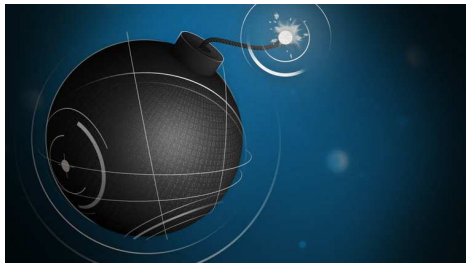
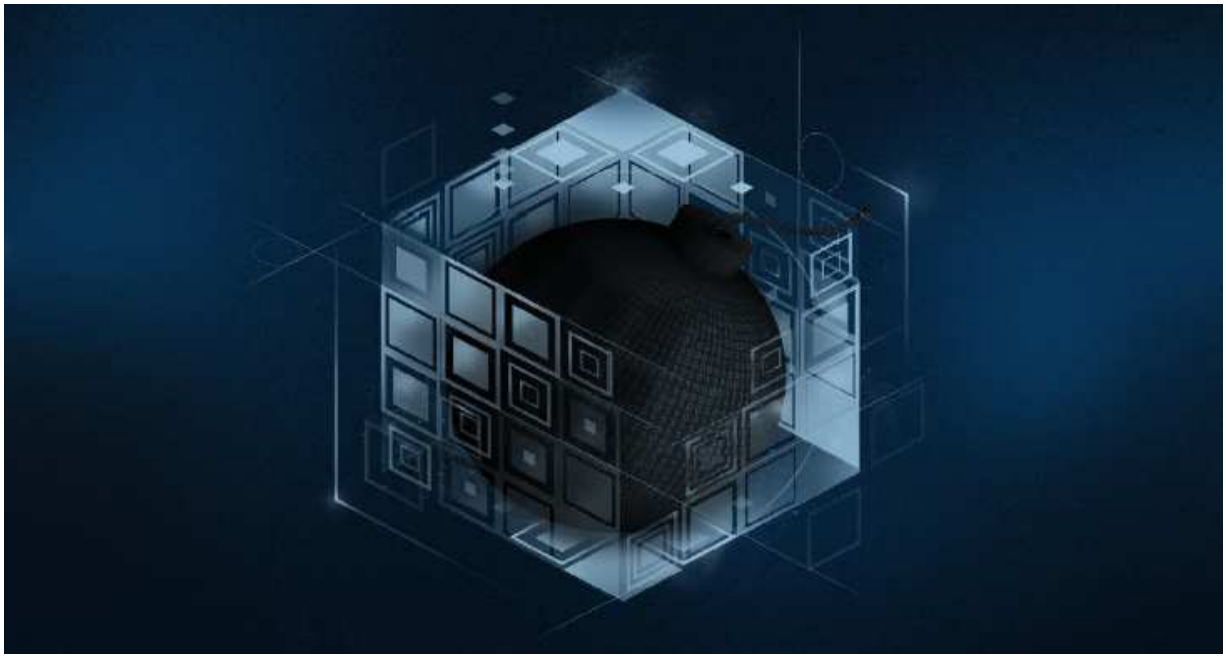
APPGUARD

