proofpoint.

LIBRO ELECTRÓNICO

El coste de la seguridad "suficientemente buena"

Cálculo del valor real de las soluciones de ciberseguridad

Ciberdelincuencia y riesgos para las empresas

Quien dijo que la delincuencia no compensa, no parece que anticipara los ciberataques modernos. El coste medio de una fuga de datos para las empresas de EE. UU. afectadas pasó de los 5,4 millones de dólares en 2013 a los 9,44 millones de dólares en 2022[1] (superando al crecimiento de la inflación durante el mismo período). En conjunto, las fugas de datos cuestan a las empresas de EE. UU. alrededor de 1400 millones de dólares al año. Esto equivale a 5400 dólares por cada adulto estadounidense [2].

A nivel mundial, la ciberdelincuencia se prevé que cueste 10,5 billones de dólares para 2025[3]. Otros investigadores calculan que la ciberdelincuencia cuesta a las empresas la increíble cifra de 1,79 millones de dólares cada *minuto*[4].

Sin duda estos costes son enormes. Pero no se quedan en las pérdidas financieras inmediatas. La ciberdelincuencia puede dañar la reputación de su empresa o dar lugar a sanciones normativas por parte de los organismos reguladores. Puede alterar las operaciones e incluso frustrar su modelo de negocio, imposibilitando seguir con su actividad principal.

No existe forma de eliminar por completo los riesgos asociados a la ciberdelincuencia. Digamos que, en el mundo actual, son un elemento más de la actividad empresarial.

Sin embargo, es posible gestionar esos riesgos. De igual forma que los líderes de las empresas y los responsables de la gestión de riesgos planifican y se preparan para otros riesgos implícitos de la actividad empresarial, también pueden limitar su exposición a los riesgos asociados a la ciberdelincuencia. Como en el caso de esos otros riesgos, necesitará modelizar las pérdidas financieras que un ciberataque podría generar a su empresa. A partir de ahí puede planificar la forma de equilibrar esos riesgos respecto a lo que costaría reducirlos.

A nivel mundial, el coste medio de una fuga de datos es de

4,24 M$[5].

Los expertos prevén que la ciberdelincuencia costará al mundo

10,5 B$[6]

Un uno por ciento

del PIB mundial se pierde actualmente por causa de la ciberdelincuencia[7].

La ciberdelincuencia cuesta a las empresas

1,79 M$

por minuto.

1 IBM. "**Cost of Data Breach Report 2022**" (Informe sobre el coste de una fuga de datos en 2022), julio de 2022.
2 Rick Newman *(Yahoo Finance)*. "**We're all paying a cybersecurity tax**" (Todos pagamos un impuesto de ciberseguridad), mayo de 2021.
3 Steve Morgan *(Cybersecurity Ventures)*. "**Cybercrime to Cost the World $10.5 Trillion Annually by 2025**" (La ciberdelincuencia costará al mundo 10,5 billones de dólares al año para 2025), noviembre de 2020.
4 James Coker *(Infosecurity Magazine)*. "**Cybercrime Costs Organizations Nearly $1.79 Million Per Minute**" (La ciberdelincuencia cuesta a las organizaciones casi 1,79 millones de dólares cada minuto), julio de 2021.
5 IBM. "**Cost of Data Breach Report 2022**" (Informe sobre el coste de una fuga de datos en 2022), julio de 2022.
6 Steve Morgan *(Cybersecurity Ventures)*. "**Cybercrime to Cost the World $10.5 Trillion Annually by 2025**" (La ciberdelincuencia costará al mundo 10,5 billones de dólares al año para 2025), noviembre de 2020.
7 Zhanna Malekos Smith and Eugenia Lostri *(Center for Strategic and International Studies)*. "**The Hidden Cost of Cybercrime: Report**" (Informe sobre el coste oculto de la ciberdelincuencia), diciembre de 2020.

