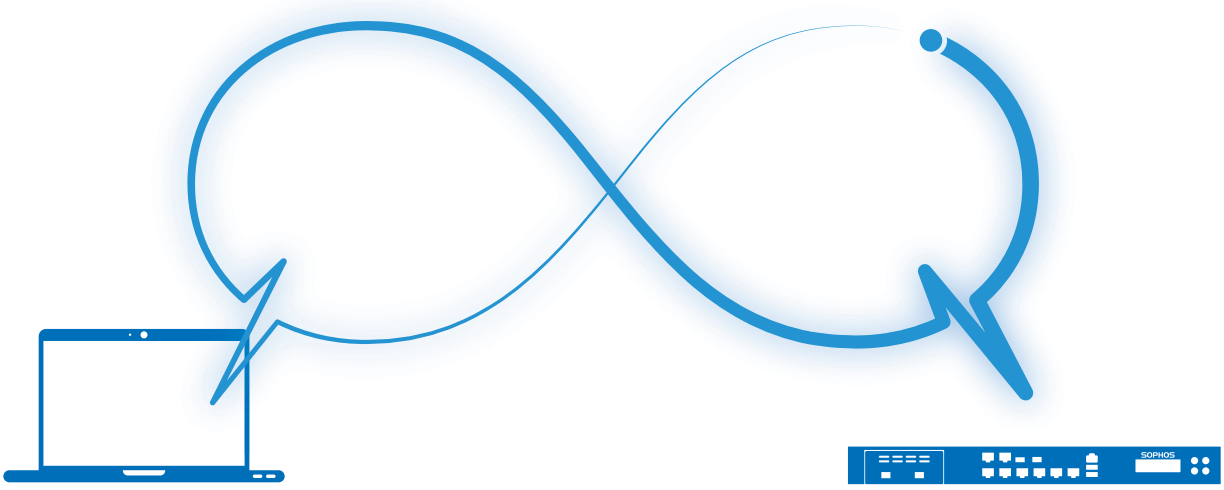
SOPHOS

Security made simple.



Seguridad sincronizada: una revolución en la protección

Sección 1: el mundo actual del ciberriesgo

Aumento del número, la complejidad y la sofisticación de los ataques

Las empresas de hoy en día, desde las más grandes a las más pequeñas, deben convivir y aprender a prosperar en un mundo en el que el ciberriesgo está más presente que nunca. El nivel de riesgo cada vez es mayor por múltiples razones, entre ellas el crecimiento de la superficie expuesta a ataques y el aumento de la complejidad y la sofisticación de los mismos.

Por un lado, los dispositivos móviles y los servicios en la nube son utilizados cada vez más por los empleados y, por el otro, las organizaciones de todos los tamaños despliegan infraestructuras virtuales y en la nube. Esto ha hecho crecer de forma espectacular lo que se denomina la "superficie expuesta a ataques".

Basta ver los datos siguientes:

- **Dispositivos:** El usuario medio del Reino Unido tiene conectados 3,1 dispositivos.[1]
- **Apps:** Las empresas con 250-999 empleados utilizan 16 aplicaciones en la nube aprobadas, mientras que las empresas con 1000-4000 empleados usan 14; las empresas más grandes usan una media de 11.[2]
- **Nube:** Las estimaciones de la industria calculan que la facturación de las infraestructuras como servicio (IaaS) superará los 16.000 millones de dólares en el 2015. [3]
- **Internet de las cosas:** A finales del 2015, se estima que 4900 millones de "cosas" estarán conectadas a Internet. En el 2020, esa cifra alcanzará los 25 mil millones. [4]

Con este aumento de los vectores de ataque, hemos podido ver cómo ha crecido el número de ataques y filtraciones que han tenido éxito, con el consiguiente aumento de fugas de datos.

A medida que aumenta la sofisticación de los ataques, los toolkits con apoyo comercial disponibles en los mercados gris y negro han hecho posible llevar a cabo tales ataques con menos experiencia que nunca.