Intelligent Prevention for the Endpoint



La protección efectiva del Endpoint simplifica las operaciones de IT/Sec

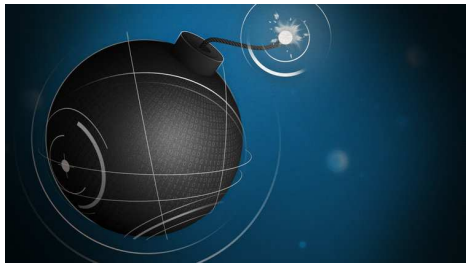


February 2018

APPGUARD

APPGUARD

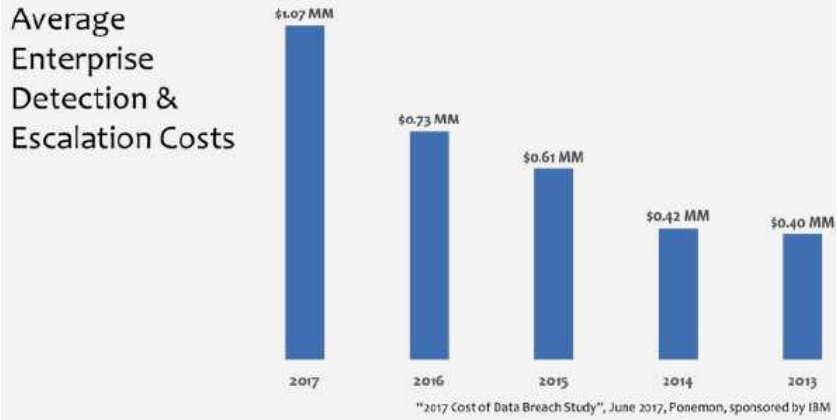
Intelligent Prevention for the Endpoint



La empresa está invadida con herramientas ineficaces de ciberseguridad

En 2016, IDC estimó que el 70% de las violaciones empresariales exitosas comenzaron en el punto final. Esto ha estado ocurriendo por más de una década. Y, cada año, la empresa ha agregado una nueva herramienta o práctica para evitar o reducir las infracciones. Éstas se han acumulado para producir un nudo complejo de Operaciones de IT/Sec. La prevención en el endpoint reduce el tiempo utilizado en detección+reacción.

Más brechas, más gasto cibernético



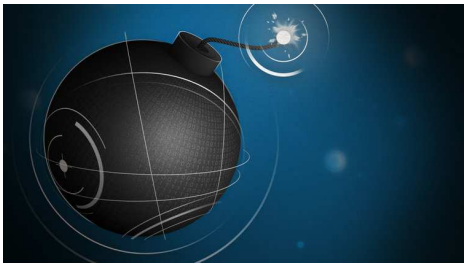
Las operaciones empresariales de IT/Sec se han vuelto cada vez más costosas y complejas año a año, durante más de una década y todas las indicaciones apuntan a una tendencia continua. Casualmente, el término "plataforma de protección de punto final" (EPP) se acuñó hace aproximadamente una década, concretamente en 2007. El concepto era simple: un único agente con un solo panel de administración debería simplificar las operaciones de IT/Sec en comparación con la de muchos agentes y paneles. Cualquier ahorro de consolidación que pudiera haberse generado fue eclipsada por los costos crecientes de la "protección" inadecuada del PPE. Esta situación ha creado un nuevo mercado de agentes de endpoint llamado "detección y respuesta de endpoint" (EDR), que recientemente ha sido declarado oficialmente como un elemento vital de EPP.

Las nuevas características de EPP no suponen mayor eficiencia de seguridad

Antes de mirar más allá de EPP a otras herramientas y tareas que exprimen los presupuestos de Operaciones de IT/ Sec, hay un punto que cualquier persona involucrada con la seguridad de los endpoint debe explorar con respecto a la combinación de varias herramientas en un solo binario. Sin esta perspectiva, uno elige erróneamente el EPP con la lista más larga de características, en lugar de la que produce los mejores resultados. ¿Cómo la integración de UN SOLO control cibernético con los demás hace que los otros sean más simples? Un ejemplo rápido de AppGuard (no un EPP) se refiere a dos controles diferentes: la lista blanca de aplicaciones y la conformidad del proceso adaptativo (*adaptive process conformance*). Este último asegura que las aplicaciones en riesgo no pueden alterar el espacio del sistema de un endpoint. Esto significa que la lista blanca de AppGuard sólo necesita centrarse en el espacio del usuario, reduciéndola de 100.000 elementos a menos de dos docenas. Con la mayoría de los EPP, existe poca o ninguna sinergia con la combinación de múltiples agentes en uno.

APPGUARD

Intelligent Prevention for the Endpoint



'Detect & React': más complejidad, menos resultados

Más allá del software de endpoint, SIEM evolucionó para servir como almacén de datos para todas las fuentes de datos relevantes de operaciones de IT/Sec, incluidos los eventos de registro de los endpoint. Las herramientas de red superpuestas de la última década, como los firewalls de próxima generación, los sistemas de detección/prevención de intrusiones y los sistemas de detección de brechas generan volúmenes de alerta que se correlacionan fuertemente con el uso de los endpoint de los empleados. La facilidad de movimiento lateral de un endpoint a otro hasta obtener el control de administrador ha llevado a otra categoría de herramientas llamada análisis de comportamiento del usuario del endpoint. Estas herramientas técnicas y otras conforman gran parte de lo que se conoce como la postura de "detectar y reaccionar " que impregna el espacio de operaciones IT/Sec empresariales. Una variedad de herramientas de corrección (re-imaging, clean-up, password management, key management, backup management, etc.) completan el resto de la carga de trabajo de "detección y reacción".

