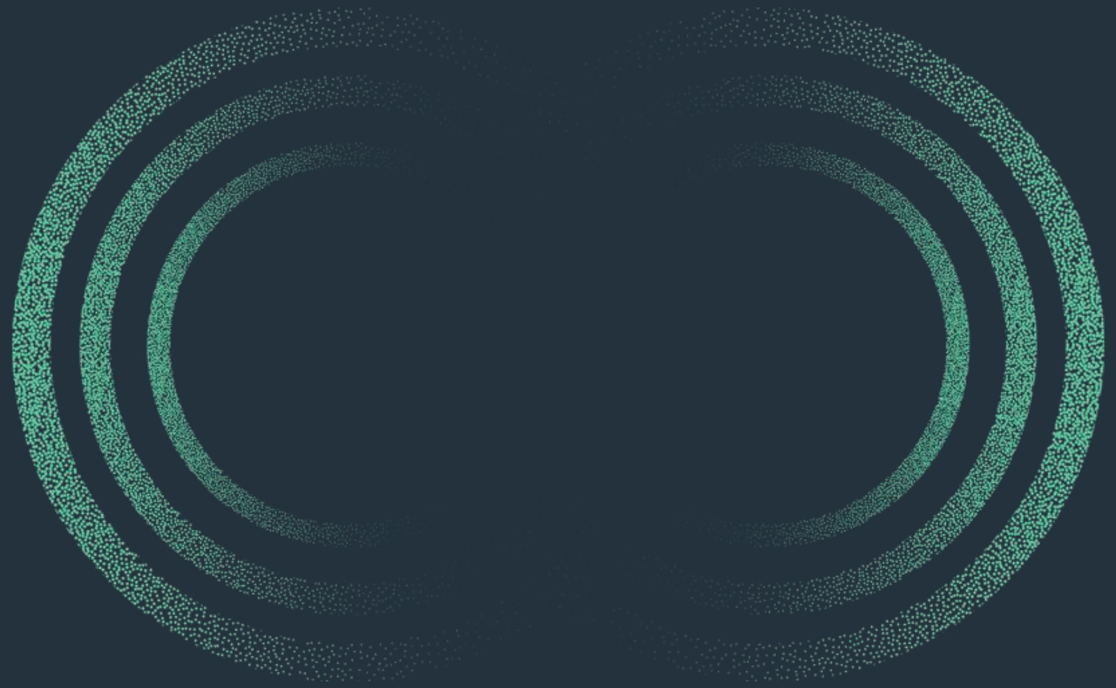
WithSecure™ Pulse 2023

Todo lo que necesita saber sobre las últimas tendencias en TI y ciberseguridad

WITH secure

Contenido



Resumen Ejecutivo

Introducción

Nuestra encuesta de investigación de mercado global hizo a miles de profesionales de TI una serie de preguntas sobre sus trabajos, organizaciones y prioridades para el próximo año. Los datos resultantes se pueden usar para informar sus estrategias de TI y seguridad en 2023 y más allá.

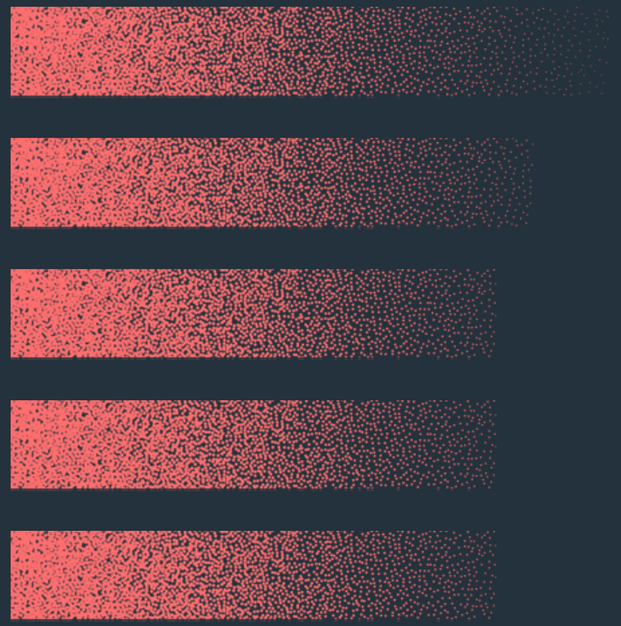
Pulse 2023 llegó a 3072 encuestados en 12 países: el Reino Unido, Francia, Alemania, Bélgica, los Países Bajos, Dinamarca, Finlandia, Noruega, Suecia, además de los EE. UU., Canadá y Japón. Todos los encuestados eran tomadores de decisiones de seguridad e influyentes en TI, redes y espacios en la nube, responsables
para comprar productos y servicios de seguridad de TI para sus organizaciones.