Estos "kits" se han probado ampliamente y no siempre son fáciles de detectar o derrotar. Por ejemplo, el kit de herramienta de acceso remoto (RAT) UnRecom, denunciado por primera vez por Threatgeek.com en mayor del 2014, ha pasado por varias iteraciones incluyendo AlienSpy y, más recientemente, JSOCKET. Este kit ha estado implicado en incidentes de todo tipo, desde fugas de datos hasta desempeñar un papel en un asesinato político. [5]

Panorama de amenazas

Por desgracia, las investigaciones indican que las pymes son víctimas del creciente número de casos confirmados de filtraciones de datos de forma desproporcionada. Según el informe de las investigaciones sobre la filtración de datos de Verizon en el 2016:

- En el 2015 se produjeron 100.000 incidentes de seguridad, de los cuales 3141 fueron casos confirmados de filtraciones de datos.
- Estas cifras representan un aumento del 23 % en los incidentes de seguridad y un vertiginoso incremento del 48 % en las filtraciones de datos en comparación con el 2014.
- Las organizaciones con menos de 1000 empleados representaron el 20 % de los casos de filtraciones de datos confirmados y clasificados, a pesar de representar menos del 1 % de los incidentes.
- Los incidentes y las fugas de datos en empresas pequeñas afectan a diversos sectores, pero el mayor número de ataques tiene lugar en los sectores de servicios financieros, alojamiento, comercio minorista y salud.

Asimismo, Privacy Rights Clearinghouse estima que el 51 % de las filtraciones de datos de 2014 se debieron a la piratería o al malware, mientras que el informe de Verizon llega a la conclusión de que la principal motivación detrás de los autores de estos ataques es el dinero. Para las pymes que corren mayor riesgo, el coste puede ser catastrófico.

Un aumento de los ataques, cada vez más complejos, y un incremento de las pérdidas. Tenemos que plantearnos: ¿qué tenemos que hacer de forma distinta?

Equipos pequeños, recursos escasos, mercado laboral limitado

Uno podría pensar que la reacción lógica ante el aumento de ataques debería ser dedicar más efectivos al problema: contratar personal y mejorar la seguridad. Sin embargo, muchas empresas cuentan con equipos de seguridad informática pequeños. Ampliar o redistribuir los recursos no es una opción realista para las organizaciones pequeñas o medianas.

Como puede verse en la Figura 1, antes de llegar al entorno de las grandes empresas, los equipos especializados en seguridad informática son muy limitados en lo que se refiere al tamaño y los recursos:

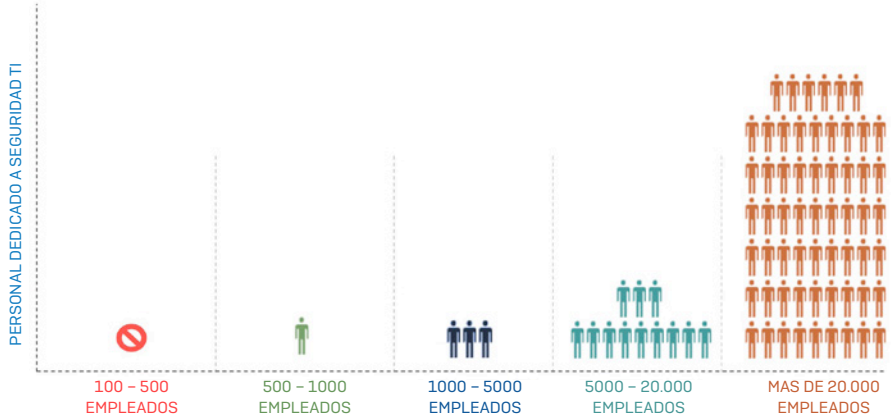


Figura 1: Poco personal y recursos limitados en la seguridad informática de pymes (Fuente: Departamento de Seguridad Nacional de los EE. UU., 2014)

Aunque la dirección desee ampliar su equipo de seguridad, esta tiene que lidiar con otro obstáculo: un mercado laboral extremadamente competitivo. Según el informe sobre empleo de ciberseguridad de BurningGlass del 2015, los puestos en ciberseguridad crecieron en un 91 % entre el 2010 y el 2014, un 325 % más rápido que el resto de empleos en el sector informático, y "en los EE. UU., las empresas publicaron 49.493 empleos que requerían la certificación CISSP en un mercado que a nivel nacional solo cuenta con 65.362 profesionales con esa certificación".