El primer paso para evaluar soluciones de seguridad es comparar su resistencia a riesgos con sus costes, a fin de asegurarse de obtener la mejor relación calidad-precio.

Invertir en tecnologías de seguridad es una estrategia para reducir estos riesgos. Sin embargo, ¿puede tener la garantía de que las inversiones que realiza son las más acertadas?

Como CISO, su prioridad es la reducción de riesgos. El primer paso para evaluar soluciones de seguridad es comparar su resistencia a riesgos con sus costes, a fin de asegurarse de obtener la mejor relación calidad-precio. Tampoco debe olvidar los costes más allá de la licencia, como el hardware, el despliegue, la operatividad y los costes continuos de mantenimiento. Y considere los beneficios o ventajas adicionales que las soluciones pueden ofrecer, como la mejora del rendimiento de la plantilla.

Baste como ejemplo la presión sobre su personal de seguridad interno. Los CISO actuales se enfrentan a la escasez de personal en sus programas de operaciones de seguridad. A nivel global, 2,72 millones de puestos de ciberseguridad siguen vacantes[8]. Se calcula que para proteger adecuadamente los activos críticos de las organizaciones la plantilla de ciberseguridad tendría que aumentar un 65 % [9]. Para los CISO, estos retos son una realidad cotidiana.

Está claro que el tiempo de los profesionales de seguridad es valioso y que entre los costes de una solución de ciberseguridad deben considerarse las cargas administrativas. Pero ¿qué hay de la productividad de los usuarios? ¿O los costes laborales asociados a la respuesta a incidentes? ¿O los derivados de informar sobre un incidente?

En esta guía, analizaremos en detalle los costes asociados al despliegue (y ejecución) de una solución de ciberseguridad. Examinaremos todos los factores que pueden determinar el valor total de una solución, incluidos algunos que es posible que no haya considerado. Calcularemos cuándo puede ser más rentable invertir en una solución avanzada de seguridad del correo electrónico o una solución completa de protección frente a amenazas por correo electrónico y la nube que optar por complementos (add-on) de "bajo coste" o soluciones tradicionales.

8 (ISC)2. "**Cybersecurity Workforce Study**" (Estudio sobre el mercado de trabajo de la ciberseguridad), marzo de 2022.
9 Ibid.

Gestión de los riesgos de ciberseguridad: los costes reales

Sus inversiones en ciberseguridad son sin duda una manera de reducir los riesgos operativos y empresariales. Pero no existe una sencilla relación directa entre el dinero invertido y la amplitud de la cobertura. Para disponer de una defensa sólida, necesita un enfoque de seguridad multicapa.

Algunas soluciones de seguridad serán más eficaces que otras a la hora de reducir su exposición a riesgos. Pequeñas diferencias en la eficacia pueden tener un enorme impacto en el riesgo (y el coste potencial) de una fuga de datos. Tampoco son iguales los precios de todas las soluciones.

Es fundamental tener en cuenta estos elementos a la hora de tomar una decisión. Esto significa tener en cuenta su retorno sobre la inversión en seguridad (ROSI) potencial.

Para ello, necesitará pensar en todas las pérdidas que provocaría un evento de pérdida de datos de envergadura. Esto va mucho más allá de los costes asociados a la propia fuga de datos. El daño a largo plazo para las empresas y su reputación puede tener un impacto años después.

Frente a estas posibles pérdidas, necesitará sopesar el coste de la propia solución de ciberseguridad. A primera vista, esto podría parecer fácil de calcular: basta con mirar los precios de las licencias.

Pero cuando se trata del valor económico total de una solución de ciberseguridad, los costes de licencia son solo la punta del iceberg. Si solamente mira la licencia, no podrá tener una visión completa del coste que una solución supondrá para su organización. Hay otros muchos costes ocultos de propiedad debajo de la superficie y pueden aumentar drásticamente el coste total de una solución.