Para obtener los conocimientos más valiosos para usted, use nuestras funciones de personalización para ver los datos que son relevantes para su industria, región y tipo de función.

Prioridades de seguridad para 2023

Nuestros encuestados nos contaron sus principales prioridades comerciales y técnicas para los próximos 12 meses. Las cinco prioridades principales para los líderes de ciberseguridad son:

Mayores desafíos de seguridad técnica (5 respuestas principales)



34% Prevención de violaciones de datos

29% Garantizar la protección contra el malware y ransomware

27% Prevención de amenazas avanzadas basadas en correo electrónico, como phishing o compromiso de correo electrónico comercial (BEC)

27% Garantizar la seguridad de las aplicaciones de colaboración basadas en la nube, como Office 365 y Salesforce

26% Ensuring the security of an increasingly diverse pool of devices, services and software

Our deep dive article on security priorities (starting on page 10) outlines the trends we saw in our Pulse 2023 survey.

“El punto interesante es que las opciones que nadie eligió como sus prioridades son las cosas que marcan la mayor diferencia cuando se trata de la postura de seguridad; por experiencia, estas son las competencias y prácticas que faltan en muchas organizaciones”.

Peter Page, Director de consultoría de soluciones de WithSecure™

Security Spend

En medio de todo el ruido en torno a la ciberseguridad, quizás el tema más importante para las empresas es el resultado final. ¿Cuánto se supone que debemos gastar en seguridad? ¿Cualquier cantidad es suficiente? ¿Depende de cuántos asientos tenemos, nuestra ubicación geográfica o el tipo de industria en la que estamos? ¿Mis compañeros están tan preocupados por cuánto están gastando y cuánto de su presupuesto están asignando a esto?

Nuestra investigación produjo información interesante sobre cómo las organizaciones gastan en seguridad cibernética. Los datos sugieren que a medida que las empresas evolucionan su estrategia, el costo se vuelve un factor menos crítico.

86% de los encuestados dice que sus intenciones presupuestarias de seguridad aumentarán en los próximos 12 meses.

“Siempre digo que deberías empezar desde un nivel absoluto.
mínimo del 5%. Ahora, eso es sin ninguna advertencia: cuanto más vital es la seguridad para el cliente, mayor es el porcentaje. Y viceversa.“

Teemu Myllykangas, director de gestión de productos B2B en WithSecure™

“Las empresas deben decidir cuánta seguridad quieren. Deben acordar cuánto riesgo están dispuestos a aceptar, cuánta interrupción del negocio pueden tolerar y qué apetito tienen por asumir riesgos. Según lo que decidan, se pueden tomar decisiones racionales de gasto en seguridad”.

Paul Brucciani, director de marketing de productos de WithSecure™

Residencia de datos

Nuestra encuesta Pulse 2023 mostró que las personas en TI tienen opiniones firmes sobre dónde se almacenan y procesan los datos de su organización. No es sorprendente: las reglas y regulaciones sobre los datos, y muchos ejemplos de uso indebido y abuso de datos, hacen que este tema tenga muchas consecuencias y sea emotivo para muchos.

Las opiniones tendían a diferir entre personas de organizaciones de diferentes tamaños, así como entre quienes trabajaban en diferentes regiones e industrias.

Cuando hay tanto desacuerdo sobre la forma correcta de manejar los datos, ¿cómo se puede llegar a un consenso? ¿La política de residencia de datos de una organización afecta su relación
¿con clientes? La mayoría de las veces, los reguladores y los defensores de la privacidad son influencias poderosas.

