7 VERDADES INCÓMODAS

DE LA SEGURIDAD PARA ENDPOINTS

Resultados de una encuesta independiente patrocinada por Sophos a 3100 directores de TI

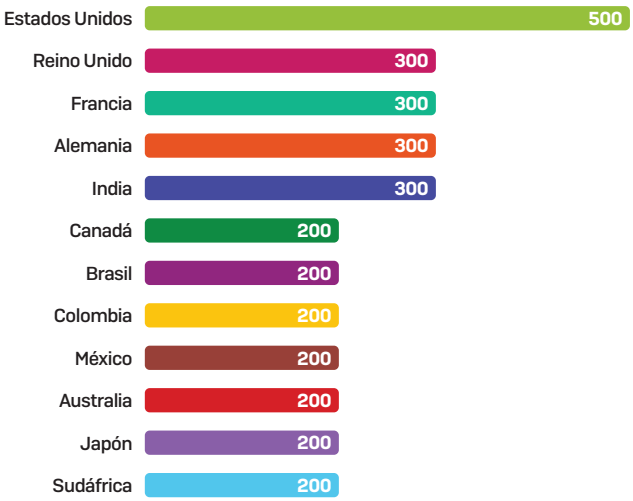
Para comprender la realidad actual de la seguridad para endpoints, Sophos encargó a la consultora independiente Vanson Bourne la realización de una encuesta a 3100 directores de TI de todo el mundo. Este monográfico revela las experiencias, las preocupaciones y los planes futuros de empresas en 12 países y 6 continentes. Proporciona un análisis detallado de los retos diarios a los que se enfrentan los equipos de TI para proteger a sus empresas frente a los ataques cibernéticos, así como su experiencia con las tecnologías de detección y respuesta para endpoints (EDR).

SOPHOS

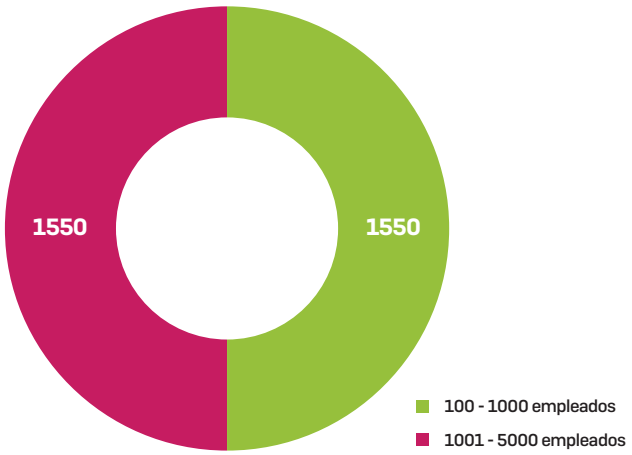
La encuesta

La consultora británica Vanson Bourne entrevistó a 3100 responsables de TI entre diciembre de 2018 y enero de 2019. Para proporcionar un tamaño representativo dentro de cada país, los encuestados se dividieron a partes iguales entre empresas de 100-1000 usuarios y empresas de 1001-5000 usuarios.

Número de encuestados por país



Distribución de los encuestados por tamaño de la empresa



Distribución de los encuestados por sector

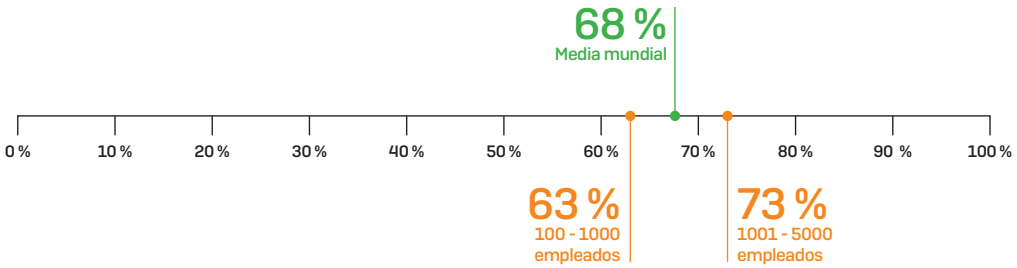
Verdad núm. 1: ser víctima de un ciberataque es ahora la norma

Más de dos tercios (68 %) de las empresas afirman que sufrieron un ciberataque durante el último año. Las empresas grandes sufrieron más ataques (73 %) que las pequeñas (63 %). Hay dos posibles razones para explicar esta diferencia:

- Las empresas más grandes son el principal objetivo de los ciberdelincuentes, al ser consideradas víctimas más lucrativas.
- Las empresas más grandes son más conscientes de que se han visto afectadas por una amenaza cibernética, ya que disponen de más recursos de TI para detectar e investigar problemas.