Y la reducción del riesgo no siempre es tan sencilla. Utilizar todas las funciones de una solución puede reducir su nivel de riesgo un 50 %, pero rara vez podrá aprovechar todas las funciones de un producto de forma inmediata. Y la mayoría de las soluciones ofrecen ventajas que van más allá de la reducción de riesgos, incluida la mejora del rendimiento de los equipos de seguridad, lo que aumenta el valor de la solución.

Las secuelas de una fuga de datos

Las pérdidas asociadas a una fuga de datos pueden incluir todo lo siguiente:

- Pérdida de negocio y de clientes
- Pérdida de datos y del valor que se conseguiría al analizar esos datos
- Pérdidas económicas directas*
- Daños a la reputación
- Pérdida de productividad de los empleados
- Tiempo de inactividad
- Disminución del valor de las acciones
- Pérdida de propiedad intelectual
- Pérdida de la ventaja competitiva
- Sanciones o multas por incumplimiento

*Estas pueden incluir los pagos de rescate y los costes laborales y de servicio asociados a la respuesta y recuperación.

Suma de los costes

Para la mayoría de las organizaciones, la adopción de una nueva solución de ciberseguridad puede resultar caro y laborioso. El proceso también puede perturbar la actividad de los usuarios, así como las operaciones ordinarias de TI y de seguridad. Algunas herramientas son difíciles de mantener, por lo que aumentarían la carga de trabajo de equipos de seguridad ya sobrecargados. Para calcular el impacto financiero total que la adquisición tendrá en su organización, necesitará tener en cuenta varios factores:

Licencia

¿Qué paga al proveedor al año por el uso de la solución? Su coste total de licencia es el coste anual por usuario multiplicado por el número de usuarios.

Hardware

Algunas soluciones también pueden necesitar hardware, con el consiguiente aumento de costes. Esto puede ser particularmente cierto si administra el hardware de forma local. ¿Qué le costará mantener actualizado este hardware, garantizar la conectividad, mantener las instalaciones adecuadas o preparar y recuperarse frente a desastres? ¿Cuál será el número de empleados encargados de mantener el equipo?

Administración permanente

Piense en los costes permanentes de administración como el tiempo dedicado por los empleados especialistas en mantener las actividades de administración permanente. Es muy importante tener en cuenta este factor. Imagine que una solución requiere para su administración dos empleados a tiempo completo, y otra solamente uno. Debería tener en cuenta que, en el caso de la primera solución, la administración permanente costaría el doble a largo plazo. Mirado de esta forma, una solución que es aparentemente "gratis" puede convertirse rápidamente en mucho más costosa que un producto de pago que sea fácil de administrar, sobre todo si el proveedor de ese producto lo acompaña con un soporte técnico robusto.

Despliegue

Servicios profesionales
Muchos proveedores recomendarán o incluso necesitarán su equipo de servicios profesionales para ayudarle a configurar y desplegar la solución. Y estos servicios, por supuesto, tienen un coste.

Tiempo de recursos
Tanto si interviene el equipo de servicios profesionales como si no, el despliegue de un nuevo producto requiere al menos algo de trabajo de sus empleados internos. ¿Cuántas horas habrá que dedicar al proyecto? ¿Quiénes serán los encargados del trabajo? El cálculo del número de horas de trabajo de sus empleados en nómina es solo el primer paso. ¿Qué otras responsabilidades necesitará poner a un lado para centrarse en esta iniciativa? También necesitará considerar el coste que podría suponer que esos profesionales dejaran de realizar tareas de alto valor.

Si profundizamos en el coste total de propiedad de una solución de ciberseguridad, pronto queda claro que los costes de implementación y de mantenimiento continuo pueden superar los gastos asociados a la licencia.

Consideración de beneficios

Para conocer el valor total de una solución, considere todos los costes anteriores y evalúelos en relación con los beneficios que ofrece el producto. La resistencia a riesgos es sin duda el principal beneficio de cualquier solución de seguridad. Pero al igual que en el caso de los costes, existen otros factores a considerar.