Nos enfrentamos a un número mucho mayor de ataques más sofisticados (y eficaces) que nunca y, además, no hay suficiente personal cualificado. Las empresas se hallan en una situación de riesgo que ha adquirido proporciones inaceptables.

Sección 2: pero, ¿qué hay de todo lo que hemos invertido?

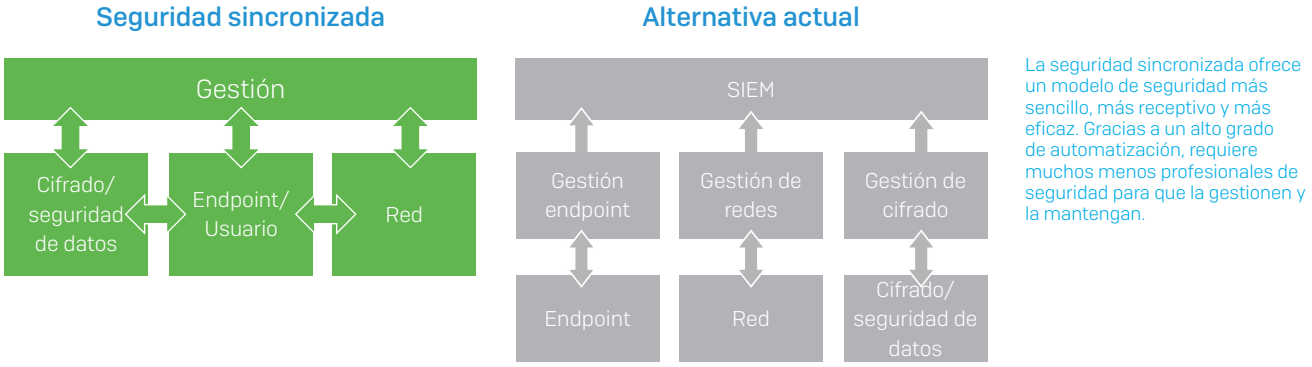
Fragmentadas y mal integradas. Complejas y miopes. Desconectadas del contexto inmediato. Decisiones aisladas. Todos estos calificativos pueden aplicarse a nuestras inversiones actuales en seguridad.

Seguimos inmersos en un mundo de productos independientes y complejos, desde los antivirus, el cifrado de datos y las puertas de enlace de red, web y correo a productos más modernos como suites, UTM, espacios seguros, protección endpoint y soluciones de respuesta ante amenazas. Los atacantes se sirven de ataques coordinados contra el conjunto de nuestro ecosistema informático. No es de extrañar que nos cueste seguir el ritmo. Un ataque puede comenzar en un endpoint, pero es increíble lo rápido que puede propagarse por toda la red, robando información no cifrada sirviéndose de nuestra conexión saliente de Internet.

Los profesionales de seguridad informática han intentado "unir los puntos" entre las fuentes de datos empleando motores de correlación, centros de macrodatos, sistemas de gestión de información y eventos de seguridad (SIEM), planes emergentes para compartir información como STIX y OpenIOC y un gran número de analistas humanos. Sin embargo, incluso con las herramientas más avanzadas, resulta muy difícil comprender los datos de una variedad de productos independientes para detectar y remediar rápidamente el riesgo y detener la fuga de datos.

La correlación entre los eventos y los registros sigue dependiendo de la creación y el mantenimiento de reglas de correlación complejas, la asignación de campos y la definición de filtros, así como horas de esfuerzo de analistas altamente capacitados difíciles de encontrar. SIEM requiere unas inversiones considerables en capital y gastos operativos permanentes. En lo que se refiere a compartir información, aunque ciertamente sea clave para el futuro de la seguridad, todavía no ha madurado lo suficiente como para que se pueda adoptar ya de forma generalizada y sencilla.

