SOPHOS
Security made simple.

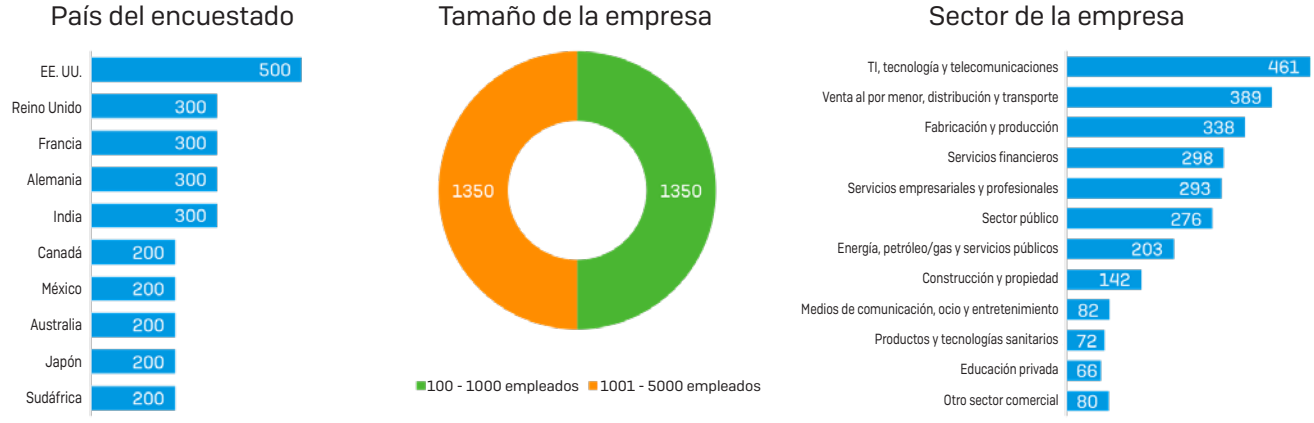
Estado actual de la seguridad para endpoints

Estudio independiente de 2700 medianas empresas en cinco continentes

Introducción

A finales de 2017, Sophos patrocinó un estudio de investigación global independiente para conocer más a fondo el estado de la seguridad para endpoints en medianas empresas de todo el mundo. Este amplio programa de investigación explora áreas clave de interés y desarrollo: las brechas de seguridad, el uso de la tecnología, las actitudes ante amenazas y futuros planes de inversión.

El estudio, realizado por la firma líder de investigación británica Vanson Bourne, preguntó a 2700 directores de TI de empresas de 100 a 5000 usuarios en 10 países de cinco continentes.



Datos demográficos del estudio: número de encuestados por país, tamaño de la empresa y sector empresarial

Este documento resultante ofrece datos muy significativos sobre los problemas de ciberseguridad corrientes a los que se enfrentan las empresas hoy día: incluye las experiencias y los planes futuros, desde el ransomware y los exploits hasta el Machine Learning, de los directores de TI de todo el planeta. Es una lectura esclarecedora sobre el punto en que se encuentra el sector en cuanto a estos problemas.

La sombra del ransomware

Resumen ejecutivo

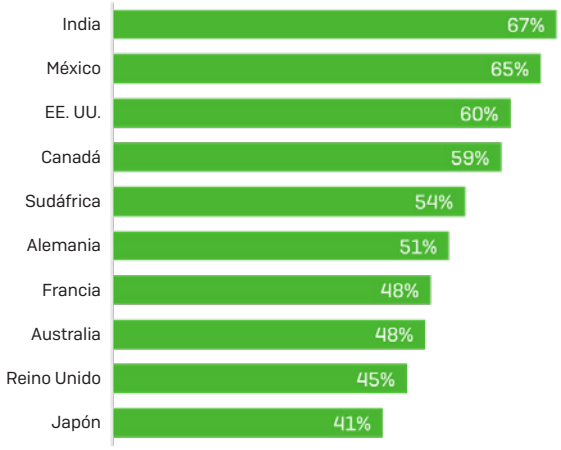
- El 54 % de las empresas se vieron afectadas por el ransomware en el último año.
- Dos ataques de ransomware por empresa de promedio.
- Media del impacto por empresa afectada ≈ 133 000 USD (100 000 GBP).
- El sector sanitario fue el principal objetivo, seguido por el energético, los servicios profesionales y la venta al por menor.
- La India es el país que sufrió más infecciones, seguida de México, EE. UU. y Canadá.
- El 77 % de las empresas contaban con una solución de seguridad para endpoints actualizada en el momento del ataque.
- El 54 % de las empresas no disponen de una protección antiransomware específica.

Los ataques de ransomware son recurrentes

El ransomware sigue siendo un gran problema en todo el mundo: más del 54 % de las empresas encuestadas sufrieron ataques en el último año, y se espera que un 31 % más sean víctimas en el futuro. Desafortunadamente, los ataques de ransomware pueden repetirse, ya que las empresas afectadas sufrieron una media de dos en los 12 meses anteriores.