Definición: ser víctima de un ciberataque

Sufrir un ciberataque y no poder impedir que entre en la red o los endpoints.

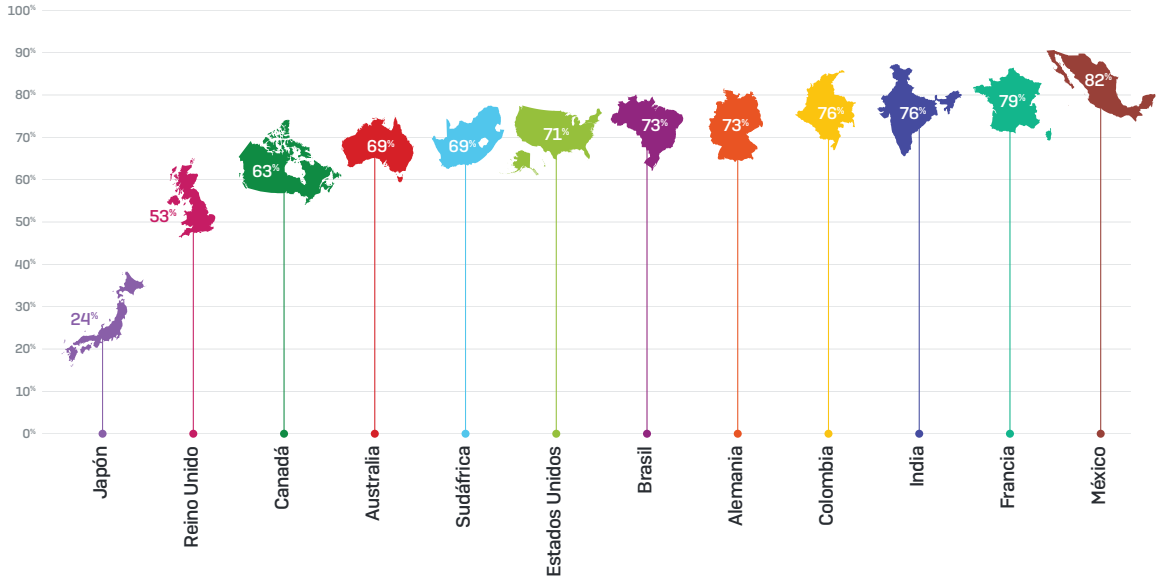


Porcentaje de empresas que fueron víctimas de un ciberataque durante el último año. Preguntado a todos los encuestados (3100)

Por supuesto, estos son solo los ataques que las empresas han descubierto. El número real podría ser mayor.

La conclusión final es que **todos debemos dar por sentado que seremos víctimas de un ciberataque**. Parta de esa base cuando planifique y evalúe su estrategia de seguridad, en lugar de creer que las amenazas no entrarán o que eludirá la atención de los atacantes.

Existen variaciones regionales significativas en los niveles de los ciberataques. Japón experimentó el menor número de ataques (solo un 24 % fue víctima de un ciberataque durante el último año), mientras que México sufrió el mayor número de ataques (un 82 % de los encuestados admitió haber sido afectado).



Porcentaje de empresas que fueron víctimas de un ciberataque durante el último año, dividido por país. Preguntado a todos los encuestados (3100)

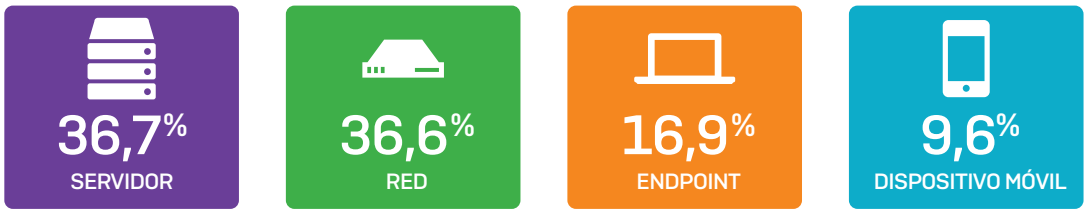
Una explicación de esta discrepancia es que los objetivos de los ciberataques no están repartidos por igual en todo el mundo. Cuando observamos las amenazas individuales, a menudo vemos claros objetivos geográficos en juego. Por ejemplo, hasta la fecha, el Emotet se ha centrado especialmente en América, Europa del Norte y Occidental, Australia y la India, mientras que el WannaCry ha causado más estragos en Ucrania.

