SOPHOS
Security made simple.

Cambiar a una protección Next-Gen Endpoint

Marty Ward, vicepresidente de marketing de productos, Sophos

Las amenazas son cada vez más dinámicas e industrializadas, lo que obliga a las organizaciones no solo a defenderse contra el malware tradicional, sino también contra nuevos ataques más avanzados. La consecuencia es que cada vez más organizaciones están tomando la decisión de cambiar a la protección Next-Gen Endpoint de Sophos para obtener la defensa innovadora y de fiabilidad probada que necesitan. Este informe describe cómo la protección Next-Gen Endpoint de Sophos proporciona la protección, facilidad de uso y soporte necesarios para estar un paso por delante del panorama de amenazas actual en continua evolución.

"Cibercriminales más astutos y rápidos provocan un gran pico en el número de ciberataques."[1]

Un día más, un titular más. Filtraciones de datos importantes. Nuevas estadísticas alarmantes.

El entorno de las ciberamenazas es más dinámico que nunca. La información del informe de las investigaciones sobre la filtración de datos de Verizon del 2015 [2] dibuja un panorama preocupante de un entorno de amenazas que sigue creciendo en lo que se refiere al volumen de los ataques, así como su velocidad y sofisticación.

- En el 2014, los incidentes de seguridad aumentaron un 26%, mientras que las filtraciones de datos confirmadas tuvieron un crecimiento masivo del 55%.
- En el 60% de los casos, los atacantes son capaces de infectar una organización en cuestión de minutos.
- Entre el 70 y el 90% de las muestras de malware son únicas para cada organización.

Además, la concienciación sobre el problema de las ciberamenazas no ha dejado de crecer, tanto entre el público en general, como en el entorno empresarial. De nuevo citamos el informe de Verizon: "El New York Times [dedicó] más de 700 artículos a temas sobre filtraciones de datos, en comparación con los menos de 125 del año anterior." De forma similar, la concienciación sobre las ciberamenazas dentro de las organizaciones también está creciendo, tanto entre los empleados como entre directivos.

Aumento del gasto en seguridad, con algunos peros

Con el aumento de la concienciación entre el público en general y el entorno empresarial, no debe sorprender que las organizaciones sigan incrementando su gasto en seguridad informática. Según el estudio global sobre el gasto e inversiones en seguridad informática del 2015 de Ponemon [3], el 46% de las organizaciones aumentaron sus partidas dedicadas a seguridad en los dos últimos años, y el 50% tiene previsto aumentarlas durante los dos años siguientes.

Sin embargo, el estudio de Ponemon también plantea preguntas sobre el resultado que han tenido esas inversiones en seguridad: "Las empresas admiten que algunas de sus compras tecnológicas les han defraudado. Según las respuestas obtenidas, de media, el 37% de las inversiones realizadas en seguridad durante los últimos 2 años no cumplieron las expectativas."

Los cinco principales temas de preocupación y causantes de este descontento señalados por las organizaciones en el estudio de Ponemon se encuadran dentro de las siguientes 3 áreas principales:

1. Protección (efectividad del sistema)
2. Facilidad de uso (complejidad del sistema, personal y falta de experiencia a nivel interno de la empresa, costes de instalación)
3. Soporte (soporte del proveedor)

En Sophos preguntamos a nuestros nuevos clientes sobre los motivos de su cambio a nuestras soluciones de protección endpoint, y muchas de las respuestas que obtuvimos coinciden con los principales temas de preocupación desvelados en el estudio de Ponemon. Principalmente están frustrados con los continuos brotes de malware que su solución anterior no lograba detener, un rendimiento deficiente, el empleo de múltiples agentes, la complejidad del producto, soporte insuficiente y las dificultades para configurar una serie más amplia de defensas integradas.

Evolución de las amenazas

Los problemas anteriores son el resultado, por una parte, de la evolución permanente de las amenazas, y por otra, que los clientes siguen intentando defenderse con soluciones anticuadas. La seguridad endpoint tradicional se creaba contra virus, troyanos y gusanos, pero las amenazas actuales han evolucionado hacia técnicas de aprovechamiento de vulnerabilidades, ransomware y ataques en memoria. Las amenazas de hoy en día han cambiado tanto de tipo como de objetivos.