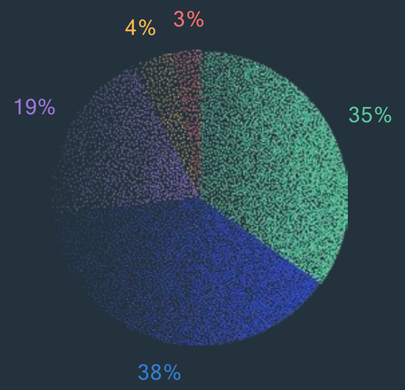
Quizás la pregunta más importante es por qué existen las diferencias de opinión. Los desacuerdos y malentendidos pueden causar problemas, particularmente entre personas influyentes de TI y quienes toman las decisiones en la misma organización. Cuando se trata de privacidad y protección, no hay lugar para el error.

“La residencia de datos es algo que debe considerar como empresa que opera hoy. La razón es que es posible que tenga clientes que se preocupan por los problemas de seguridad nacional y usted, como empresa nueva, por ejemplo, podría haber proporcionado su software como un producto de servicio utilizando proveedores de servicios en la nube estadounidenses. ¿Es algo que puedes seguir haciendo, puedes seguir innovando al mismo ritmo que antes, o tienes que encontrar una solución alternativa a eso?
Eso es algo que debes considerar”.
Albert Koubov González, Consultor, WithSecure™

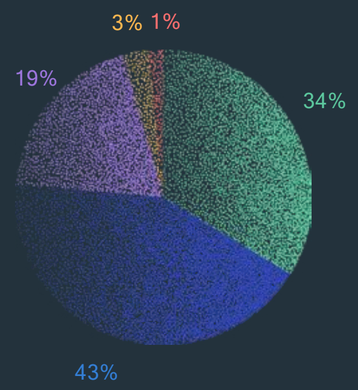
Dónde guardas los datos

¿Qué importancia tiene la ubicación geográfica para el procesamiento de datos en su función?

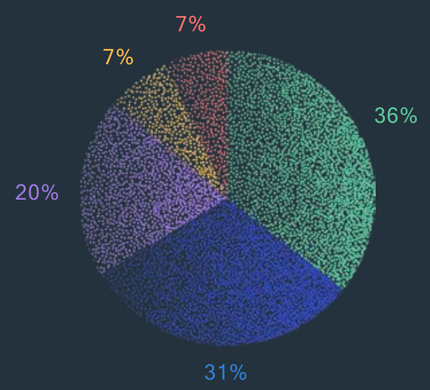
Total



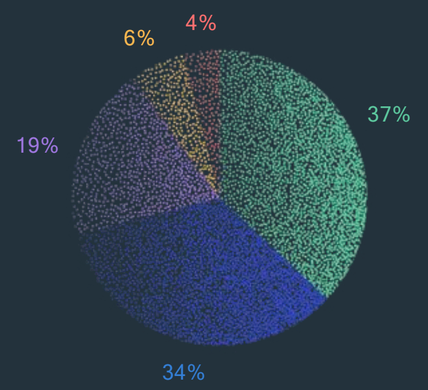
Decisores de TI



IT influencers



Top management



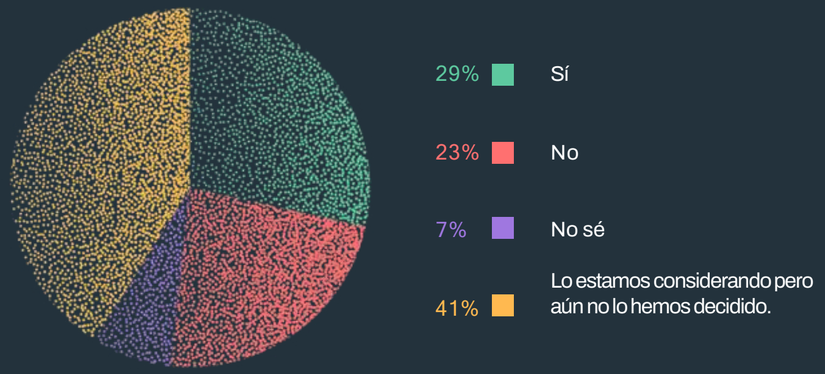
- Los datos deben ser procesados dentro del mismo país que nuestras operaciones.
- Los datos deben procesarse dentro de la misma región (por ejemplo, UE, América del Norte, APAC) que nuestras operaciones
- No tiene importancia dónde procesamos los datos de nuestros clientes finales, siempre que se cumplan todos los requisitos legales y de cumplimiento pertinentes.
- No procesamos datos para clientes finales.
- No sé