Los resultados, o más bien su ausencia, hablan por sí solos. Como hemos visto, las filtraciones de datos y el riesgo siguen creciendo sin ningún indicio de que vayan a reducirse. El personal se ha reducido al máximo. Según un informe reciente de Ponemon Institute, el 74 % de las filtraciones no se descubren hasta seis meses más tarde. Y lo que es peor, parece que a las empresas del mercado medio les cuesta aún más mitigar los riesgos que a las empresas más grandes con mejores recursos. Indudablemente, la respuesta no es otro producto independiente no integrado ni más consolas, más personal o SIEM complejos. Estos enfoques no están dando resultados. Debemos encontrar un enfoque mejor y más eficaz.



La seguridad sincronizada ofrece un modelo de seguridad más sencillo, más receptivo y más eficaz. Gracias a un alto grado de automatización, requiere muchos menos profesionales de seguridad para que la gestionen y la mantengan.

Sección 3: la seguridad sincronizada, un nuevo enfoque

Una nueva idea revolucionaria

Durante décadas, la industria de la seguridad ha tratado la seguridad de las redes, la seguridad endpoint y la seguridad de los datos como entidades completamente distintas. Es como poner tres guardias de seguridad en el edificio – uno en la puerta de entrada, otro en el interior y otro custodiando la caja fuerte –, pero sin dejar que hablen entre ellos. La seguridad sincronizada entrega a cada uno de esos guardias de seguridad un teléfono inteligente para que puedan coordinarse y comunicarse entre sí de forma rápida y eficaz. Es un concepto sencillo a la vez que revolucionario.

¿Y si volviéramos a empezar planteando la seguridad informática con un enfoque totalmente nuevo? Un enfoque más eficaz, que proporcionase una protección optimizada y permitiese una comunicación automatizada y en tiempo real entre las soluciones de cifrado, de protección para redes y de seguridad endpoint. Uno que se sincronizara en toda la superficie expuesta a ataques. Uno que estuviese sumamente automatizado, con el que no fuera necesario más personal ni aumentar la carga de trabajo.

Para ello necesitamos un sistema:

Centrado en el ecosistema. Debemos prevenir, encontrar y detener las filtraciones en todo el ecosistema informático siendo totalmente conscientes de los objetos y eventos próximos.

Integral. La solución debe ser integral y comprender todo el "sistema" informático, múltiples plataformas, dispositivos, usuarios y datos, para poder proporcionar protección contra los ataques coordinados.

Eficiente. La solución debe reducir la carga de trabajo del equipo al tiempo que mejora la protección. No puede añadir carga de trabajo adicional al personal sobrecargado.

Eficaz. La solución debe prevenir, detectar, investigar y remediar de forma eficaz las amenazas actuales en toda la superficie expuesta.

Basado en los datos. La solución no se centra solamente en los dispositivos y las redes, sino que también protege la información valiosa dondequiera que esté, siempre que se acceda a ella.

Sencillo. Fácil de comprar, fácil de comprender, fácil de desplegar y fácil de usar.

Una lista que ciertamente parece exigente. Los productos de seguridad TI actuales son justamente lo contrario: productos independientes centrados en la amenaza, complejos, acaparadores de recursos y mucho menos coordinados que los ataques de los que deben defendernos. Está claro que para obtener resultados es necesario innovar. Este reto se resume en la figura 2.

Soluciones de seguridad de varios niveles de hoy en día	Seguridad sincronizada
Centradas en la amenaza, operan sin tener en cuenta los objetos o los eventos próximos	Centradas en el ecosistema, operan plenamente conscientes de los objetos y los eventos próximos
Productos independientes especializados	Productos coordinados
Necesitan más personal para ser eficaces	Son eficaces gracias a la automatización y la innovación; no requieren más personal
Gestión de cifrado independiente	Protección de cifrado integrada que responde ante las amenazas de forma automática
Complejas	Sencillas

Figura 2: Las soluciones actuales deben cambiar drásticamente

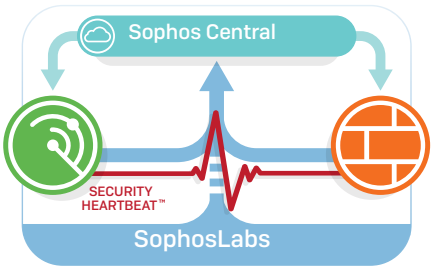
Proporcionar esta sencillez y eficacia en el entorno actual requiere una innovación tecnológica considerable. Nosotros la llamamos Sophos Security Heartbeat.