Las ciberamenazas son recurrentes

Las empresas que fueron víctimas de un ciberataque sufrieron una media de dos incidentes. Además, el 10 % de las empresas encuestadas sufrió cuatro o más ciberataques durante el último año. Esto sugiere que muchas empresas tienen debilidades continuas en sus defensas que se pueden explotar.

La mayoría de los ataques se detectan en el servidor o en la red

Analizar en qué parte de su entorno las empresas detectan los ciberataques revela información interesante.



Lugar donde las empresas encontraron/detectaron el ciberataque más significativo del que fueron víctimas durante el último año. Preguntado a los encuestados de las empresas que fueron víctimas de un ciberataque durante el último año (2109)

1. La mayoría de las amenazas (36,7 %) se detectan en el servidor

Por lo general, los administradores de TI consideran "seguros" los servidores ya que los usuarios no inician sesión en ellos, pero, en realidad, los datos demuestran que son los que corren mayor riesgo. Los ataques modernos suelen comenzar en los endpoints antes de propagarse lateralmente a los servidores, los objetivos de mayor valor. El hecho de que las empresas detecten las amenazas en los servidores en lugar de en los endpoints sugiere una falta de visibilidad de lo que ocurre en etapas anteriores de la cadena de amenazas, así como lagunas en la seguridad de los endpoints. También es posible que los ataques se adviertan en el servidor porque es entonces cuando pueden causar el mayor impacto en el negocio.

2. Casi 1 de cada 10 amenazas se detecta en dispositivos móviles

El 9,6 % de las amenazas se detecta en los dispositivos móviles. Estos datos sugieren que las amenazas móviles son un peligro significativo y las empresas necesitan garantizar que todos los dispositivos con acceso a la información corporativa estén debidamente protegidos.

3. La India tiene casi el doble de probabilidades de detectar amenazas en los dispositivos móviles

Mientras que el 9,6 % de las amenazas se detecta en dispositivos móviles en todo el mundo, en la India esta cifra es casi el doble, un 18,8 %. Esto es probablemente un reflejo tanto de la tecnología como de los factores culturales. En primer lugar, puesto que nueve de cada diez teléfonos móviles en la India utilizan Android, la plataforma preferida de los autores de malware móvil, los dispositivos indios son especialmente vulnerables a las amenazas móviles. La India también tiene uno de los índices más altos de instalación de aplicaciones inadecuadas, lo que aumenta su propensión a infecciones móviles. Además, la dependencia exclusiva del mundo empresarial en los dispositivos móviles es mucho mayor en la India que en muchas otras partes del mundo, por lo que la probabilidad de que un dispositivo móvil sufra un ataque malicioso posiblemente también es mayor.

https://economictimes.indiatimes.com/tech/software/the-critical-flaw-in-indias-mobile-security/articleshow/65085273.cms

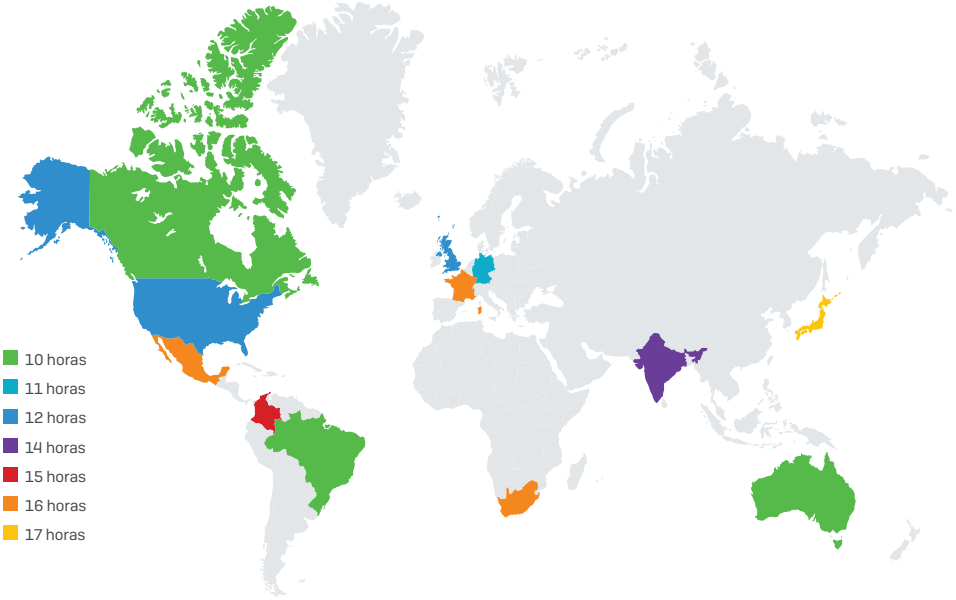
Verdad núm. 2: los equipos de TI tienen poca visibilidad del tiempo de permanencia del atacante

Preguntamos a las empresas cuánto tiempo tardaron en detectar el ciberataque más significativo del año pasado. Para los que sabían la respuesta, la media era de 13 horas.

