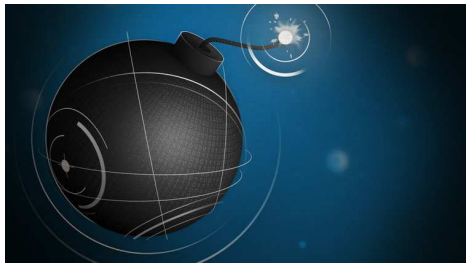
APPGUARD

Intelligent Prevention for the Endpoint



Software-based Endpoint Compromise Prevention

AppGuard protege eficazmente los ordenadores contra los tipos de amenazas de códigos maliciosos que quitan el sueño a los CISO porque sus productos antivirus tradicionales no lo hacen y las alternativas avanzadas tienen puntos ciegos y/o costos operativos inaceptables. Los expertos y analistas de seguridad recomiendan que las empresas complementen su plataforma de protección de endpoints con agentes de protección avanzados como AppGuard.

¿AppGuard reemplaza su AV?

Sí, pero AppGuard no es un producto de escaneo. Funciona de una manera completamente diferente. Muchos de nuestros clientes han reemplazado su AV tradicional con el Windows Defender gratuito de Microsoft para cumplir con los mandatos regulatorios que explícitamente requieren un escaneo periódico de los endpoints. Esta combinación protege los endpoint de las amenazas avanzadas y cumple con los mandatos reglamentarios. Otros clientes han conservado su AV tradicional. AppGuard generalmente coexiste con todas las herramientas de seguridad de endpoint.

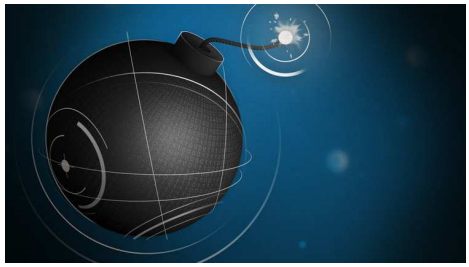
¿Qué es AppGuard y qué lo hace diferente?

AppGuard derrota todas las formas de malware para el consumidor, malware avanzado, exploit -less (por ejemplo, PowerShell u otros scripts que usan utilidades legítimas para causar daño) y ataques fileless (residen solo en la memoria) en los endpoints. Lo hace evitando el embudo de distinguir lo bueno de lo malo o lo normal de los comportamientos anormales entre infinitas y efímeras posibilidades. Es por eso que las alternativas fallan e incurren en altos costos operativos. En cambio, el enfoque patentado de AppGuard combina de manera única controles de bajo nivel que bloquean dinámicamente acciones inaceptables pero deterministas. Los atacantes pueden cambiar fácilmente la apariencia y el comportamiento de los códigos maliciosos, pero es extremadamente raro cambiar lo que finalmente hace sin sacrificar sus objetivos. Los atacantes del endpoint no pueden lograr sus objetivos sin ejecutar con éxito estas acciones finitas.

Los controles patentados únicos de AppGuard no permiten que las aplicaciones y lo que generen implanten malware persistente alterando el espacio del sistema (por ejemplo, Windows, directorios de Archivos de programa, nodos de registro importantes, etc.), inyecten código en otros procesos o roben datos de la memoria de otras aplicaciones (scrappers de memoria). También bloquean lanzamientos ejecutables no confiables del espacio de usuario. Permiten lanzamientos desde el espacio de usuario para ejecutables firmados digitalmente de editores confiables. Pero éstos están sujetos a los controles de protección antes mencionados. AppGuard también mitiga los riesgos de malware sin exploits o ataques sin malware que usan motores de scripting y otras utilidades legítimas en los endpoint. Lo hace mediante el acceso denegado predeterminado a estos recursos, deshabilitando selectivamente los que no se necesitan y/o limitando lo que pueden hacer. Sin embargo, AppGuard tiene en cuenta el uso legítimo de estos recursos por parte de los IT-Ops. Estos y otros controles de AppGuard se combinan para vencer todas las formas de ataques de malware de punto final, incluso de zero-day.