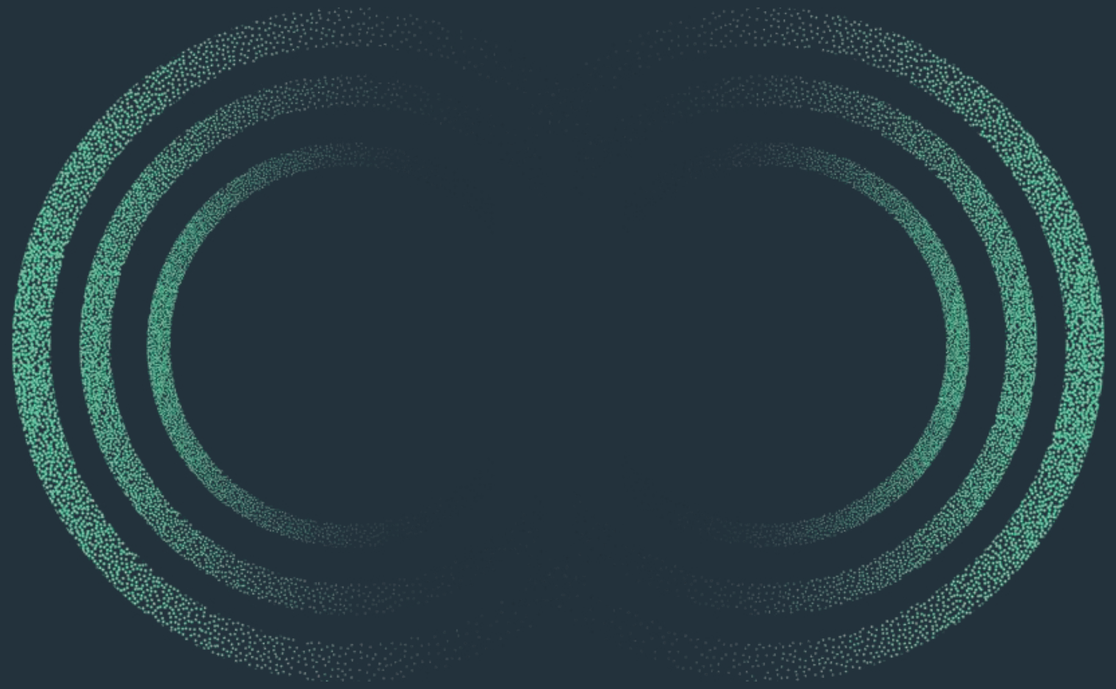
Migración de proveedores

Cambiar de proveedor de seguridad es una empresa enorme. Es una gran inversión de tiempo y recursos. A pesar de esto, nuestra encuesta Pulse 2023 muestra que más del 30 % de los encuestados cambió de proveedor en los últimos seis meses, y la misma proporción planea cambiar de proveedor en los próximos seis meses.

Esto indica que se está produciendo una ola masiva de migración de proveedores. ¿Por qué - y cuál - será el costo?

¿Su empresa/organización planea cambiar su solución/proveedor de seguridad de TI comercial en los próximos seis meses?