Promedio de tiempo que la amenaza más significativa ha estado en su entorno antes de detectarse

Obviamente, 13 horas es mucho tiempo para que un hacker tenga acceso ininterrumpido a sus sistemas y datos. En ese tiempo, un cibercriminal puede provocar graves daños, incluida la extracción de datos confidenciales, el robo de credenciales, la instalación de troyanos para robar dinero, la instalación de ransomware y mucho más.

El tiempo que se tarda en detectar las amenazas varía de un país a otro: Australia, Brasil y Canadá son los más rápidos, con una media de 10 horas, mientras que en el extremo opuesto, los equipos de TI japoneses tardan una media de 17 horas.



Promedio de tiempo que la amenaza más significativa ha estado en la empresa antes de que se detectara. Preguntado a todos los encuestados que sabían cuánto tiempo estuvo la amenaza en su entorno (1744 encuestados)

Trece horas es tan solo la punta del iceberg

Si bien 13 horas es mucho tiempo, es importante recordar que, en realidad, se trata del mejor de los casos.

Además, la media del tiempo de permanencia de 13 horas citado por los 1744 encuestados, que sabían cuánto tiempo estuvo la amenaza en el entorno de su empresa antes de que se detectara, puede parecer a primera vista incongruente con otras investigaciones, como el Informe de investigación sobre filtraciones de datos de Verizon, que sostiene que el 68 % de las filtraciones de datos tarda en detectarse varios meses o más. Esta diferencia en los datos es muy esclarecedora y nos permite conocer mejor las realidades a las que se enfrentan las empresas que actualmente no cuentan con un sólido equipo dedicado a la detección y respuesta ante amenazas.

Con el 17 % de las amenazas, las empresas no saben cuánto tiempo han pasado en su entorno antes de detectarlas.

Las empresas solo ven una parte de la historia. Como hemos visto anteriormente, la mayoría de las amenazas se detectan en el servidor, lo que sugiere una falta de visibilidad en el endpoint. Como resultado, es probable que las empresas solo vean un fragmento del rastro de la amenaza, en lugar de la situación completa, subestimando así el tiempo que la amenaza ha estado en su entorno. Por consiguiente, están tomando decisiones relativas a la seguridad con información parcial y sin entender del todo el riesgo cibernético que corren.

Las empresas carecen de las herramientas necesarias para evaluar con precisión el tiempo de permanencia. Para la gran mayoría de pequeñas y medianas empresas, el poder entender completamente cuánto tiempo ha estado una amenaza en su entorno requiere tiempo, herramientas y experiencia que no tienen.

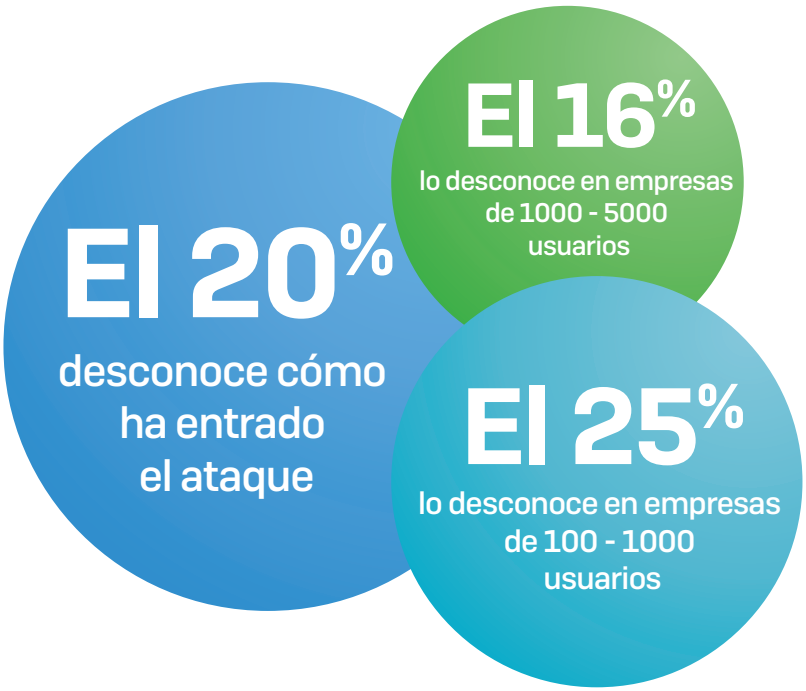
Algunos tipos de amenazas son más fáciles de detectar que otros. Las amenazas varían mucho en cuanto al método de distribución, las técnicas utilizadas y los objetivos finales. Los ataques «a ciegas» genéricos que tienen éxito debido en parte a su volumen (la creencia de que si se envían suficientes ataques, uno se abrirá paso) generalmente no se camuflan tan bien como los ataques furtivos sofisticados y selectivos. De hecho, muchas de estas amenazas del «mercado de masas» se detectan y detienen en cuestión de segundos.