A continuación se citan algunos de los beneficios que debería tener en cuenta:

- **Resistencia a riesgos**

  Para calcular la resistencia a riesgos de una solución, en primer lugar necesita conocer la magnitud de las pérdidas potenciales para su organización. ¿Cuál es el coste medio de una fuga de datos en su sector y región, y para una empresa del tamaño de la suya? Necesitará evaluar estos datos respecto a su vulnerabilidad y la fortaleza frente a riesgos de la solución. Por último, tenga en cuenta que puede llevar tiempo conseguir el máximo rendimiento de una solución y aprovechar todas sus ventajas

- **Mejora del rendimiento de la plantilla**

  Productividad de los usuarios
  La productividad puede adoptar muchas formas. Sin embargo, las dos más importantes para los responsables de la seguridad son la productividad de los usuarios en su conjunto y la de sus equipos de seguridad y TI. Una solución de ciberseguridad puede afectar a la productividad de los empleados de distintas y complicadas maneras. Estos efectos se extienden a los usuarios, así como a los equipos de ciberseguridad y TI. ¿Cuántos minutos u horas del tiempo de analistas de una empresa se perderían si no tuvieran acceso a sus portátiles mientras se limpian sus dispositivos de malware, por ejemplo? ¿Cuánto le costaría a su empresa si los miembros del equipo de ventas no pudieran ponerse en contacto con los clientes debido al compromiso de una cuenta cloud? Cada vez se bloquean mensajes de spam y maliciosos, está impidiendo interrupciones que pueden provocar daños a su empresa. Además, cada vez que un mensaje malicioso consigue pasar, el incidente podría robar tiempo a los profesionales del centro de ayuda y a los administradores de TI.

El coste anual de los ataques relacionados con el phishing es ahora superior a

14,7 M$[10].

Cada trabajador capacitado pierde de media

siete horas

de tiempo productivo al año por causa del phishing[11].

Un ataque de ransomware en 2021 costó de media a su víctima

4,54 M$[12].

Las víctimas de estafas Business Email Compromise (BEC) han pagado más de

43 B$

a los ciberdelincuentes entre 2016 y 2021[13].

10 Ponemon Institute. "**2021 Cost of Phishing Study**" (Estudio sobre el coste del phishing en 2021), junio de 2021.
11 Ibid.
12 IBM. "**Cost of a Data Breach Report 2022**" (Informe sobre el coste de una fuga de datos en 2022), julio de 2022.
13 Federal Bureau of Investigation. "**Business Email Compromise: The $43 Billion Scam**" (Ataques BEC: la estafa que cuesta 43 000 millones de dólares), mayo de 2022.

Supervisión, clasificación y análisis
Los analistas de ciberseguridad se encuentran entre los profesionales más cualificados y mejor remunerados de las plantillas de TI actuales. Y su número es escaso. La forma en la que los equipos de operaciones de seguridad asignan su tiempo y prioridad es una cuestión de importancia estratégica para su empresa. ¿Facilita o complica sus trabajos la solución que está considerando? ¿Se integra fácilmente en las soluciones de supervisión de eventos o de detección y respuesta que utiliza actualmente en su entorno? Tal vez externalice estas responsabilidades a un proveedor de servicios. En ese caso, ¿mejorará la solución la capacidad de su partner de mantener la visibilidad y la cobertura?

Respuesta y corrección
Cuando un equipo de seguridad actúa para impedir que los ciberdelincuentes se desplacen por el entorno, el tiempo es fundamental. ¿Tiene la solución una plataforma consolidada? ¿Puede utilizar la administración de políticas para agilizar los cambios en la configuración? Cuando más rápido pueda bloquear y corregir las amenazas entrantes, menor será la probabilidad de que progresen y provoquen fugas de datos.