Si bien el ransomware logró paralizar empresas en todos los países de la encuesta, el alcance de los ataques varía notablemente en todo el grupo de estudio. La India está a la cabeza de las víctimas del ransomware; en este país, dos tercios de los encuestados (67 %) se vieron afectados por el ransomware durante el año previo. En el otro extremo, encontramos a Japón, donde cuatro de cada diez (41 %) sufrieron un ataque. Es probable que el idioma tenga un papel importante en este sentido, puesto que los ataques de ransomware suelen comenzar con un correo electrónico de phishing. Un mismo correo en inglés puede utilizarse en al menos seis de los países estudiados, mientras que un correo en japonés solo puede emplearse en un área geográfica. En este caso, la complejidad del idioma sirve a los japoneses como protección adicional.

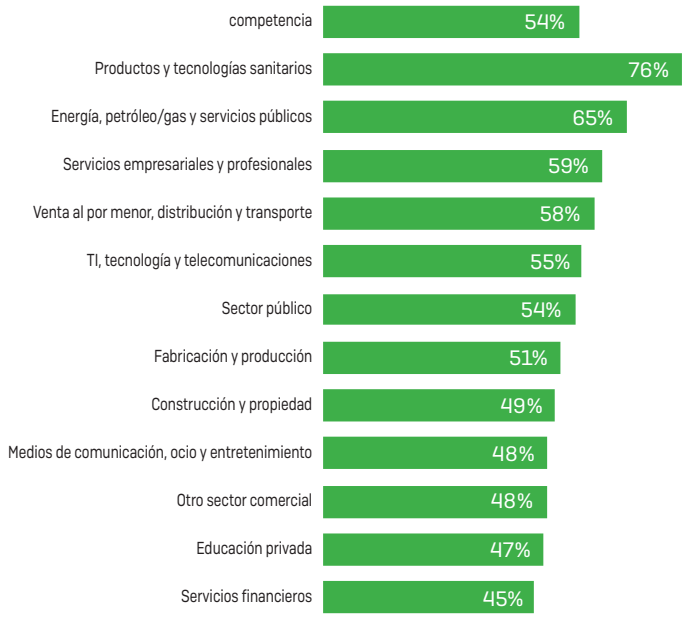
Afectados por el ransomware, por país



% de empresas afectadas por el ransomware en los 12 meses anteriores

La propensión a sufrir un ataque de ransomware varía enormemente de un sector industrial a otro. El sector sanitario destaca con un 76 % de encuestados que afirman haber sido víctimas en el último año. En el extremo opuesto, los servicios financieros es el sector con menos probabilidades de haber sufrido un ataque, aunque incluso este sector sufre el problema con un 45 % de encuestados afectados.

Afectados por el ransomware, por sector



% de empresas que se habían visto afectadas por el ransomware en los 12 meses anteriores, por sector

Aunque tanto el sector sanitario como los servicios financieros gestionan datos de gran valor, el sector sanitario suele considerarse un blanco fácil, por lo que recibe ataques con más frecuencia. Y hay motivos para ello, puesto que el sector sanitario suele tener una infraestructura de TI más anticuada con agujeros de seguridad, además de unos recursos limitados para mejorar la seguridad informática. También se considera que las organizaciones de este sector son más proclives a pagar un rescate.

Resulta interesante que los hackers no hacen distinciones por tamaño de empresa. Las probabilidades de sufrir un ataque son prácticamente las mismas para las empresas grandes y pequeñas que han participado en el estudio: el 50 % de las empresas de 100-1000 usuarios han sido víctimas, frente al 58 % en la categoría de 1001-5000 usuarios. Todas las empresas, grandes y pequeñas, se ven afectadas.

La protección tradicional para endpoints no es suficiente por sí sola

Más de tres cuartos (77 %) de las víctimas del ransomware ya ejecutaban soluciones de seguridad para endpoints actualizadas, así que se están dando cuenta por las malas de que detener el ransomware requiere una protección especializada.

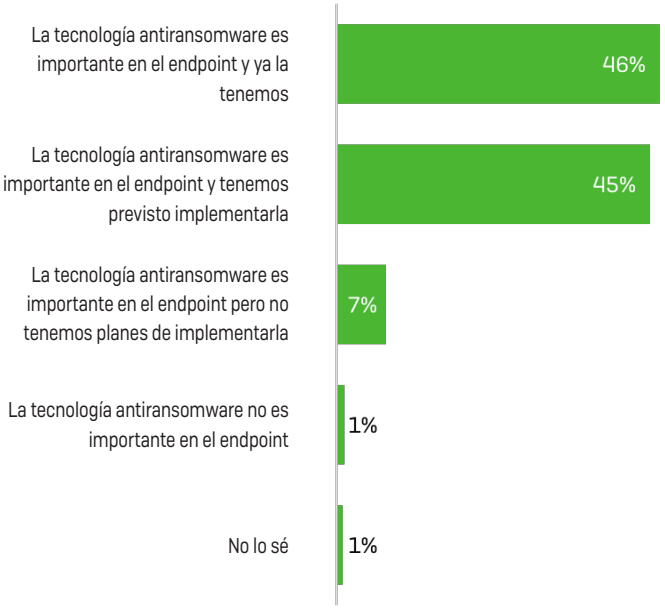
Porcentaje de empresas afectadas por el ransomware en los 12 meses anteriores que contaban con una protección para endpoints actualizada en el momento del ataque

Estado de la protección para endpoints	Total
Contamos con una protección para endpoints actualizada	77%
No contamos con una protección para endpoints actualizada	21%
No lo sé	1%

Base de 1468

Después de los sonados ataques de ransomware WannaCry y Petya de 2017 y la notoriedad de las víctimas, no sorprende que casi todos los encuestados (98 %) afirme que es importante disponer de una tecnología antiransomware en el endpoint. Sin embargo, más del 50 % de las empresas no han implantado ninguna tecnología antiransomware, con lo que tienen más riesgo de ser atacadas.