El Informe de investigación sobre filtraciones de datos de Verizon se centró exclusivamente en las filtraciones de datos, mientras que los participantes de la encuesta de Sophos respondieron basándose en una gama más amplia de ciberataques. Las amenazas más impactantes y dañinas son a menudo las más sofisticadas, con el mayor tiempo de permanencia.

Dado que los ciberdelincuentes son ahora maestros del camuflaje, los administradores de TI son plenamente conscientes de la necesidad de identificar los ataques complejos y avanzados que causan los daños más graves. De hecho, los encuestados afirmaron que la función más importante de una solución de detección y respuesta para endpoints (EDR) es la capacidad de identificar eventos sospechosos.

Verdad núm. 3: los equipos de TI no pueden subsanar las carencias de seguridad porque no saben cuáles son

Un elemento clave de una estrategia de seguridad eficaz es impedir que las amenazas entren en la empresa en primer lugar. Sin embargo, uno de cada cinco directores de TI no sabe cómo ha entrado en su empresa el ciberataque más significativo. Como resultado, no pueden proteger estos puntos de entrada.



Porcentaje de encuestados que desconoce cómo ha entrado en su empresa el ciberataque más significativo. Preguntado a todos los encuestados que fueron víctimas de un ciberataque durante el último año (2109)

Las empresas grandes tienen más probabilidades de saber cómo han entrado las amenazas que las pequeñas. Es probable que esto se deba a que disponen tanto de recursos más cualificados como de soluciones de ciberseguridad más completas que las empresas más pequeñas. A menudo, las empresas pequeñas simplemente no tienen los recursos ni la experiencia para investigar lo que ha ocurrido durante un ataque, sino que solo se concentran en limpiarlo. Los ciberdelincuentes se dirigen a empresas de cualquier tamaño. Sin embargo, la incapacidad de las empresas más pequeñas para identificar sus brechas de seguridad las hace más vulnerables.

Verdad núm. 4: las empresas pierden 41 días al año para investigar cuestiones sin importancia

Las empresas dedican, de media, cuatro días al mes a investigar posibles problemas de seguridad, o 48 días al año. Sin embargo, solo el 15 % resultan ser infecciones reales. Como consecuencia, las empresas dedican el 85 % del tiempo a investigar asuntos sin importancia, lo que equivale a unos 41 días al año. Evidentemente, esto tiene repercusiones financieras y de productividad considerables:

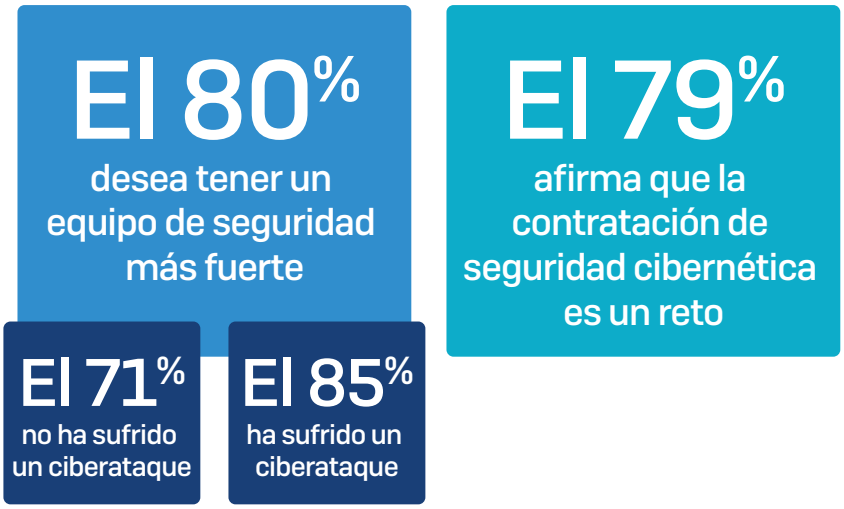
- Coste directo: el impacto financiero y a nivel de recursos de gastar una cantidad tan significativa de tiempo investigando lo que no es un problema.
- Coste de oportunidad: las actividades de TI de las que el personal no puede hacerse cargo ya que están investigando asuntos que no son importantes.