Lamentablemente, muchos expertos ven la ciberseguridad demasiado como una cuestión de tecnología y muy poco como un atolladero para la gente. Las diferentes tecnologías que bloquean, defienden, supervisan y restauran redes y endpoint empresariales requieren cada vez más personas para operar cada año. Por otra parte, la novedad del machine learning y la inteligencia artificial, al menos tácitamente, reconoce que los enfoques actuales de las actuaciones de IT / Sec son ineficaces e insostenibles con los recursos actualmente disponibles por los usuarios.

Top Challenges Facing SOC	
70%	Detection of Advanced Threats
59%	Lack of Expert Staff
49%	Intruder/Insider Detection
49%	Slow Incident Response
47%	Time Wasted on False Positives

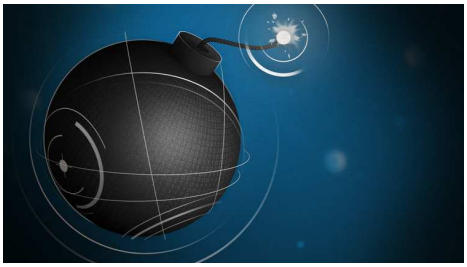
Source: "Cybersecurity Trends, Spotlight Report", (ISC)², June 2017

Para simplificar las operaciones de IT/Sec, analice el tiempo empleado

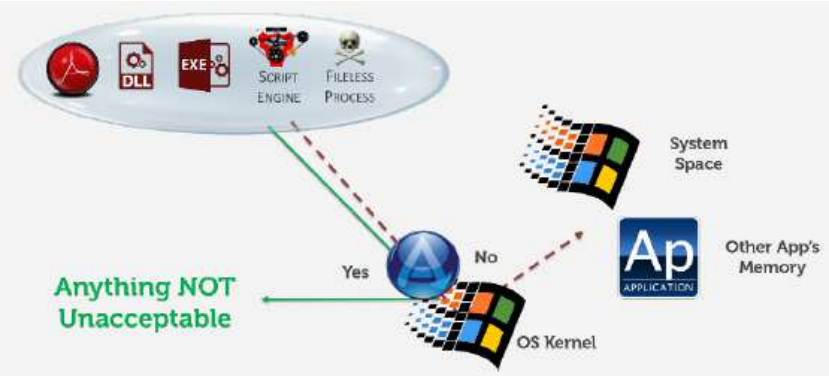
Los líderes empresariales no pueden permitirse el lujo de apostar únicamente en las tecnologías de big data revirtiendo las tendencias de operaciones IT/Sec, especialmente porque los atacantes las usan también. En cambio, su búsqueda de operaciones IT/Sec más simples y efectivas debe basar sus decisiones y selecciones de herramientas en minimizar el tiempo que se dedica. Bajo este punto obvio se encuentra la clave menos conocida para hacer que las operaciones IT/Sec sean más simples, más livianas y más efectivas: la mitad o más del tiempo utilizado en operaciones IT/Sec se correlacionan con lo que ocurre en sus endpoint. Una manera simple pero cruda de comenzar a ver esto es comparar volúmenes de alertas o incidentes para 'días de trabajo' con los de 'días libres', cuando los empleados están mucho menos involucrados con sus endpoint. Una mirada más metódica puede mostrar correlaciones estadísticamente significativas para todos los elementos de desglose del trabajo de operaciones IT/ Sec en el endpoint. Estas correlaciones identifican muchas herramientas y tareas que consumen grandes cantidades de tiempo de trabajo.

APPGUARD

Intelligent Prevention for the Endpoint



AppGuard alivia los desafíos de gestión de parches



Comencemos con la administración de parches del endpoint; AppGuard efectivamente 'contiene' cualquier aplicación no parcheada, bloqueando acciones dañinas, permitiendo todas las demás. Por ejemplo, en la ilustración con Adobe Acrobat en una burbuja, AppGuard garantiza dinámicamente que cualquier cosa que genere o lo que genere no puede realizar cambios en el espacio del sistema, ni interferir con la memoria de otra aplicación. Lo mismo se aplica si una aplicación está parcheada o no.

Además, las actualizaciones de la aplicación raramente afectan a las protecciones de AppGuard. Obtenga más información sobre qué y cómo AppGuard bloquea los ataques de códigos maliciosos. Esto no debería eliminar su agente de administración de parches. Pero cualquiera que sea la tarea que habitualmente se interrumpe o retrasa para probar, implementar y verificar rápidamente uno o más parches urgentes, no es necesario que lo haga más. También debería haber menos parches que salieron mal porque AppGuard concede a los "tester" suficiente tiempo para que puedan trabajar de manera metódica.