Opiniones de los encuestados sobre la incorporación de tecnología antiransomware específica a la protección para endpoints de su empresa



El nivel de inversión en la protección contra el ransomware varía notablemente de un sector a otro. Los sectores de la energía, el petróleo/gas, los servicios públicos y la sanidad son los que más han invertido en la tecnología antiransomware. Se consideran objetivos de alto valor para los delincuentes, y operan con un equipamiento muy caro y fabricado a medida con tecnología anticuada, como escáneres de IRM en el sector sanitario o perforadoras en el sector del petróleo.

En cambio, los medios de comunicación, el sector público y la educación privada son los que menos probabilidades tienen de haber invertido en tecnología antiransomware. Los motivos de ello son varios, pero a menudo se debe a limitaciones presupuestarias (el sector público se ve especialmente afectado en este sentido) o a la falta de concienciación. Unos recursos de TI limitados también pueden dejar atrás a estas empresas a la hora de incorporar protección antiransomware.

Opiniones de los encuestados sobre la incorporación de tecnología antiransomware específica a la protección para endpoints de su empresa por sector

	Promedio	Servicios empresariales y profesionales	Construcción y propiedad	Energía, petróleo/gas, servicios públicos	Servicios financieros	Salud	TI, tecnología, telecomunicaciones	Fabricación	Medios de comunicación, ocio, entretenimiento	Sector público	Educación privada	Venta al por menor, distribución, transporte	Otros
La tecnología antiransomware es importante en el endpoint y ya la tenemos	**46%**	47%	46%	53%	52%	53%	44%	46%	38%	39%	35%	46%	51%
La tecnología antiransomware es importante en el endpoint y tenemos previsto implementarla	**45%**	42%	46%	42%	41%	42%	47%	46%	51%	50%	45%	43%	36%

El misterio del sector sanitario: la mayor víctima y el mayor inversor en prevención

El sector sanitario constituye un caso interesante. Estas empresas son las que más probabilidades tienen de sufrir un ataque (76 %) y, sin embargo, también son las que más invierten en protección antiransomware (un 53 % junto a los sectores energético, del petróleo/gas y los servicios públicos).

¿Cómo se interpreta esta dicotomía? En parte, se debe a que los delincuentes siguen viendo el sector sanitario como un blanco fácil, de modo que se produce un número desproporcionado de ataques contra él. Asimismo, la tecnología más anticuada de la que se sirve este sector (como las máquinas de IRM anteriormente mencionadas) solo funciona con sistemas operativos antiguos.

El sector sanitario también debe enfrentarse a menudo al reto de unos recursos restringidos o ilimitados en esta área. La falta de personal, hardware y software tiene como resultado una seguridad poco uniforme, de modo que una parte de la organización puede contar con la protección antiransomware necesaria, mientras que otras no. El malware puede infiltrarse.

Y también está la cuestión de la calidad. No todas las soluciones de protección antiransomware son iguales. Algunas opciones simplemente no son tan efectivas a la hora de detener un ataque.

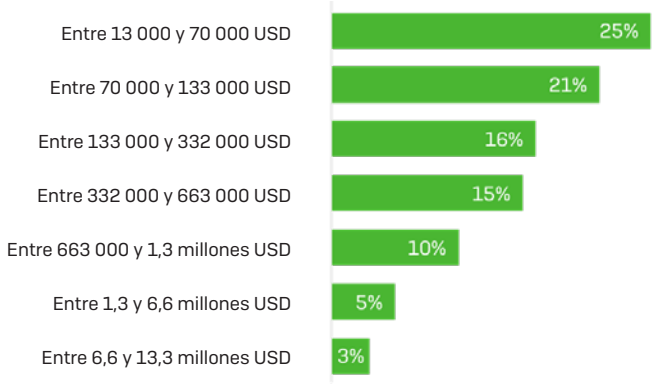
Por suerte, las organizaciones del sector sanitario están aprendiendo de la experiencia y han optado por invertir en tecnología antiransomware después de observar el daño causado por las brechas de seguridad anteriores.

El alto coste de un ataque de ransomware

El coste de un ataque de ransomware va mucho más allá del rescate pagado. La encuesta reveló que el impacto financiero total de un ataque de ransomware (incluido el tiempo de inactividad, las horas de trabajo, el coste de dispositivos, el coste de redes, las oportunidades perdidas y el pago del rescate) es invariablemente de muchos miles de dólares, euros, yenes, libras, pesos, rands o rupias.

El coste promedio de un ataque de ransomware es de casi 133 000 USD (100 000 GBP), dividido a partes casi iguales entre las empresas que afirmaron que el coste fue superior a esta cifra (51 %) y las que afirmaron que fue inferior (49 %). El coste más habitual para las empresas fue de entre 13 000 y 70 000 USD, pero casi la mitad de los encuestados (46 %) incurrieron en costes de entre 13 000 y 133 000 USD.