Automatización
¿Incluye la solución flujos de trabajo de automatización predefinidos para que pueda realizar tareas que forman parte de sus actividades de TI o de seguridad del correo electrónico habituales? Si su equipo tiene que dedicar mucho tiempo al diseño y configuración para que la solución pueda ejecutar flujos de trabajo automatizados, también debería tener en cuenta este factor. Si dos soluciones pueden completar la misma tarea, pero se tarda más en configurar una de ellas (o requiere mucha codificación o carga administrativa permanente), su coste será mayor.

Inteligencia
La caza de amenazas es una función de seguridad muy especializada que puede ayudar a detectar vulnerabilidades o a prevenir que incidentes menores acaben convirtiéndose en fugas de datos. Pero la caza de amenazas requiere conocimientos y experiencia, con la que puede que cuente o no internamente. La solución que está considerando, ¿proporciona inteligencia que permita reducir la carga de trabajo de su equipo? ¿Permite disponer de visibilidad para que pueda dedicar menos tiempo y esfuerzo en la caza de amenazas, o profundizar con el mismo número de recursos?

Equilibrio entre costes y beneficios en el mundo real

Ahora que ya ha descrito los costes y beneficios que podría aportar una solución de seguridad a su organización, examinemos más detenidamente cómo calcular el valor total de las soluciones en el mundo real.

¿Cuáles son las diferencias reales entre las llamadas funciones "gratuitas" o de "bajo coste" y las que obtendría con una solución líder del sector?

Cuando sopese las opciones de la solución, puede calcular el valor total de cada solución restando los costes de los beneficios o ventajas. Utilizaremos dos ejemplos para ilustrar cómo:

Ejemplo 1

Seguridad del correo electrónico

El objetivo de los ataques por correo electrónico actuales son las personas, no los sistemas. Emplean tácticas de ingeniería social para engañar a los usuarios y convencerlos para que visiten sitios web maliciosos o les proporcionen credenciales. Una solución de seguridad del correo electrónico eficaz debe tener la capacidad de prevenir, detectar y responder a las amenazas que se dirigen contra sus empleados. También debe poder dotar a sus equipos de seguridad de la visibilidad y la información que necesitan para ser eficaces, sin ser difíciles de configurar y administrar.

Evaluación de costes

Supongamos que su empresa es una firma de servicios financieros ubicada en Estados Unidos, que cuenta con 15 000 empleados y que está considerando dos soluciones de seguridad del correo electrónico, una de las cuales es una solución de las llamadas "gratis", que se incluye con un producto existente para el que tiene licencia. En este ejemplo suponemos que un empleado a tiempo completo cuesta 150 000 dólares al año.

Sus costes (en tres años) podría ser como se indica a continuación:

CATEGORÍA DE COSTE	SOLUCIÓN DE SEGURIDAD DEL CORREO ELECTRÓNICO A	SOLUCIÓN DE SEGURIDAD DEL CORREO ELECTRÓNICO B
Costes de licencia	-787 500 $	- 0 $ (ya que mantendrá el bundle, la nueva solución se considera una adición)
Servicios profesionales	-27 000 $	-0 $ (ya desplegada)
Tiempo de empleados: despliegue	-6250 $ (1 a tiempo completo durante 0,5 meses)	-0 $ (ya desplegada)
Tiempo de empleados: tareas permanentes	-450 000 $ (1 a tiempo completo por año)	-450 000 $
Total	**-1 270 750 $**	**-450 000 $**

En este caso, un vistazo inicial a los costes podría llevarle a pensar que la Solución B tiene una mejor relación calidad/precio, ya que la Solución A cuesta más de 700 000 dólares más. Los servicios profesionales y el despliegue de la actual se consideran gastos previos, luego los excluimos.

Beneficios de las soluciones de seguridad del correo electrónico

Sin embargo, para conocer el valor total de las soluciones, debe considerar también los beneficios o ventajas de cada una, incluida la resistencia a riesgos y la mejora del rendimiento de la plantilla.