En la figura 1 a continuación destacamos algunas de las tendencias claves, incluyendo el hecho de que la mayoría de las amenazas ahora son ataques desconocidos de día cero. También han pasado de ser malware sencillo a ataques industrializados muy coordinados, que frecuentemente incluyen técnicas de ataque y mecanismos de comunicación múltiples. Dado el hecho de que la seguridad endpoint tradicional ha cumplido su objetivo en la prevención contra el malware, los cibercriminales han pasado a la apropiación de credenciales con el fin de poder moverse por los sistemas como un usuario legítimo o administrador.

Figura 1. Tendencias en la evolución de las amenazas

Amenazas	Objetivos
Conocidas a desconocidas El 75% del malware dentro de una organización es exclusivo a esa organización (Fuente: Sophos Labs)	**Empresas grandes a pequeñas** El 70% de todas las organizaciones informan haberse visto afectadas en los últimos 12 meses. (Fuente: Sophos Labs)
Simples a industrializadas A medida que las plataformas de malware como servicio evolucionan, los códigos maliciosos están siendo monetizados en la Web Oscura con las mismas presiones de mercado que las que gobiernan a cualquier industria convencional. (Fuente: FBI / InfoSec London)	**Generales a específicas** Los kits de exploits provocan más del 90% de todas las filtraciones de datos (Fuente: NSS Labs)
Malware a hacking El 63% de todas las filtraciones de datos están relacionadas con credenciales robadas (Fuente: Verizon DBIR)	**Cualquiera hasta el más débil** El tiempo medio para solventar vulnerabilidades es 193 días (Fuente: WhiteHat Security)

Además, los objetivos de los ataques también han cambiado. En lugar de centrarse solo en las grandes empresas, los ciberdelincuentes se han dado cuenta de que las PYMES también tienen datos igualmente de valiosos y que, además, frecuentemente están asociadas con estas grandes empresas, por lo que los datos están compartidos por doquier, hecho que les facilita moverse entre las empresas para acceder a los datos que quieren.

Los kits de exploits, que son herramientas de "hacking como servicio" que cualquiera puede usar, ahora son los responsables del 90% de todas las filtraciones de datos. Permiten a los cibercriminales dirigir sus ataques de forma muy precisa, seleccionando la demografía que desean para maximizar la efectividad de sus acciones. Además, como las empresas todavía suelen tardar medio año en solventar las vulnerabilidades conocidas, los ciberdelincuentes están cambiando su forma de actuar con ráfagas de ataques "a ciegas" por ataques centrados en aprovechar esta falta de celo.

Evolución de la seguridad endpoint

La buena noticia es que la industria de la seguridad también ha seguido evolucionando. En esta partida de ajedrez entre cibercriminales y proveedores de seguridad que ya dura años, cada movimiento es contrarrestado por otro movimiento, con cada parte esperando poder saltarse al contrario. La industria de la seguridad siempre ha estado fascinada por el concepto de la bala de plata, y como tal, hay más de 1000 empresas de tecnología de seguridad en el mundo hoy en día, muchas de ellas con una sola tecnología que creen que es la solución a todos los problemas. Desafortunadamente, sabemos que esta no es la respuesta.

Al igual que hay múltiples piezas en una partida de ajedrez, también son necesarias múltiples tecnologías para proteger completamente todos los endpoints. Las opciones de seguridad tradicionales enumeradas en la figura 2, como prevención de la exposición, análisis previo a la ejecución y escaneado de archivos, siguen siendo ingredientes necesarios para bloquear el malware tradicional. Como suele decir Chet Wisniewski, científico investigador jefe en Sophos: "Quemar el pajar hace mucho más fácil encontrar la aguja".

Figura 2. Evolución de la seguridad endpoint
Desde anti-malware a anti-exploits

Seguridad tradicional			Seguridad avanzada	
Prevención de la exposición	**Análisis previo a la ejecución.**	**Escaneado de archivos**	**Tiempo de ejecución**	**Detección de vulnerabilidades**
Bloqueo de direcciones web Web/App/Contr. disp. Rep. descargas	Identificación genérica Heurística Reglas básicas	Malware conocido Malware Bits	Análisis de comportamiento Comportamientos en tiempo de ejecución	Identificación de técnicas

Es muy probable que esta aguja aparezca en forma de un avanzado ataque en memoria o exploit, que es la razón por la que se necesita la detección y prevención en tiempo de ejecución, así como la detección de exploits en las soluciones para la protección endpoint. Estas avanzadas tecnologías de prevención (y sin firma) buscan técnicas exploit y comportamientos que bloquearán ataques avanzados desconocidos.