Esta enorme ineficiencia también ayuda a explicar por qué la función de EDR más deseada es la identificación de eventos sospechosos. Contar con herramientas eficaces que ayuden a identificar lo que es sospechoso permite a las empresas concentrar sus limitados recursos en los lugares adecuados, en lugar de buscar agujas en un pajar. A su vez, una mejor identificación de los eventos sospechosos permitirá a las empresas:

- Mejorar la eficiencia: utilizar sus limitados recursos de manera más eficaz.
- Reducir la exposición: encontrar y abordar los incidentes de seguridad reales con mayor rapidez.
- Minimizar el riesgo: concentrar los recursos en los eventos sospechosos que tienen más probabilidades de poner en riesgo a la empresa.

Verdad núm. 5: cuatro de cada cinco empresas tienen dificultades para detectar las amenazas y responder a ellas debido a la falta de experiencia en seguridad

La falta de conocimientos especializados en materia de seguridad para hacer frente a estas amenazas es un problema importante. El 80 % de los directores de TI admite que desea contar con un equipo más fuerte para detectar, investigar y responder adecuadamente a los incidentes de seguridad, por lo que es evidente que las empresas van a ciegas debido a la falta de conocimientos relativos a la ciberseguridad.



Hay una marcada diferencia en el deseo de disponer de un equipo más fuerte entre las empresas que sufrieron un ciberataque (el 85 % quiere un equipo más fuerte) y las que no (el 71 %). Esto sugiere que las empresas que han sufrido un ciberataque muestran una mayor conciencia, tanto de su propia falta de experiencia en seguridad (han aprendido a la fuerza que las amenazas pueden burlar sus defensas) como de los desafíos para detener los ataques avanzados actuales y la necesidad de contar con conocimientos especializados en materia de ciberseguridad para hacerles frente.

Por desgracia, abordar esta escasez de conocimientos no es fácil. Si bien las empresas reconocen que necesitan más ayuda, llevar esa ayuda a la empresa es otro tema. Un 79 % de los encuestados coincide en que la contratación en materia de ciberseguridad es un reto. En este sentido, la creación de los equipos que necesitan es una batalla cuesta arriba, y las empresas tendrán que recurrir a la tecnología, como la inteligencia artificial, para compensar las carencias.

Verdad núm. 6: más de la mitad de las empresas creen que no rentabilizan sus soluciones EDR

La EDR se ha convertido rápidamente en una tecnología imprescindible. Más de 9 de cada 10 directores de TI encuestados (93 %) tienen o se plantean tener EDR en sus arsenales de seguridad. De los encuestados que actualmente no tienen EDR, un 89 % tiene previsto añadirlo a sus defensas y un 61 % tiene intención de hacerlo en los próximos seis meses. A la luz de las revelaciones anteriores sobre el tiempo dedicado a la investigación de incidentes de seguridad y la falta de visibilidad de la cadena de amenazas, estos planes en cuanto a la EDR tienen mucho sentido.

El 93%
quiere EDR en su arsenal de seguridad

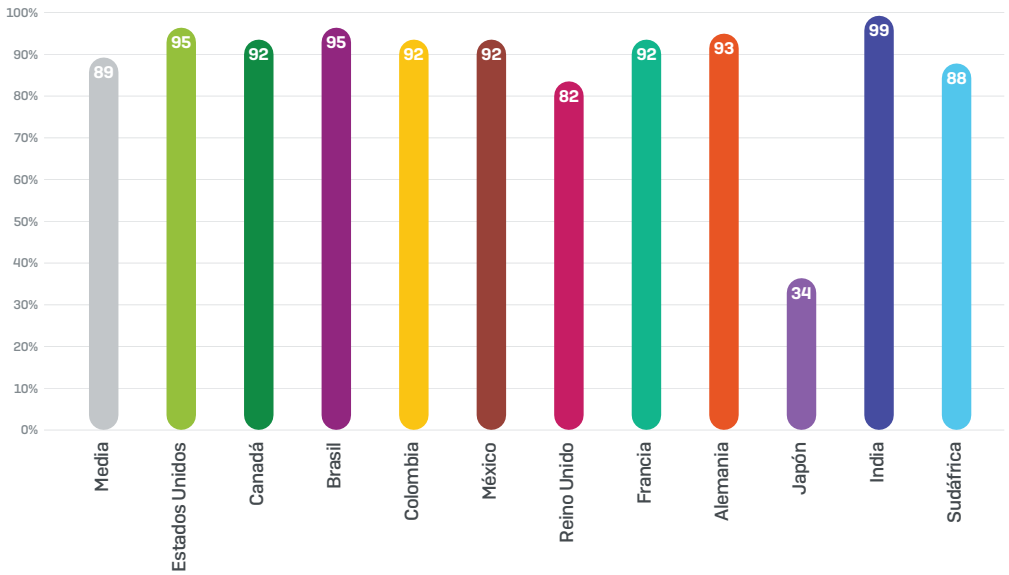
9 de cada 10
empresas sin EDR tienen previsto añadirla