En el transcurso de tres años, podría ser algo así:

CATEGORÍA DE BENEFICIO	SOLUCIÓN DE SEGURIDAD DEL CORREO ELECTRÓNICO A	SOLUCIÓN DE SEGURIDAD DEL CORREO ELECTRÓNICO B
Resistencia a riesgos	5 707 901 $	4 442 698 $
Productividad de los usuarios	1 200 208 $	974 788 $
Supervisión, clasificación y análisis	1 532 510 $	1 224 135 $
Respuesta y corrección	2 651 671 $	2 153 641 $
Automatización	0 $	756 685 $
Inteligencia sobre amenazas	0 $	0 $
Total	**11 092 290 $**	**9 551 947 $**

La solución A proporciona mucha más resistencia a riesgos y mejora la eficacia de la plantilla, lo que complica el panorama. La solución B tiene una función adicional, por lo que en este caso investigaríamos si podemos añadir esta opción con la solución A, lo que aumentaría nuestro retorno sobre la inversión en seguridad (ROSI).

Por último, convendrá sopesar los costes totales respecto a las ventajas de cada solución, para poder obtener el valor total de cada solución:

CATEGORÍA	SOLUCIÓN DE SEGURIDAD DEL CORREO ELECTRÓNICO A	SOLUCIÓN DE SEGURIDAD DEL CORREO ELECTRÓNICO B
Beneficios	11 092 290 $	9 551 947 $
Costes	-1 270 750 $	-450 000 $
Valor total	**9 821 540 $**	**9 101 947 $**

Aquí es cuando se aprecia el panorama completo. La Solución A puede tener un precio mayor, pero su valor total supera en más de 700 000 dólares al de la opción "gratuita" de la Solución B. En la comparación también debería tenerse en cuenta las necesidades de su empresa.

Ejemplo 2

Seguridad cloud

Las soluciones de seguridad de aplicaciones cloud modernas ayudan a las organizaciones a gestionar los riesgos basados en las personas en la nube. Las empresas actuales utilizan las plataformas y servicios cloud a niveles cada vez mayores. Lo hacen para favorecer plantillas híbridas y remotas, así como para aprovechar la flexibilidad y la agilidad empresarial que permite la nube. Ahora bien, las aplicaciones y servicios basados en la nube no solo ofrecen ventajas, desafortunadamente también introducen nuevos riesgos. Una solución CASB (Cloud Application Security Broker) protege las aplicaciones de TI aprobadas en la nube. Sin embargo, también ofrece visibilidad y control del acceso y uso de las personas a las aplicaciones cloud, y cómo comparten los datos sensibles.

En 2021, el número de fugas de datos en las que se vieron implicados recursos de la nube fue mayor que el de fugas de activos locales por primera vez[14]. Las empresas migran a la nube, y los ciberdelincuentes hacen lo propio. La dependencia de las empresas de aplicaciones de software como servicio como Microsoft 365 y Google Workspace sigue aumentando, por lo que prevemos que esta tendencia continúe.

Si va a trasladar una parte importante de su infraestructura a la nube, no se trata de tanto de si necesita una solución de protección de la nube, sino de cuál.

Evaluación de costes

Supongamos que tiene una organización de servicios de atención sanitaria ubicada en Estados Unidos con 15 000 empleados y que está considerando una nueva solución cloud (Solución A) y la compara con su solución existente (Solución B). En este ejemplo también suponemos que un empleado a tiempo completo cuesta 150 000 dólares al año.

Este sería el desglose de costes durante un período de tres años:

CATEGORÍA DE COSTE	SOLUCIÓN DE SEGURIDAD PARA LA NUBE A	SOLUCIÓN DE SEGURIDAD PARA LA NUBE B
Costes de licencia	-776 250 $	-765 000 $
Servicios profesionales	-26 000 $	-0 $ (ya desplegada)
Tiempo de empleados: despliegue	-6250 $ (1 a tiempo completo durante 0,5 meses)	-0 $ (ya desplegada)
Tiempo de empleados: tareas permanentes	-450 000 $ (1 a tiempo completo por año)	-450 000 $
Total	**-1 258 500 $**	**-1 215 000 $**

En este caso, los costes de la Solución A superan ligeramente los de la Solución B. Los servicios profesionales y el despliegue para la actual se consideran gastos previos, luego los excluimos. La diferencia real entre las soluciones se reflejará al comparar los beneficios.