Aunque pensamos que la "defensa profunda" sigue siendo una buena estrategia, la bala de plata de la seguridad es la integración de todas estas tecnologías para que actúen como un sistema de seguridad coordinado, un sistema incluso más sofisticado que los ataques avanzados dirigidos que sufren las empresas de hoy en día.

Transformar la protección endpoint con Sophos

Para hacer progresos reales contra las amenazas de hoy en día, es esencial invertir en las soluciones de seguridad informática más efectivas, considerando la plantilla y la experiencia disponibles. Sophos Next-Gen Endpoint Protection no sólo integra un amplio abanico de avanzadas tecnologías de seguridad, sino que también ofrece un diseño inteligente, además de estar respaldado por un soporte de categoría mundial para un rendimiento pleno en su organización.

Protección innovadora

Sophos combina las defensas contra amenazas más recientes con tecnología anti-malware probada:

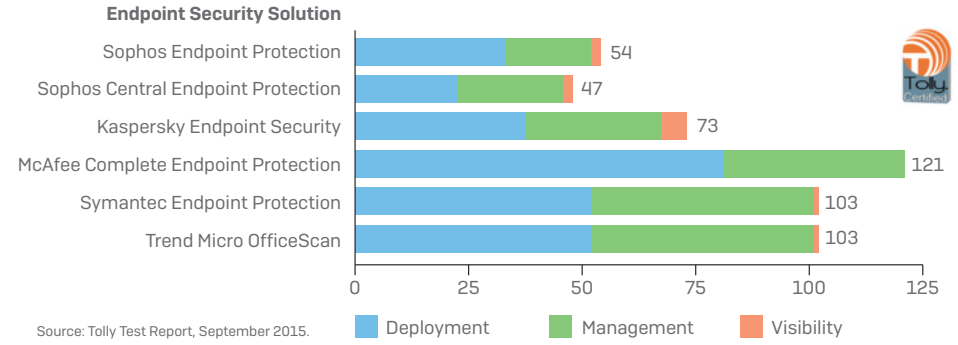
PREVENIR		DETECTAR	RESPONDER
Antes de que llegue al dispositivo	Antes de que se ejecute en el dispositivo	Detener la amenaza en ejecución	Investigar y eliminar
Protección web Bloqueo de scripts maliciosos y redireccionamientos usados para entregar amenazas. **Reputación de descargas** Uso de múltiples variables para avisar a los usuarios sobre archivos que aunque no se hayan confirmado como maliciosos pueden no ser de confianza. **Control web** Filtrado web por categorías impuesto tanto en la red corporativa como fuera. **Control de dispositivos (p. ej., memoria USB)** Gestión del acceso a medios extraíbles y dispositivos móviles y prevención de filtraciones de datos utilizando reglas predeterminadas o personalizadas. **Restricción de aplicaciones** Bloqueo de aplicaciones mediante clic por categoría o nombre. **Prevención de ataques a navegadores** Identifica y bloquea los intentos para aprovechar las vulnerabilidades que podrían usarse para secuestrar el navegador web.	**Escaneado de archivos anti-malware** Se ejecuta activamente en un endpoint para identificar malware conocido y archivos sospechosos y evitar su ejecución. **Protección activa** Comunicación en tiempo real con SophosLabs para el análisis de firmas de archivos sospechosos, consultas de reputación de URL y descargas y enviar archivos altamente sospechosos a Labs para su análisis adicional en un espacio seguro. **Análisis de comportamiento previo a la ejecución / HIPS** Se sirve de la tecnología de protección Behavioral Genotype de Sophos para bloquear código de ordenador susceptible de ser malicioso antes de que se ejecute. **Bloqueo de aplicaciones no deseadas** Bloquea programas que no son necesariamente maliciosos, pero que por lo general se consideran inadecuados en la mayoría de las redes empresariales. **Prevención de exploits** Identificación y bloqueo de intentos para aprovechar vulnerabilidades de aplicaciones o sistemas operativos.	**Análisis de comportamiento en tiempo de ejecución / HIPS** Analiza de forma dinámica el comportamiento de todos los programas ejecutándose en el sistema para detectar y bloquear aquellos cuya actividad parezca maliciosa. **Detección de tráfico malicioso (MTD)** Identificación y alerta cuando el malware intenta comunicarse con los servidores de comando y control. **Protección CryptoGuard contra ransomware** Detecta el cifrado espontáneo malicioso de archivos, detiene el ataque y, a continuación, devuelve los archivos a su estado seguro.	**Eliminación de malware automatizada** Elimina el malware de los endpoints sin la intervención del administrador, generando una alerta si se requiere una intervención manual. **Seguridad sincronizada** Comunicación entre las estaciones y el cortafuegos mediante el avanzado Security Heartbeat™ para acelerar la detección de amenazas y automatizar la respuesta ante incidentes. **Análisis de causa raíz** Hace un seguimiento de la historia de un ataque, desde la aplicación utilizada para el ataque hasta el punto en el que se ha condenado el ataque. También proporciona consejos para acciones correctivas y una guía de prácticas recomendadas. **Sophos Clean** Limpieza analítica en profundidad de ataques avanzados que extermina el malware incluyendo los archivos afectados remanentes y las claves de registro.