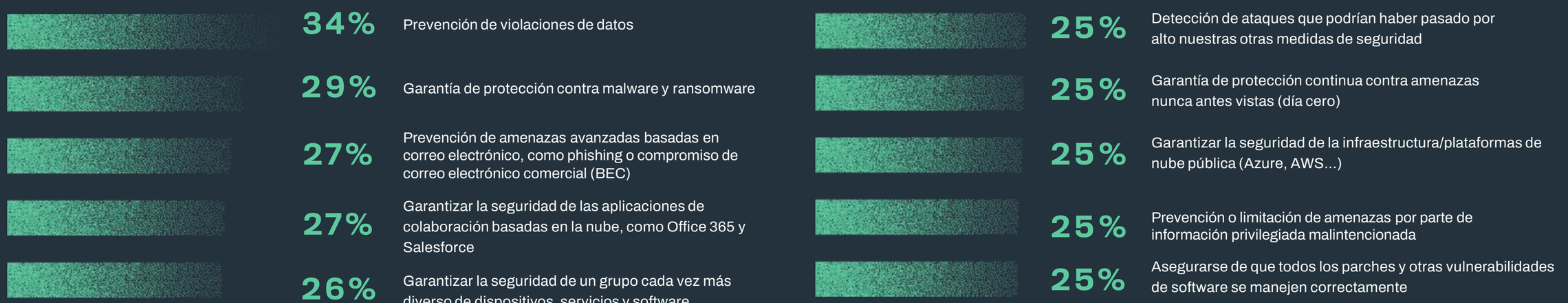




1. Prioridades de seguridad para 2023

Prioridades de seguridad técnica

Mayores prioridades de seguridad técnica

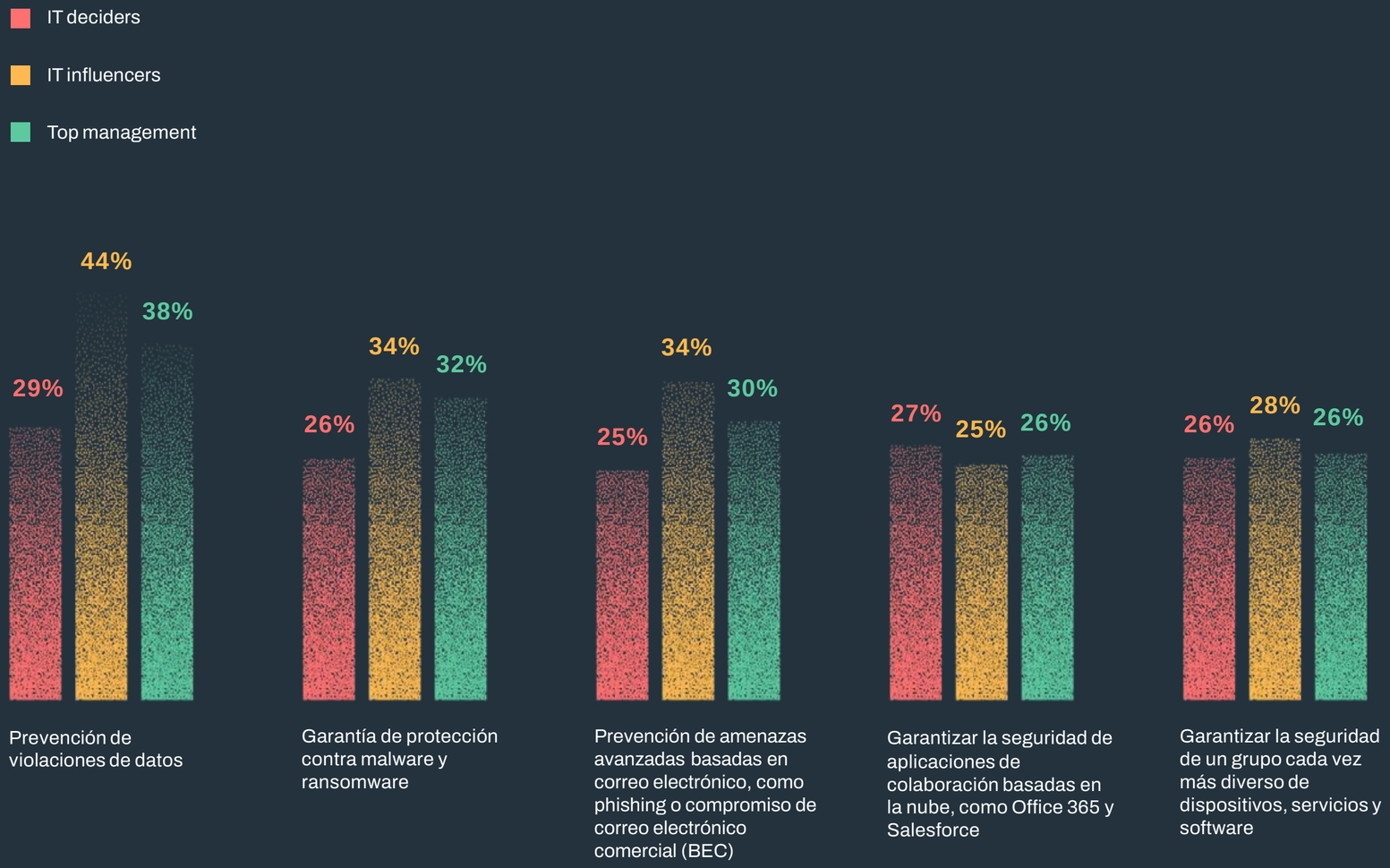


Los resultados muestran que hubo un amplio consenso sobre qué prioridades técnicas son las más preocupantes. El principal desafío es previsiblemente 'prevención de violaciones de datos' (33.7%).
Prevención de amenazas basadas en correo electrónico y garantizar la seguridad de las aplicaciones de colaboración basadas en la nube, como Office 365 y Salesforce, también obtienen una puntuación alta en la lista. Las otras prioridades que se eligieron generalmente se ajustan al tema de la detección y respuesta a amenazas.

"El punto interesante es que las cosas que hacen la mayor diferencia cuando se trata de la postura de seguridad no están entre las principales prioridades; por experiencia, estas son las competencias y prácticas que faltan en muchas organizaciones. Todo el mundo se preocupa por prevenir ataques utilizando soluciones como *EDR* y *consultoría*, *pero ambos son cruciales. EDR es algo que debe estar en su lugar además de EPP para crear una solución estanca. Además, las cosas de BAU que tienen un impacto