Coste aproximado para la empresa de los encuestados de rectificar los perjuicios del ataque de ransomware más reciente (teniendo en cuenta el tiempo de inactividad, el tiempo de las personas, el coste de dispositivos, el coste de redes, las oportunidades perdidas, el rescate pagado, etc.)



La encuesta también reveló que el **ransomware cuesta a las empresas de EE. UU. más que el PIB de Jamaica.** Según los resultados de la encuesta, calculamos que el ransomware costó a las empresas de EE. UU. de 100 personas o más 18,6 mil millones de USD en el último año, mientras que el PIB de Jamaica fue de 14 mil millones en 2016.

La perspectiva de Sophos

A pesar de haberse producido una serie de ataques de ransomware de gran repercusión en 2017, las empresas están empezando 2018 con una protección contra el ransomware inadecuada. Mientras tanto, quienes estén implementando tecnología antiransomware deberán asegurarse de que la opción que eligieron incluye funciones antiransomware específicas en lugar de una protección contra amenazas genérica.

Sophos cree que ha llegado el momento de realizar más pruebas independientes por parte de terceros sobre la eficacia de los productos antiransomware y su capacidad de detener amenazas previamente desconocidas, para que las empresas y los profesionales informáticos puedan tomar decisiones informadas.

Por último, esperamos ver incluso más ataques de ransomware en 2018, impulsados por el ransomware como servicio (RaaS) y amplificados por el resurgimiento de los gusanos. Ahora no es el momento de posponer la actualización de su tecnología. Añada una protección antiransomware especializada antes de que sea demasiado tarde.

Recomendaciones de Sophos

Su empresa es un objetivo en cualquier caso, así que debe prepararse. El ransomware ha atacado a todo tipo de empresas, ya sean grandes, medianas o pequeñas.

Empiece por los conocimientos. Asegúrese de concienciarse usted y a sus usuarios finales. Forme a sus empleados mediante simulaciones de ataques para que sean capaces de identificar uno cuando lo vean. Los usuarios finales (y los errores humanos) son a menudo el eslabón más débil en un sistema de seguridad, pero unos usuarios bien formados pueden convertirse en su mejor arma.

Estudie las tecnologías avanzadas para saber cuáles son sus opciones. Los productos antivirus o de seguridad para endpoints tradicionales solo bloquearán el ransomware conocido y, con la velocidad a la que se desarrolla y distribuye nuevo malware, necesita una verdadera protección antiransomware para bloquear los ataques de día cero.

Actualice su tecnología. Las opciones disponibles han mejorado notablemente en los últimos años a la hora de detener el ransomware e impedir el uso de exploits. Y recuerde que el coste de invertir en tecnología de defensa no es nada en comparación con el impacto de un ataque. Al protegerse, ahorrará dinero y salvará su reputación.

Detener exploits

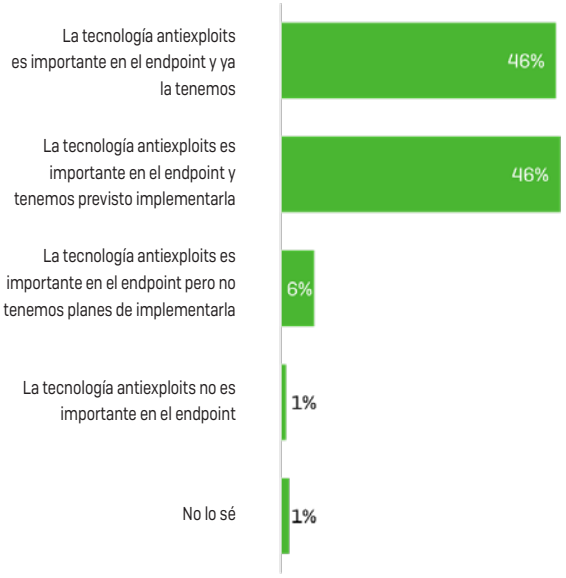
Resumen ejecutivo

- El 54 % de las empresas no cuentan con tecnología antiexploits.
- 2/3 de los directores de TI no entienden lo que es la tecnología antiexploits.
- EE. UU. es el país que mejor conoce la tecnología antiexploits, seguido de México.