AppGuard reemplaza las herramientas de endpoint y su gestión con mejoras

En cuanto a la protección de endpoints, AppGuard reemplaza todas y cada una de esas herramientas, excepto para el escaneo reglamentario obligatorio. La mayoría de los clientes de AppGuard satisfacen esto con Windows Defender o cualquier AV gratuito. Un EPP, sin embargo, puede incluir muchos conjuntos de herramientas diferentes que requieren una gran cantidad de tiempo de trabajo para configurar y mantener. AppGuard puede eliminar todas las horas dedicadas por sus operaciones de IT/Sec en lo siguiente:

- Aplicación lista blanca
- Protección contra exploits / memoria
- Sandbox basado en el host
- Antivirus basado en Machine Learning

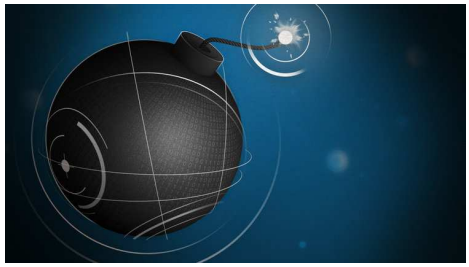
Las operaciones de IT/Sec para AppGuard reducen significativamente o, en algunos casos, eliminan el tiempo de trabajo en comparación con estas herramientas. Las implementaciones típicas de AppGuard Enterprise se ejecutan durante muchos meses sin NINGUNA actualización, de ningún tipo.

AppGuard reduce la fatiga de alerta y el tiempo de trabajo utilizado

En cuanto a 'detectar y reaccionar', hablemos de las alertas. La fatiga de las alertas está agotando al personal y dejando mucho trabajo sin realizar. Si sólo la mitad de su volumen de alerta fuera directa o indirectamente manejado por el endpoint, entonces AppGuard liberaría a su personal de IT para investigar las alertas no estudiadas, que serían principalmente de sus servidores de aplicaciones de misión crítica interna y de Internet, donde con baja frecuencia tiende a ocurrir alertas de infracciones.

APPGUARD

Intelligent Prevention for the Endpoint



Alerts Fatigue	
56%	Alerts Investigated
28%	Of Investigated, are Legitimate
46%	Of Legitimate, are Remediated

Source: "2017 Security Capabilities Study", January 2017, Cisco

Después de algunos meses de confianza en la protección, tras la implementación de AppGuard en sus endpoints, puede decidir que su agente EDR ya no es necesario. En este momento, su volumen de alertas de EDR no sólo se desplomará, sino que los eventos de registro de AppGuard que se ejecutan a través de su SIEM revelarán que AppGuard está bloqueando los ataques antes de que EDR pueda detectarlos. Esta fue una excusa de un vendedor de EDR bien conocido cuando nuestro cliente común le preguntó al por qué no detectaban una campaña de ataques de weaponized document. De forma similar, si tiene implementados agentes de endpoint SIEM, puede cuestionar el valor de seguir usando éstos también. Recuerde, las implementaciones de agentes EDR y SIEM fueron necesarias al existir soluciones de protección poco efectivas, antiguas y muy extendidas en los endpoint.

AppGuard reduce las operaciones de respuesta de red e incidentes

Al mismo tiempo, es probable que su liderazgo cibernético reconsidere el valor de retener por completo un firewall de próxima generación, un IDS/IPS dedicado y/o un sistema de detección de brechas. Una vez más, esto depende de la infraestructura IT existente y de qué proporción de ella consiste en la actividad de los técnicos especializados.

Y lo mismo le ocurrirá con respecto a su respuesta a incidentes y recursos de protección. La decisión más difícil que se encontrará durante esta transición será decidir qué hacer con todos esos recursos, después de que el volumen de los incidentes de endpoint se haya desplomado.

Impact from Cyber Skills Shortage	
63%	Increased Workload for Staff
41%	Rely on Junior Personnel
41%	Reactive over Proactive

Source: "The Life and Times of Cybersecurity Professionals", Enterprise Strategy Group, Information Systems Security Association, November 2017

AppGuard permite el cambio de reactivo a proactivo

Con tantos recursos variados disponibles, con gran parte de su personal de operaciones de IT/Sec que ya no está en constante búsqueda del próximo incidente, su organización puede perseguir estratagemas de madurez de seguridad de alto nivel. Por ejemplo, si la clasificación de alertas fue demasiado abrumadora, reactiva y desafinada, entonces no podría permitirse invertir en una adecuada investigación de amenazas. Muchas capacidades diferidas serán posibles una vez que la protección del endpoint sea efectiva.

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