APPGUARD

Intelligent Prevention for the Endpoint

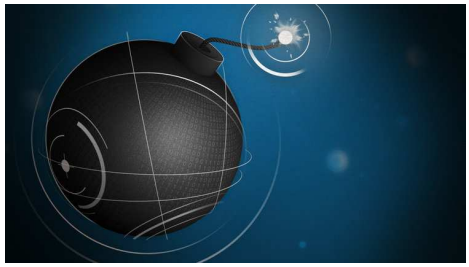


APPGUARD	ADVANCED THREATS	EDR	ML/EPP	WHITELISTING	CONTAINERS
●	Morphed & 0-day Malware	◔	◔	◑	◑
●	Weaponized Dox	◔	◔	○	◑
●	In-Memory	◔	◔	○	◔
●	Exploit-less Attacks	◔	◔	○	◑
●	Credential Theft (PtH/T)	◔	○	○	◔
●	Memory Scrapers	○	○	○	◔
●	Ransomware	◔	◔	◑	◑
●	Spear Phishing	◔	◔	◑	◑

APP GUARD	MITIGATION COSTS	EDR	ML/EPP	WHITELISTING	CONTAINERS
●	Overhead (CPU, RAM)	●	◕	●	◔
●	Cloud Dependence	○	◔	◑	◕
●	Transparent to End-users	◕	◕	●	○
●	App Compatibility	●	●	●	○
●	Complex Tuning	◕	◑	○	◕
●	Downstream Ops	○	○	◔	◑
●	False Positives	◑	◑	◕	◕
●	High Skills Admin	○	●	◕	◑

Recorta los Costes Cibernéticos en el Endpoint

La efectiva prevención de compromiso del endpoint de AppGuard reduce el volumen de alerta/incidente para la empresa. Considere los últimos cinco años: los fallos crónicos de los AV han hecho aumentar el volumen de violación de datos. Esto ha incrementado los costes de los IT-Ops y Sec-Ops necesarios para prevenirlos, detectarlos y responder a ellos. Estos costes se manifiestan en forma de herramientas, servicios, personal, procesos de negocio y ejercicios de preparación para áreas tales como: ciber higie-



ne, gestión de incidentes y eventos de seguridad (SIEM), cortafuegos de próxima generación, sistema de detección de brechas (BDS), respuesta a incidentes, análisis forense, remediación, inteligencia de amenazas y optimización de operaciones. El volumen de alerta/incidente del endpoint se relaciona directamente con todos estos costes indirectos. AppGuard reduce estos costes en el endpoint.

Reduce la brecha en habilidades empresariales

AppGuard fue diseñado para administradores competentes de Windows. La edición de políticas es tan simple como agregar un tema a una lista de reproducción. Debido a que AppGuard simplemente bloquea acciones inaceptables, los administradores no tienen que analizar y reaccionar a las alertas como se requiere de EDR y otros métodos que actúan después de la ejecución. AppGuard alivia la generalizada brecha de capacidades cibernéticas de dos maneras: en primer lugar, reduce las destrezas requeridas para proteger los endpoint; en segundo lugar, su protección altamente efectiva reduce todas las formas de volumen de incidente/alerta en cascada para los endpoint potencialmente comprometidos. La mayoría de las organizaciones, que carecen de protección de endpoint similar a AppGuard, implementan tantas funciones cibernéticas diferentes en cascada que exacerban la brecha de capacidades.

Bloquea al atacante por movimiento lateral (Pass the Hash/Ticket)

Sin embargo, el primero o más endpoint empresariales se ven comprometidos a través de un ataque dirigido; por lo general sirven como un principio de puente para extenderse al resto de la empresa hasta que los atacantes logren sus objetivos. Lo hacen conduciendo los ataques de hash/ticket. En pocas palabras, el hash y el ticket generalmente son desconocidos para los usuarios finales a pesar de la gran comodidad que les brindan. De lo contrario, los usuarios finales tendrían que responder a un desafío de inicio de sesión cada vez que acceden a algo en la empresa. El sistema operativo reproduce estos hash/ticket para los endpoint libres. Desafortunadamente, los atacantes pueden copiarlos desde la memoria de un endpoint para suplantar a los usuarios finales. Peor aún, la memoria también incluye frecuentemente altas credenciales de privilegio. ¿Por qué perder tiempo infectando otras máquinas cuando hacerse pasar por identidades existentes es mucho más fácil?