Detener el exploit es detener el ataque

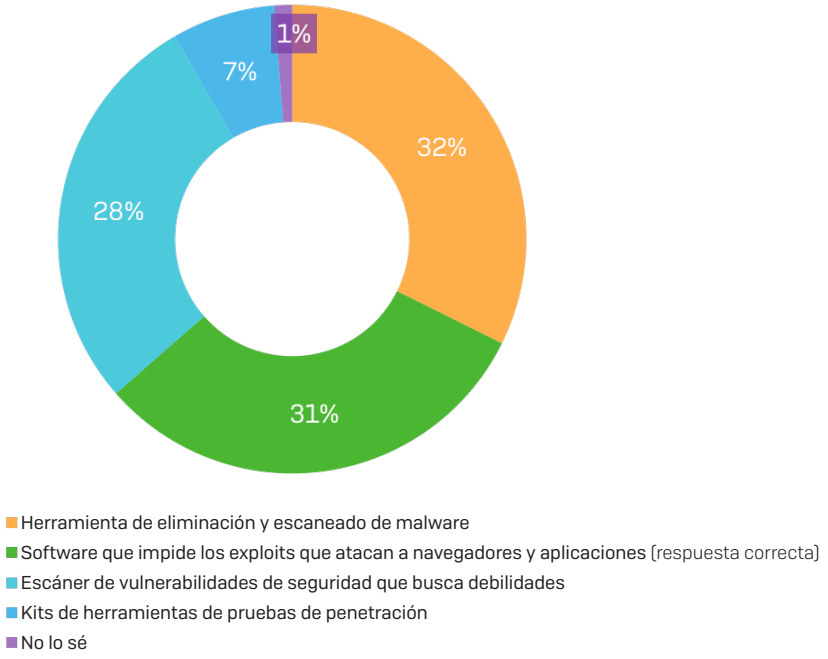
Los exploits, las técnicas que utilizan los hackers para aprovechar las vulnerabilidades del software legítimo, se han desplegado en numerosos ataques de gran repercusión. El uso del exploit Eternal Blue en el ataque de ransomware WannaCry generó titulares en todo el mundo. A la luz de esta cobertura mediática, no resulta sorprendente que casi todos los encuestados (98 %) están de acuerdo en que es importante tener tecnología antiexploits en el endpoint. Sin embargo, más de la mitad de las empresas del estudio (54 %) dicen que no cuentan con ninguna tecnología antiexploits en el endpoint, con lo que son vulnerables a ataques.

Opiniones de los encuestados sobre la incorporación de tecnología antiexploits específica a la protección para endpoints de su empresa



Aunque el 46 % de las empresas afirman que cuentan con tecnología antiexploits, menos de un tercio de los encuestados (31 %) pudieron identificar correctamente la definición del software antiexploits. Esto sugiere que una parte importante de las empresas creen equivocadamente que están protegidas contra esta técnica de ataque común, cuando en realidad están corriendo un riesgo considerable.

Cuál es la mejor descripción para el software antiexploits



El nivel de conocimiento varía de un país a otro, con EE. UU. a la cabeza de la lista con un 39 % de encuestados que la definen correctamente, frente a solo el 22 % en Francia. Puede resultar sorprendente que las empresas más pequeñas hayan demostrado un mejor conocimiento de la tecnología antiexploits que las de mayor tamaño: el 34 % de las empresas en la categoría de 100-1000 usuarios lograron definirla correctamente, frente al 29 % en el grupo de 1001-5000 usuarios.

Software antiexploits correctamente definido

Reino Unido	Francia	Alemania	EE. UU.	Canadá	México	India	Australia	Japón	Sudáfrica
35%	22%	32%	39%	26%	35%	28%	34%	26%	30%

% de encuestados que identificaron correctamente la definición del software antiexploits por país

Recomendaciones de Sophos

Dado el uso extendido de exploits en los ataques de hoy día y la notable falta de tecnología antiexploits en todos los frentes, se necesitan acciones urgentes para entender cómo detener estos ataques. Si no entiende los exploits, es momento de aprender. Si cree que entiende los exploits, vale la pena refrescar la memoria para asegurarse de que conoce los enfoques más recientes.

Ha llegado el momento de actualizar su tecnología. Para protegerse contra las técnicas de explotación utilizadas en los ataques de malware, asegúrese de tener implementadas las soluciones de seguridad adecuadas para detenerlos.

Amenazas avanzadas y Machine Learning

Resumen ejecutivo

- El 87 % está de acuerdo en que las amenazas se han vuelto más complejas en el último año.
- El 60 % afirma que sus actuales ciberdefensas no son suficiente.
- El 60 % tiene previsto implementar tecnología predictiva contra amenazas como Machine Learning o Deep Learning en el próximo año.
- Canadá, la India y México tienen los niveles más altos de tecnología de Machine Learning.
- La India es el país más optimista en cuanto al potencial del Machine Learning.

No está solo

La encuesta confirmó que gestionar los ataques de malware sofisticados de hoy día es un desafío cada vez mayor para casi todos los directores de TI de todo el planeta:

- El 83 % está de acuerdo en que detener las amenazas de malware se ha vuelto más difícil en el último año.
- El 87 % está de acuerdo en que las amenazas de malware se han vuelto más complejas en el último año.

Si bien todas las regiones del estudio comparten mayoritariamente estas opiniones, los directores de TI de Japón son los que más notan el cambio: el 92 % afirma que se ha vuelto más difícil detener las amenazas, mientras que el 97 % está de acuerdo en que se han vuelto más complejas.