El 61%
de las empresas sin EDR tiene previsto añadirla en un plazo de seis meses

EDR para todos
La misma demanda para empresas grandes y pequeñas

Curiosamente, vemos una demanda de EDR casi igual por parte de empresas pequeñas y grandes. Es evidente que la EDR ya no es exclusiva de las grandes empresas, sino más bien una herramienta para todos.

Si analizamos todos los países encuestados, Japón es un caso aparte en cuanto a planes de adopción de la EDR.



Porcentaje de encuestados que tienen previsto añadir funciones de EDR. Preguntado a todos los encuestados que no tienen EDR actualmente (1990)

En todos los países menos Japón, al menos 8 de cada 10 empresas sin tecnología EDR tienen intención de añadirla. La India encabeza la lista: el 99 % de sus empresas que no tienen EDR tiene previsto incorporarla; le siguen de cerca Australia (97 %), los Estados Unidos y Brasil (ambos 95 %). Sin embargo, en Japón solo una de cada tres (34 %) empresas sin tecnología EDR tiene intención de añadirla a sus defensas de seguridad.

Tener solo EDR no es la respuesta

Aunque la EDR es una potente herramienta que puede aumentar sus defensas cibernéticas, necesita tener los recursos para usarla de manera efectiva y sacar el máximo partido a su inversión. Desafortunadamente, más de la mitad de los encuestados que invirtieron en EDR no pueden hacerlo. Para el 54 % de las empresas, la EDR fue desperdiciar el dinero, ya que no pueden obtener el máximo beneficio de sus soluciones.

El 54%

no puede sacar el máximo partido a su solución EDR

Curiosamente, aunque se podría pensar que las empresas pequeñas tendrían más dificultades para beneficiarse de sus inversiones en EDR, la realidad es que el tamaño de la empresa no es determinante. Los datos de respuesta fueron casi los mismos para las empresas encuestadas de todos los tamaños.

Hay varias explicaciones posibles para estos resultados y es probable que las dos siguientes entren en juego entre los encuestados:

Falta de recursos de gestión de EDR. Las empresas necesitan considerar quién gestionará sus soluciones EDR para asegurarse de que pueden aprovecharlas al máximo. Como ya hemos visto, la falta de conocimientos de ciberseguridad es un problema generalizado.

Usabilidad: disparidad de competencias. La tecnología solo puede añadir valor si se puede utilizar de forma eficaz. Las empresas deben prestar la debida atención a lo fácil que es utilizar una solución EDR y a cómo encaja con sus habilidades y recursos disponibles.

Verdad núm. 7: una mala experiencia nos hace más precavidos; las cibervíctimas aprenden por las malas

La encuesta ha revelado diferencias muy claras en algunas áreas entre los que habían sido víctimas de un ciberataque y los que habían evitado a los hackers. Las empresas que fueron víctimas de un ciberataque durante el último año:

- Son más prudentes: investigan el doble de incidentes que otras empresas.
- Dedican más tiempo a la ciberseguridad: pasan cuatro días al mes investigando posibles incidentes, en lugar de tres para las personas que no son víctimas.

2 veces más
investigaciones de incidentes

1/3
más de tiempo perdido

Es probable que aquí haya varios factores en juego:

1. **Han aumentado su seguridad después del incidente.** Es probable que las víctimas aprecien mucho más el impacto de los ciberataques y estén dispuestas a dedicar más tiempo, esfuerzo y recursos para detenerlos.
2. **Tienen una visibilidad limitada de su entorno.** Las defensas cibernéticas deficientes significan que se abren paso más amenazas y que tienen menos capacidad para investigarlas. Como resultado, tienen más incidentes potenciales que investigar, con menos herramientas para hacerlo, lo que lleva más tiempo.
3. **Son más conscientes de lo que buscar.** Al haber sufrido un ataque, estas empresas son más conscientes de los signos que deberían hacerlas sospechar.

La verdad acerca de la EDR

Esta encuesta ha puesto de manifiesto una serie de retos a los que se enfrentan las empresas de todo el mundo en lo que respecta a la seguridad para endpoints, así como los retos que plantea la tecnología EDR. Entonces, ¿cuál es la verdad sobre la EDR y cómo encaja realmente en la protección para endpoints?