NOTA IMPORTANTE: si su solución existente es una solución de administración de identidades y acceso y está considerando pasarse a una solución CASB, es posible que haya costes de hardware adicionales a tener en cuenta. La migración a la nube significa por lo general gastar menos en hardware, pero su ahorro total dependerá del proveedor que elija.

14 Verizon. "2021 Data Breach Investigations Report" (Informe sobre el coste de una fuga de datos en 2021), mayo de 2021.

Evaluación de beneficios

Como en el caso de la evaluación de su seguridad del correo electrónico, para poder comparar su valor total, debe considerar también las ventajas o beneficios que ofrece cada solución. En el transcurso de tres años, podría ser algo así:

CATEGORÍA DE BENEFICIO	SOLUCIÓN DE SEGURIDAD PARA LA NUBE A	SOLUCIÓN DE SEGURIDAD PARA LA NUBE B
Resistencia a riesgos	6 137 377 $	3 625 216 $
Productividad de los usuarios	42 684 $	34 667 $
Supervisión, clasificación y análisis	104 339 $	84 742 $
Respuesta y corrección	94 853 $	77 038 $
Inteligencia sobre amenazas	**1 264 707 $**	**1 027 174 $**
Total	**7 643 961 $**	**4 848 837 $**

En este caso, la solución A proporciona mucha más resistencia a riesgos, así como un mayor rendimiento de la plantilla.

	SOLUCIÓN DE SEGURIDAD PARA LA NUBE A	SOLUCIÓN DE SEGURIDAD PARA LA NUBE B
Beneficios	**7 643 961 $**	**4 848 837 $**
Costes	-1 258 500 $	-1 215 000 $
Valor total	6 385 461 $	3 633 837 $

Debido a su mayor resistencia a riesgos y a las mejoras en el rendimiento de la plantilla, la Solución A proporciona casi el doble de valor que la Solución B.

Visión general

Antes de tomar la decisión de invertir en una solución de seguridad es necesario que sopese los costes y beneficios de cada una de las opciones disponibles. Resulta absolutamente fundamental encontrar una solución que satisfaga sus necesidades presupuestarias a corto plazo, pero igualmente importante resulta encontrar una que reduzca los riesgos financieros que presenta la ciberdelincuencia para su negocio a largo plazo.

Las opciones con bajos costes de licencia podrían parecer un buen negocio a primera vista, pero debe considerar un conjunto de factores mucho más amplio si desea tomar la mejor decisión posible. Busque un proveedor cuyas soluciones proporcionen cobertura holística completa para los vectores de ataques más utilizados en la actualidad.