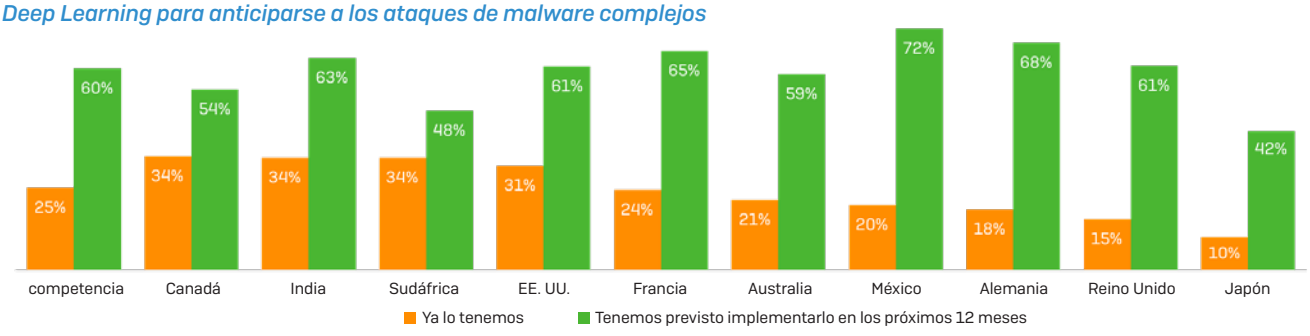
	De acuerdo en que detener las amenazas se ha vuelto más difícil en el último año	De acuerdo en que las amenazas de malware se han vuelto más complejas en el último año
Reino Unido	85%	89%
Francia	74%	79%
Alemania	77%	87%
EE. UU.	88%	90%
Canadá	76%	82%
México	81%	86%
India	89%	88%
Australia	85%	84%
Japón	92%	97%
Sudáfrica	85%	89%

A menudo, las tecnologías para endpoints tradicionales no consiguen seguir el ritmo a los ataques avanzados y complejos de la actualidad. El 60 % de los encuestados admitió que sus defensas para endpoints actuales no son totalmente suficientes para bloquear los ataques que han visto en el último año. Aunque las respuestas fueron similares en todas las regiones y en empresas de todos los tamaños, la sanidad fue el sector con menor confianza en sus defensas para endpoints: el 72 % está de acuerdo en que no son completamente eficaces. Teniendo en cuenta la gran propensión de las empresas de sanidad a sufrir ataques de ransomware, no resulta sorprendente.

Por tanto, no es de extrañar que cada vez más empresas estén eligiendo tecnologías predictivas de prevención de amenazas, como el Deep Learning y el Machine Learning, para que les ayuden a anticiparse a estas amenazas de malware. El 85 % de las empresas ya tienen (25 %) o tienen previsto implementar una tecnología predictiva contra amenazas en el plazo de un año (60 %).

La encuesta reveló un cambio significativo en los planes para las tecnologías predictivas en todo el mundo. Canadá, la India y Sudáfrica están a la cabeza del grupo con un tercio (34 %) de encuestados que ya utilizan tecnologías predictivas contra amenazas como el Deep Learning y el Machine Learning. México es el país con más planes para estas tecnologías: el 72 % tiene previsto implementarlas durante el próximo año. Japón destaca como el país más prudente en cuanto al despliegue de tecnologías predictivas, con solo un 10 %, el valor más bajo de todas la regiones del estudio, que ya las utiliza y un 41 % que afirma que no tiene planes de implementarlas.

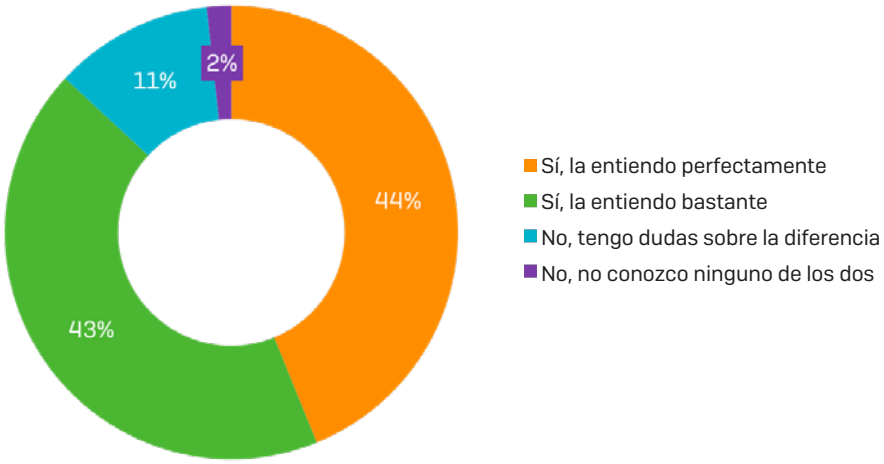
Opiniones de los encuestados sobre la incorporación de tecnologías predictivas contra amenazas como el Machine Learning y el Deep Learning para anticiparse a los ataques de malware complejos



Confusión en cuanto a la diferencia entre Machine Learning y Deep Learning

Aunque el Machine Learning es un concepto de moda, casi seis de cada diez encuestados (56 %) reconocen que no entienden del todo la diferencia entre Machine Learning y Deep Learning. Como resultado, no pueden evaluar exhaustivamente las opciones de seguridad que tienen a su disposición.

