, la interoperabilidad es crucial. La tecnología de contención AEP de Comodo no tiene incompatibilidades conocidas con software de productividad o seguridad.

Monitoreo y gestión remota

Acceso remoto con adquisición total del dispositivo

Gestión remota

Gestión de parches

Soporte 24 x 7 x 365

COMO FUNCIONA

Desde una perspectiva de seguridad cibernética, hay tres tipos de archivos: aquellos que se sabe que son buenos, aquellos que se sabe que son maliciosos y lo desconocido. Cuando sabes que un archivo es bueno, puedes dejarlo funcionar. Cuando sabes que un archivo es malo, puedes bloquearlo. Son los archivos desconocidos los que crean el desafío, y todo malware comienza como un código descono-cido. Comodo AEP utiliza la contención automática para aislar automáticamente los archivos desconocidos mientras que el motor de decisión del veredicto hace una buena / mala determinación.

AUTO-CONTENCIÓN

Comodo aprovecha la lista blanca de firmas más grande del mundo de archivos buenos conocidos para identificar procesos que son seguros para ejecutar en un punto final. [1]

Los ejecutables desconocidos y otros archivos que solicitan privilegios de tiempo de ejecución se ejecutan automáticamente en un contenedor virtual que no tiene acceso al los recursos del sistema host o los datos del usuario. Funcionan tan bien como lo harían en el sistema host, lo que lo hace transparente desde la perspectiva del usuario final, pero no pueden dañar ni infectar el sistema. Todos los procesos de contención leen y escriben en un registro virtual, sistema de archivos, núcleo del sistema operativo y hardware. Esto permite que los archivos seguros se ejecuten según sea necesario, a la vez que evita que los archivos maliciosos accedan al sistema para entregar sus archivos. cargas útiles.

Mientras que el archivo está en contención, el sistema registra un análisis forense completo, que puede configurarse para su entrega a SIEM y SOC. Cualquier proceso desconocido que tenga un "buen" veredicto se puede ejecutar automáticamente en el host en sesiones posteriores.

[1] Los archivos solo se pueden agregar a esta lista después de someterse a pruebas intensas por Comodo Threat Intelligence Lab. Los buenos procesos conocidos aún están sujetos a un estricto control de comportamiento y virus durante el tiempo de ejecución, pero se les permite ejecutarlos en la máquina local porque han sido completamente autenticados y no presentan ninguna amenaza.

Cómo se compara Comodo AEP con otros enfoques de contención

El enfoque de un proveedor utiliza contención selectiva, que aísla solo ciertas aplicaciones específicas, como navegadores, lectores de PDF y aplicaciones de oficina. El inconveniente es que no proporciona mecanismos para detectar y contener procesos maliciosos de otras fuentes.
Los administradores deben bloquear las aplicaciones y los servicios que los usuarios pueden ejecutar, y la configuración requiere un ajuste constante. A diferencia de Comodo AEP que ofrece una manera completamente práctica de contener archivos de todas las fuentes.

Otro proveedor crea múltiples "micro VM" para contener cada proceso generado por el usuario, generando instancias virtuales separadas del sistema operativo invitado para cada proceso contenido, todo controlado por un hipervisor que se ejecuta en el sistema operativo host. Esto aumenta la demanda en los recursos del punto final y puede llevar a la ralentización del sistema y las interrupciones del flujo de trabajo. Por el contrario, los contenedores de Comodo AEP tienen un impacto cero en la experiencia del usuario.

Control avanzado para equipos de seguridad

La autocontención de Comodo utiliza el aislamiento del proceso del espacio de usuario en tiempo de ejecución y no depende de la tecnología de virtualización de CPU para operar, pero puede implementarse para aprovechar la virtualización de CPU para mayor seguridad si así lo desea. La autocontención de Comodo utiliza tecnologías de virtualización a nivel de software y hardware y es compatible con todo el software de escritorio remoto.

La autocontención de Comodo no está limitada a aplicaciones específicas, lo que le da la flexibilidad para admitir completamente todos los casos de uso que su organización requiera. Los administradores pueden, sin embargo, especificar la contención automática solo para aplicaciones específicas o elegir contener automáticamente todos los archivos. De cualquier manera, no hay impacto en el rendimiento.

Análisis en tiempo real

100% de veredicto 100% del tiempo

Cada archivo recibe un veredicto, bueno o malo, cada vez.

Análisis humano

En el 5% de los casos en que VirusScope y Valkyrie no pueden emitir un veredicto, el archivo se puede enviar a los investigadores para su análisis humano que hacen una determinación dentro de los plazos del SLA.

Análisis del comportamiento

Comodo usa análisis de comportamiento en archivos que se ejecutan en contención. Comodo VirusScope utiliza técnicas como enganche de API, prevención de inyección de DLL y más para identificar indicadores de compromiso mientras se mantiene el punto final seguro y sin afectar la usabilidad.

Escaneo de antivirus

El sofisticado motor antivirus de Comodo escanea activamente los puntos finales contra una lista masiva de archivos conocidos como buenos y malos compilados desde años como la autoridad de certificación más grande del mundo y de los 85 millones de puntos finales desplegados en todo el mundo. Esto atrapa y elimina rápidamente el software malicioso conocido que se detecta fácilmente.

Motor de decisión del veredicto

Mientras se ejecuta en autocontención, los archivos desconocidos se cargan en Comodo Valkyrie en la nube para su análisis en tiempo real. Esta nube de amenazas globales, que analiza 73 mil millones de consultas de archivos y 300 millones de archivos desconocidos únicos al año, arroja un veredicto en 45 segundos para el 95% de los archivos enviados. Debido a que la nube global de amenazas se basa en crowdsourcing, el conocimiento adquirido sobre un archivo desconocido beneficia a todos los usuarios de Acode de Comodo. Se beneficia del efecto de red de 85 millones de usuarios.

Frustra a los hackers, no a tus usuarios

Cuando un depósito de datos de WikiLeaks 2017 expuso la CIA evaluaciones de 20 productos de seguridad, tenemos que ver el resultados sin brillo de los intentos de la comunidad de inteligencia para frustrar las tecnolo-gías en las que las empresas confían todos los días para protegerse a si mismos Si bien muchos de los nombres más importantes en el mercado demostraron ser fácil o moderadamente pirateables, había una solución que parecía frustrar sus mejores intentos. Aquí está lo que la CIA, una de las mejor financiadas y más expertas organizaciones de hacking en el mundo-tenían que decir sobre Comodo:

"Una verdadera molestia. Encuentra todo, incluso lo que no le pediste "

Esas son buenas noticias para ti. Y al implementar Comodo AEP, estás solo frustrando a los malos ; tus empleados trabajadores no notarán la diferencia.

Fuente: Cutherbertson, Anthony. "Cómo clasifican los hackers de la CIA el Antivirus de tu computador "Newsweek. 19 de marzo de 2017

Controles de dispositivo avanzados

- Perfil por defecto
- Inscripción en el dispositivo por aire
- Limpieza remota de datos
- Certificados móviles
- Funciones "Buscar mi dispositivo"
- Aislamiento de datos
- Fuerte aplicación de políticas móviles
- Imágenes "Sneak Peek" para recuperar dispositivos perdidos
- Políticas basadas en la gestión
- Políticas de VPN-aware
- Control de dispositivo externo