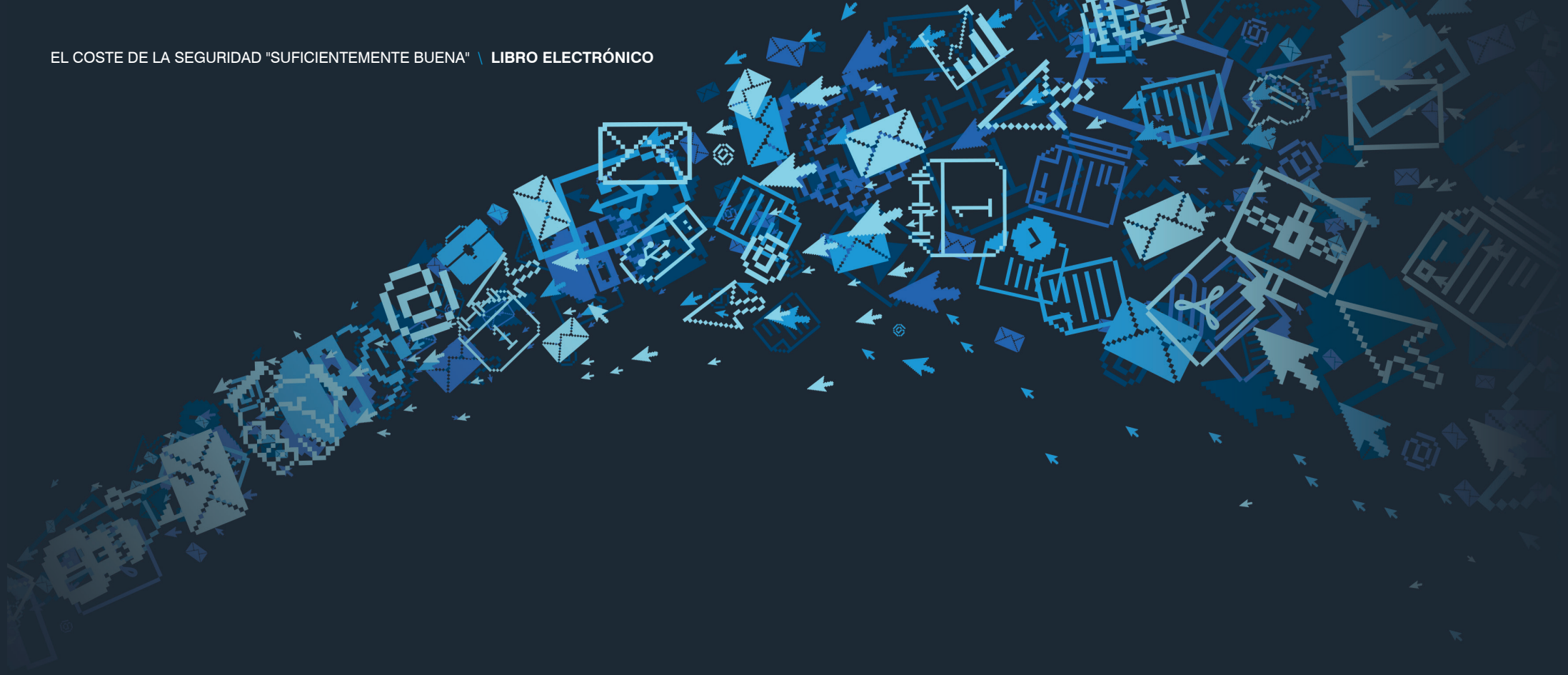
Recuerde que las integraciones con otras soluciones de seguridad proporcionarán a su equipo visibilidad imprescindible. Tenga en cuenta que esta visibilidad puede proporcionar la información que necesita para implementar controles que reduzcan el riesgo.

También es importante que ofrezcan flujos de trabajo que sean fáciles de utilizar y administrar, y bloqueo de amenazas preciso, eficaz y automatizado. En un mundo en el que escasean los profesionales de seguridad, todo lo que facilite el trabajo a los miembros de su equipo reducirá los costes laborales. Al mismo tiempo, les permitirá aportar más valor.

La visibilidad también proporciona información sobre los riesgos asociados a las personas que de otra forma podrían pasar desapercibidos. En la actualidad, los ciberdelincuentes saben que los empleados son la forma más fácil de acceder a su empresa. Esto hace que las soluciones más eficaces sean las que se centren en identificar y reducir esos riesgos. Poner la atención en los riesgos basados en las personas es la mejor estrategia para optimizar su gasto en seguridad.

Dé los pasos siguientes

Proofpoint ofrece soluciones de seguridad para el correo electrónico y la nube completas e inteligentes para proteger a sus empleados frente a las amenazas más peligrosas del momento. Para obtener más información y solicitar una evaluación rápida de riesgos para el caso particular de su empresa, **visite proofpoint.com/es**.



MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

0501-012-06-01 09/22