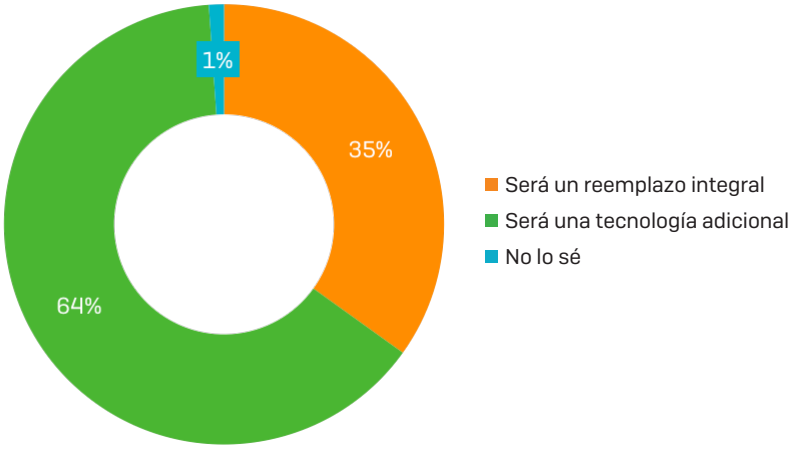
Pregunta: ¿Entiende la diferencia entre Machine Learning y Deep Learning?



El Machine Learning es el futuro

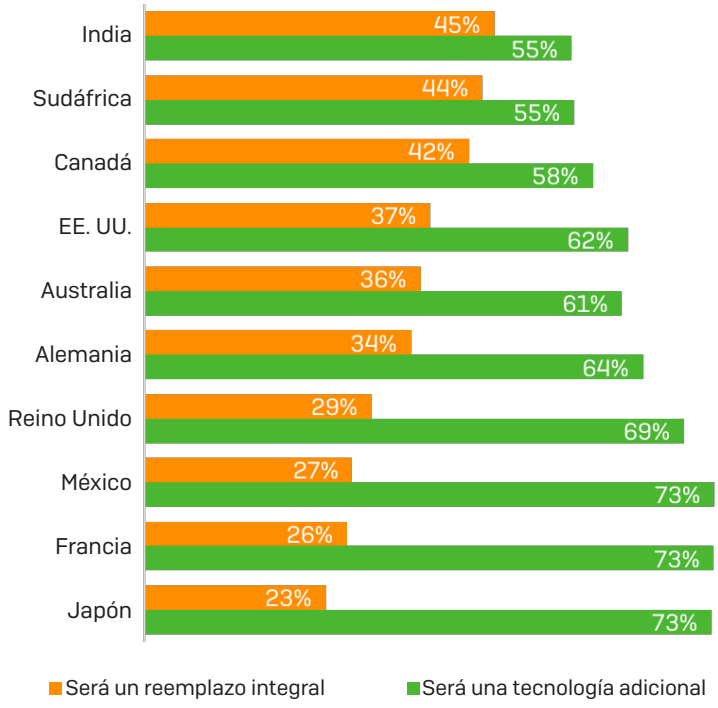
Tal como hemos visto, la gran mayoría de empresas encuestadas tienen o tienen previsto implementar tecnologías predictivas contras amenazas como el Machine Learning o el Deep Learning. No obstante, las opiniones son diversas en cuanto al lugar que corresponde a estos productos dentro de su infraestructura de seguridad. Casi dos tercios (64 %) de las empresas consideran el Machine Learning o el Deep Learning una tecnología adicional para sus endpoints, en comparación con el 35 % que lo ve como un reemplazo integral de una protección tradicional para endpoints.

Pregunta: ¿Su empresa considera el Machine Learning o el Deep Learning una tecnología de detección adicional para sus endpoints o un reemplazo integral para su antivirus?



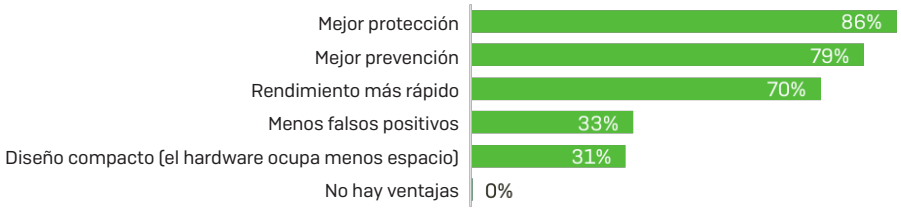
La organizaciones de la India son las que más confían en que será un reemplazo integral (45 %), mientras que, de nuevo, los encuestados japoneses son los que más prudentes se muestran con esta tecnología.

Pregunta: ¿Su empresa considera el Machine Learning o el Deep Learning una tecnología de detección adicional para sus endpoints o un reemplazo integral para su antivirus?



El principal beneficio que buscan las empresas en el Machine Learning y el Deep Learning es una mejor detección: una media del 86 % espera disfrutar de esta ventaja.

Pregunta: ¿Cuáles son las ventajas más importantes que busca su empresa en las tecnologías predictivas de prevención de amenazas que ofrecen el Machine Learning y el Deep Learning?



No obstante, también expresan cierta inquietud, ya que casi dos tercios (65 %) de los encuestados están muy preocupados o extremadamente preocupados por los falsos positivos con esta tecnología.