Simplicidad sofisticada

Para que estas defensas funcionen en su organización, en su diseño fue prioritario que fuesen fáciles de configurar, implementar y administrar. Unas políticas predeterminadas razonables y la función de seleccionar y listo mediante un clic, le ayudarán a implementar la protección de forma rápida. A su vez, un panel de control intuitivo y fácil de usar proporciona una excelente visibilidad de su entorno y un acceso rápido a las tareas administrativas rutinarias.

Las pruebas independientes sobre su facilidad de uso realizadas por Tolly[4] confirman que Sophos es significativamente más fácil de usar que otras soluciones de seguridad para estaciones (figura 3).

Figura 3. Número de pasos necesarios para la implantación, administración y visibilidad (es mejor cuanto menor sea el número).



Sophos Central Endpoint Protection, anteriormente Sophos Cloud Endpoint Protection.

Soporte especializado

Independientemente de lo fácil que sea usar una solución, habrá ocasiones en las que no queda otra que recurrir a ayuda externa. Sophos mantiene un equipo global de expertos interno disponible las 24 horas los siete días de la semana. Y más importante aún, el equipo de soporte de Sophos logra de forma persistente unas puntuaciones de satisfacción del cliente altas para que los clientes sigan volviendo en caso de que requieran ayuda y puedan aprovechar las características de seguridad adicionales de Sophos Endpoint Protection.

"De la noche a la mañana pasamos de una situación con una protección mínima y un soporte casi inexistente a una solución que no solo es efectiva y fácil de gestionar, sino que también está respaldada por un soporte fuera de serie."

ROBERT TALLEY
Director de TI, Lassen County Office of Education

"Teníamos un producto de Symantec y tardé dos horas en desplegar Sophos en unos 800 equipos. ¡Increíble!

STEVE
Administrador de redes, industria de videojuegos

Migración a Sophos Next-Gen Endpoint – un proceso de cinco pasos

Para la mayoría de las organizaciones, la barrera más importante a la hora de migrar a la protección next-gen endpoint es el incordio que supone el cambio. En Sophos el trabajo con miles de clientes nos ha permitido definir un proceso de migración perfecto. En muchos casos, este proceso puede completarse en cuestión de horas o días.

1. Selección e instalación de la consola de administración
Sophos ofrece opciones de administración local o en la nube.

- **Sophos Central** es la vía más rápida para una consola de administración completamente operativa. Tras activar una cuenta de Sophos Central, se puede configurar y distribuir en menos de cinco minutos.
- Para los clientes que prefieran una consola de administración local tradicional, instale y configure **Sophos Enterprise Console** y los correspondientes componentes de administración.