La realidad es que la EDR puede ayudar a abordar muchos de los desafíos revelados por la encuesta. Empecemos por entender los ciberataques. Dos de cada tres empresas sufrieron un ciberataque el año pasado. Sin embargo, el 17 % de los administradores de TI no sabe cuánto tiempo estuvo la amenaza en su entorno y el 20 % no sabe cómo entró. La EDR puede proporcionar respuestas a estas preguntas, permitiendo a las empresas identificar la causa raíz del ataque, cuánto tiempo ha estado en su sistema y los posibles efectos. Al disponer de esta información, las empresas pueden implementar las defensas que necesitan y tapar sus agujeros de seguridad.

También hemos visto que las empresas tardan 13 horas de media en detectar una amenaza. La EDR también puede identificar de forma proactiva los eventos sospechosos, lo que permite a los equipos de TI detectar ataques que pueden haber pasado desapercibidos durante mucho más tiempo. Por consiguiente, la EDR permite a las empresas tomar medidas eficaces para reducir la probabilidad de que se conviertan en otra víctima de un ciberataque.

Otra de las conclusiones de la encuesta es que las empresas dedican 48 días al año a investigar posibles incidentes de seguridad. La EDR puede reducir este tiempo al ofrecer un análisis experto y una respuesta guiada a los posibles incidentes que los equipos de todos los niveles de especialización pueden comprender y tomar medidas al respecto. Esto reduce drásticamente el tiempo dedicado a detectar y responder a los incidentes.

No obstante, también hemos visto que el 54 % de las empresas con EDR no puede beneficiarse plenamente de su solución. Por eso es tan importante elegir una solución EDR que funcione para su empresa, en lugar de una que simplemente añada más trabajo. Una solución EDR correctamente implementada puede ayudar a las empresas a utilizar sus limitados recursos de manera más eficiente.

Conclusión

La ciberseguridad es un reto constante para las empresas de todos los tamaños en todo el mundo. En este sentido, hay varias conclusiones importantes que podemos extraer de las experiencias de 3100 directores de TI en 12 países y 6 continentes.

En primer lugar, al planificar sus estrategias de ciberseguridad, las empresas deben partir de la base de que una amenaza se abrirá camino a través de sus defensas. Al hacerlo, también deben tener en cuenta las limitaciones de su visibilidad de las amenazas y su consiguiente incapacidad para identificar y bloquear las brechas en su armadura de seguridad.

En segundo lugar, la gran mayoría de las empresas considera que la EDR es parte integrante de sus estrategias de seguridad. No es de extrañar; la EDR es una herramienta eficaz para abordar varios de los desafíos que se destacan en la encuesta. En un momento en el que las habilidades en materia de ciberseguridad son escasas, una solución EDR inteligente puede proporcionar los conocimientos y la experiencia necesarios para anticiparse a las amenazas.

Sin embargo, como ha puesto de manifiesto la encuesta, no vale con solo comprar una solución EDR. Para demasiadas empresas, sus inversiones en tecnología EDR resultan ser una pérdida de dinero, ya que no pueden aprovechar al máximo sus soluciones EDR. Para evitar caer en esta trampa, cada empresa debe examinar a fondo tanto las funciones como la usabilidad de una solución EDR antes de añadirla a su arsenal de seguridad.

Acerca de Sophos

Sophos es un proveedor líder de protección para endpoints y redes. Más de 100 millones de usuarios en 150 países confían en Sophos para obtener la mejor protección contra amenazas sofisticadas y fugas de datos. Con **Intercept X Advanced with EDR**, las empresas pueden entender el alcance y el impacto de los incidentes de seguridad, detectar ataques que podrían haber pasado desapercibidos, analizar archivos para determinar si son una amenaza e informar con confianza sobre la postura en materia de seguridad de su empresa en cualquier momento. El Machine Learning integrado y la información sobre amenazas de SophosLabs le permite añadir experiencia, no personal. Para obtener más información y empezar una prueba gratuita de 30 días, vaya a es.sophos.com/intercept-x.

Acerca de Vanson Bourne

Vanson Bourne es una consultora independiente especializada en estudios de mercado para el sector tecnológico. Su reputación de análisis sólidos y creíbles basados en la investigación se asienta en rigurosos principios de investigación y en su capacidad para recabar las opiniones de los principales responsables de la toma de decisiones en todas las funciones técnicas y empresariales, en todos los sectores empresariales y en todos los principales mercados. Si desea más información, visite www.vansonbourne.com.

Para empezar una prueba gratuita de 30 días de EDR, vaya a es.sophos.com/intercept-x

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

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

26-02-2019 WP (RP)

SOPHOS