A pesar de esta prudencia, la actitud general hacia el Machine Learning es sumamente positiva: la mayoría (94 %) de los encuestados creen que el Machine Learning "estará a la altura de las expectativas", y más de dos de cada diez (21 %) incluso llegan a afirmar que solucionará todos sus problemas de tecnología.

	competencia	Reino Unido	Francia	Alemania	EE. UU.	Canadá	México	India	Australia	Japón	Sudáfrica
El Machine Learning estará a la altura de las expectativas	94%	90%	96%	94%	97%	97%	98%	99%	89%	79%	93%
El Machine Learning solucionará todos nuestros problemas tecnológicos	21%	13%	19%	10%	26%	20%	32%	45%	14%	9%	17%

Opinión de los encuestados sobre el Machine Learning

Si bien la mayoría de encuestados del estudio creen que el Machine Learning estará a la altura de las expectativas, tienen opiniones muy variadas sobre si será la panacea a nuestros problemas tecnológicos. Como se ha mencionado anteriormente, los directores de TI de la India son los más optimistas, con un 45 % que afirma que solucionará todos nuestros problemas de tecnología. En cambio, solo el 9 % de los encuestados japoneses y el 10 % de los alemanes comparten esta opinión.

La perspectiva de Sophos

El Machine Learning se está convirtiendo en una tecnología corriente. A pesar de ser relativamente nueva, la gran mayoría de empresas tienen planeado implementar el Machine Learning en los próximos 12 meses. Sin embargo, Sophos está de acuerdo con la mayoría de los encuestados del estudio: el Machine Learning es una capa adicional de seguridad, no un reemplazo total para toda la protección de endpoints.

Puesto que no se acaba de entender del todo la diferencia entre el Machine Learning y el Deep Learning, el sector de la seguridad necesita tomar las riendas para permitir a las empresas tomar decisiones fundamentadas sobre el Machine Learning y el Deep Learning. Esto implica pruebas públicas independientes de productos de seguridad y la disponibilidad de formación sobre estas tecnologías, cómo se utilizan y las diferencias entre ellas.

Recomendaciones de Sophos

Cada vez es más difícil defenderse contra el malware, y los cibercriminales ya están utilizando el Machine Learning en sus ataques. Debe asegurarse de que sus defensas siguen el ritmo a las amenazas con las que se enfrenta. Lo mejor es que todo el mundo adopte una protección con Machine Learning o Deep Learning lo antes posible.

Por otro lado, es necesario solventar la falta de conocimientos: los profesionales deben aprovechar las oportunidades formativas e investigar el Machine Learning y el Deep Learning para entender mejor las diferencias entre ellos y lo que significan estas diferencias en términos de seguridad. No todas las opciones de Machine Learning son iguales. Asegúrese de que cuenta con la protección adecuada para su empresa.

Conclusión

Esta encuesta ha revelado que la seguridad TI sigue siendo un área muy difícil para las empresas de todo el planeta, debido a la complejidad cada vez mayor de los ataques de malware y a los incentivos económicos para los atacantes.

Se está incrementando la brecha entre los conocimientos y las habilidades de los atacantes, en particular en las áreas del ransomware y los exploits, y aquellos de los profesionales de TI que deben detenerlos. Aunque esto supone una oportunidad para los cibercriminales, es posible corregirlo a través de la formación.

Tal como ha demostrado la encuesta, las soluciones de seguridad tradicionales ya no son suficientes para mantener a las empresas un paso por delante de los complejos ataques de hoy día. Si bien existe una serie de tecnologías avanzadas disponibles, la falta de conocimientos sobre cómo funcionan dificulta a las empresas evaluarlas eficazmente y desplegar la protección necesaria.

Sophos hace un llamamiento al sector de la seguridad para que ayude a los directores de TI a entender y evaluar estas tecnologías por medio de más formación y pruebas abiertas independientes.

Más información

- Exploits. Interceptados.: una guía muy amena sobre lo que son los exploits, cómo funcionan y cómo detenerlos.
- Los exploits a fondo: una exploración en profundidad sobre los exploits específicos que más utilizan los hackers hoy día y las funciones de protección para detenerlos.
- Cómo protegerse del ransomware: cómo funciona el ransomware y qué pasos puede seguir para protegerse contra él.
- Machine Learning for Cybersecurity, Demystified by Sophos: una recopilación de artículos sobre el Machine Learning.
- Hoja de datos de Deep Learning de Sophos Intercept X: una explicación clara del Deep Learning y de por qué supera sistemáticamente otros modelos de Machine Learning.

Presentamos Sophos Intercept X

Sophos Intercept X es la protección next-gen para endpoints más completa del mundo. Utiliza múltiples tecnologías, incluido el Deep Learning, la prevención de ransomware y funciones antiexploits, para proteger contra el ransomware y malware nunca antes visto.

Intercept X se ejecuta junto a los productos antivirus de Sophos y de otros proveedores, lo que incrementa la protección contra el ransomware y los ataques avanzados. Al utilizarse con Sophos Endpoint Protection, le proporciona la protección para endpoints más completa que existe para detener amenazas tanto conocidas como desconocidas.

Los expertos independientes y los clientes confirman la efectividad de Intercept X:

"Intercept X detuvo cada uno de los ataques complejos avanzados con que lo retamos". ESG Labs

"Una de las mejores puntuaciones de rendimiento que hemos visto". AV-TEST

Innovación en seguridad del año
Computing Security Awards 2017

"En los últimos 12-18 meses, no hemos tenido ningún incidente o interrupción grave. Intercept X es la mejor protección posible contra el ransomware y otras amenazas de Internet".
Gus Garcia, director de información y seguridad, Diócesis de Brooklyn

Para obtener más información e iniciar una evaluación gratuita de 30 días, visite es.sophos.com/interceptx.

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

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2-2-18 ES (GH)

SOPHOS