2. Preparación del paquete de implantación en el endpoint
El paquete de distribución de Sophos incluye una herramienta de eliminación de software de la competencia que se puede personalizar para eliminar completamente el software específico utilizado en su entorno. Una vez eliminado el software de seguridad anterior, el paquete de instalación de Sophos Endpoint Protection completa la implantación del software de Sophos Endpoint Protection. El proceso incluye opciones para que la instalación se produzca de forma interactiva o en segundo plano. Con esta última opción el proceso de implantación es transparente para minimizar el impacto sobre los usuarios.

3. Configuración de las políticas de Sophos Endpoint Protection
Sophos Endpoint Protection incluye una serie de características de seguridad endpoint que podrían haber estado presentes, o no, en su solución de seguridad endpoint anterior. Comience configurando las políticas de protección que estuviesen presentes en su solución anterior, como el antivirus.

Puede seleccionar activar las nuevas características de Sophos Endpoint Protection, como la detección de tráfico malicioso, el control de aplicaciones y el control web, durante la implantación inicial de Sophos Endpoint Protection o decidir implantarlas progresivamente.

4. Despliegue inicial
La práctica recomendada para cualquier despliegue inicial de software nuevo en endpoints, incluyendo Sophos Endpoint Protection, es comenzar por implantar el nuevo software en un número limitado de puestos para probar el proceso de implantación y verificar el funcionamiento del nuevo software de seguridad. Seleccione endpoints de prueba que sean fácilmente accesibles y que se estén usando de forma activa, para probar de forma rápida la implantación y comprobar el funcionamiento.

5. Despliegue definitivo en toda la organización
Tras el despliegue de prueba inicial ya está preparado para completar la implantación de Sophos Endpoint Protection en toda su organización. En el caso de organizaciones más grandes, el despliegue final se puede subdividir en fases, basándose en criterios geográficos u organizativos, o cualquier otro criterio aplicable a su organización.

Como con cualquier otra tecnología recién implantada, con Sophos Endpoint Protection también se debe superar una curva de aprendizaje antes de alcanzar el pleno rendimiento. Sin embargo, la mayoría encuentra nuestra solución tan fácil de usar que la inversión inicial es devuelta con creces gracias a los ahorros en administración, así como la posibilidad de disponer de más características de seguridad en la estación.

Conclusión

Con el avance tan rápido de las ciberamenazas, las organizaciones se ven obligadas a buscar formas de optimizar sus inversiones en seguridad informática. Para evitar el remordimiento del comprador y asegurar que tiene la solución más efectiva para su organización, tres son los factores claves que se deben considerar al seleccionar un producto para estaciones:

1. **Protección** – ¿ofrece todas las opciones de seguridad que necesita para prevenir, detectar y dar respuesta a las amenazas de hoy en día?
2. **Facilidad de uso** – ¿puede distribuir y administrar la solución de forma satisfactoria considerando sus empleados y los conocimientos de su equipo de seguridad informática?
3. **Soporte** – ¿recibirá ayuda de alta calidad de expertos en seguridad siempre que lo necesite?

Para muchas organizaciones, Sophos Next-Gen Endpoint ha sido el paso adelante necesario para obtener toda la protección, facilidad de uso y soporte que necesitan. Si no está del todo satisfecho con su proveedor de seguridad actual, a lo mejor ha llegado ya el momento de unirse a los miles de clientes que ya se han cambiado a Sophos.

Para más información sobre Sophos Next-Gen Endpoint Protection o solicitar una evaluación gratuita, visite **www.sophos.com/es-es/endpoint**.

Referencias

1. "Hackers más astutos y rápidos provocan un gran pico en el número de ciberataques", USA Today, 15 de abril del 2015
2. Informe de las investigaciones sobre la filtración de datos 2015, Verizon Enterprise Solutions, abril del 2015.
3. Estudio global sobre el gasto e inversiones en seguridad informática 2015, Ponemon Institute LLC, mayo del 2015.
4. Informe de pruebas Tolly, septiembre del 2015.

Sophos Next-Gen Endpoint Protection

Visite sophos.com/es-es/endpoint para realizar una evaluación gratuita durante 30 días

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en Latin America
Correo electrónico: Latamsales@sophos.com

2016-09-22 SB-ES (NP)

SOPHOS