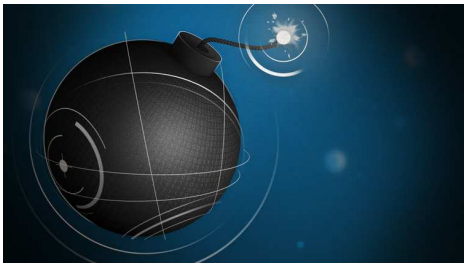
Microsoft lanzó funciones para mitigar estos riesgos, pero los pentester y los hacker poco después los habían superado. Los productos alternativos afirman que mitigan estos riesgos, pero hay dos advertencias principales: primero, lo hacen, siempre que detengan las primeras etapas de un ataque; en segundo lugar, detectan y reaccionan. AppGuard bloquea estos robos de credenciales sin salvedades y lo hace de una manera auténtica y ya no hay que preocuparse de ello.

Indicator of Attack / Threat Intelligence Data

Si bien AppGuard no necesita datos de IoA o IoC para proteger los puntos finales, recopila datos de IoA detallados sobre los ataques que la mayoría de los EPP y otras herramientas no pueden detectar hasta semanas o meses después, e incluso más para weaponized documents. Y cuando los demás se ponen al día, están capturando datos de IoC, que carece de la valiosa in-

APPGUARD

Intelligent Prevention for the Endpoint



formación encontrada en los datos de IoA. Además, los datos de IoA de AppGuard difieren de las alternativas en que no se deben comprometer endpoint para capturar datos de inteligencia de amenazas. Todo esto está disponible en el back-end para ser utilizado por SIEM y otras herramientas.

Alivia la presión de gestión de parches

Con el 75 por ciento de los profesionales de TI admitiendo que no pueden mantenerse al día con los parches de software ("The Cost of Insecure Endpoints", Ponemon, junio de 2017), AppGuard es un excelente control de compensación. Su diseño asume que las aplicaciones de endpoint tienen vulnerabilidades explotables desconocidas. Por este motivo, el producto se llama AppGuard porque muchos de sus controles efectivamente colocan estas aplicaciones bajo "guardia" para que no causen daños. La presión de parches que AppGuard alivia puede liberar recursos limitados para realizar otras tareas importantes. El parche sigue siendo recomendable, pero no es necesario apresurarlo o hacerlo a expensas de otras tareas importantes.

Auténtico "configurar y olvidarse" en la Protección del Endpoint

Al evitar compromisos en los endpoints sin firmas de ningún tipo, AppGuard no requiere actualizaciones ni ayuda de la nube para proteger los endpoints de las últimas amenazas. Si AppGuard se hubiera implementado en todas las máquinas expendedoras de PoS hace cinco años sin actualizaciones, ninguna de las infracciones de los minoristas que llegaron a los titulares se habría producido. Los productos AV y de machine learning requieren actualizaciones continuas; sus tasas de detección disminuyen cuando están fuera de línea. El acceso por Internet a una nube no está garantizado. Los casos de uso para endpoint fuera de línea van desde usuarios finales que ven archivos adjuntos de correo electrónico en aviones hasta sistemas de control industrial y otros endpoint de funciones especiales que deben estar aislados de Internet y del espacio normal de TI.

APPGUARD
A Blue Planet-works Company

Michael Oleata
moleata@appguard.us
+1 858 766 8650

C2S3H
Consultoría de CiberSeguridad
Servicios - Software - Hardware

Josep M. Felix i Zahonero
j.felix@c2s3h.com
+34 688 99 49 50

Sobre AppGuard LLC

Las personas y las organizaciones de todo el mundo están cada vez más interconectadas a través de los dispositivos terminales en sus vidas. AppGuard ofrece soluciones simples y efectivas para los complejos desafíos de seguridad que amenazan los intereses de las organizaciones y los de sus clientes. Estos endpoint van desde computadoras personales a teléfonos inteligentes/tabletas o dispositivos IoT.

Las soluciones de AppGuard evitan el compromiso del endpoint, facilitan alta seguridad en la autenticación dispositivo a dispositivo en nombre de sus usuarios, confirman la seguridad de ambos endpoint para que uno no comparta datos confidenciales con un usuario ubicado en un endpoint no confiable y protegen la privacidad de los usuarios finales a través de la autenticación anónima y de alta seguridad de dispositivo a dispositivo para que puedan comunicarse de forma segura sin revelar información de identificación personal de los usuarios finales.

"AppGuard debe estar en todos los sistemas Windows del mundo."

Robert Bigman
Former CISO, CIA

"AppGuard es un método completamente nuevo y mejor para proteger los puntos finales."

Hiro Higuma
Former President of Symantec Japan
New Chief Strategic Officer AppGuard LLC