Sophos Security Heartbeat

La seguridad sincronizada permite a las soluciones next-gen endpoint, cifrado y redes compartir de forma continua información importante sobre los comportamientos sospechosos y maliciosos en todo el ecosistema informático de una empresa. Mediante una conexión directa y segura denominada Sophos Security Heartbeat, la protección endpoint, cifrado y redes actúa como un solo sistema integrado, permitiendo a las organizaciones prevenir, detectar, investigar y remediar las amenazas prácticamente en tiempo real sin requerir personal adicional.

Por ejemplo, cuando el firewall de última generación de Sophos detecta una amenaza avanzada o un intento de fuga de datos confidenciales, puede utilizar de forma automática Sophos Security Heartbeat para tomar una serie de medidas en la red y en el endpoint para mitigar el riesgo y detener la fuga de datos al instante. De forma similar, si se detecta que un endpoint protegido corre peligro, la seguridad sincronizada permite el aislamiento automatizado y prácticamente instantáneo del mismo, incluida la revocación temporal de las claves de cifrado, evitando la fuga de información confidencial o el envío de datos delicados a un servidor de comando y control. Este tipo de descubrimiento, protección y respuesta a incidentes, que normalmente podría tardar semanas o meses, se ha reducido a segundos gracias a la seguridad sincronizada.

La seguridad sincronizada de Sophos utiliza Security Heartbeat, Sophos Labs y Sophos Central para ofrecer una seguridad sencilla y sumamente eficaz en endpoint y redes.



Por primera vez, también vemos cómo el cifrado tiene un papel significativo en la protección contra amenazas. Ahora, el cifrado, las claves de cifrado y la capacidad de compartir y descifrar archivos están directamente ligados al estado de seguridad y a la confianza y la integridad del usuario, los sistemas y las aplicaciones. Debido a ello, pueden evaluarse los riesgos y tomarse medidas que impongan políticas de cifrado, impidiendo así que las personas malintencionadas obtengan información protegida. Y aunque los atacantes acaben robando esos archivos cifrados, no los podrán leer. Asimismo, a los dispositivos móviles que no cumplan con la política se les puede prohibir el acceso a aplicaciones y datos protegidos. Esta combinación de proteger a usuarios, redes, dispositivos y datos de forma integrada y sincronizada es única, potente y sencilla.

Resumen

Los ciberriesgos nos rodean. El aumento de los ataques y su complejidad y el hecho de no haber suficiente personal para hacerles frente crean una tormenta perfecta de desafíos de seguridad informática, sobre todo para las pequeñas y medianas empresas.

Los enfoques multinivel actuales de la seguridad TI no están dando resultado y los esfuerzos por solventar sus carencias mediante el análisis también se están quedando cortos.

Los métodos actuales de soluciones complejas, centradas en la amenaza, miopes y que dependen del número de empleados no satisfarán las necesidades de los equipos de seguridad TI con recursos limitados. Para invertir la curva creciente de incidentes y filtraciones debemos aplicar un enfoque muy distinto al utilizado hasta ahora.

Debemos implantar soluciones nuevas que sean sencillas a la vez que eficaces, automatizadas y coordinadas. En resumen, sincronizar la seguridad mediante innovaciones tecnológicas como Sophos Security Heartbeat. Al sincronizar la protección de datos, puestos y redes, los equipos e infraestructuras de seguridad están equipados para reaccionar y responder ante las amenazas actuales de forma rápida y eficaz. Para saber más sobre Sophos Security Heartbeat y ver cómo la seguridad sincronizada de Sophos puede proteger mejor su organización en el entorno de alto riesgo de hoy en día, visite es.sophos.com/heartbeat.

[1] Statistica.com

[2] Okta Business@work, 2015

[3] Gartner, http://www.gartner.com/newsroom/id/3055225

[4] Gartner, http://www.gartner.com/newsroom/id/2905717, 2014

[5] Threatgeek.com

Seguridad Sincronizada

Más información en **es.sophos.com/heartbeat**

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

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

05/09/2016 WP-ES (NP)

SOPHOS