real y duradero se pasan por alto porque deben ser impulsadas internamente y, a menudo, es un trabajo muy difícil: construir una cultura de seguridad no es algo que se pueda subcontratar".*

—Peter Page, director de consultoría de soluciones de WithSecure

Top 5 de los principales desafíos técnicos 2022/3 divididos por el tipo de rol

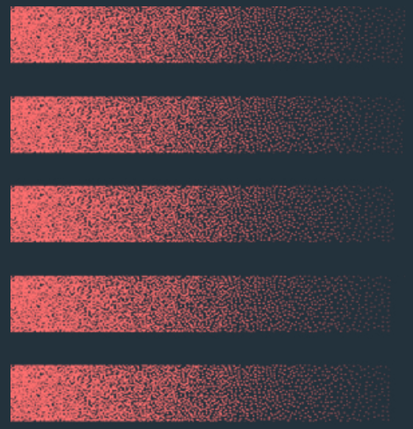


Estos datos muestran las proporciones de decisores de TI, personas influyentes de TI y alta dirección que priorizan las cinco principales prioridades técnicas generales en 2023. Una vez más, parece haber un amplio acuerdo entre nuestros encuestados sobre cuáles son las prioridades más importantes.

Ahora mismo lo son. Cuando haya discrepancias (por ejemplo, entre los decisores de TI y los influyentes de TI sobre la "prevención de violaciones de datos"), podría valer la pena verificar y asegurarse de que todos en su equipo de seguridad estén en la misma página.

Resultados de seguridad empresarial

Los mayores desafíos empresariales



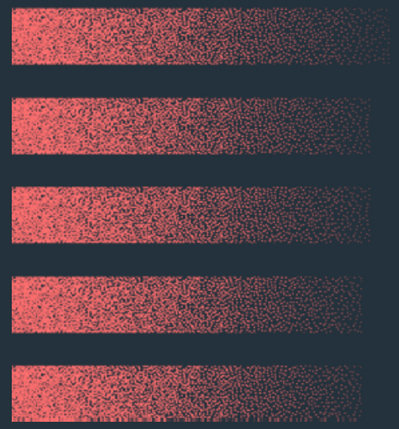
25% Proteger a la fuerza laboral en el trabajo remoto/híbrido

24% Aumente la velocidad y la eficacia para responder a los incidentes de seguridad cibernética

23% Aumentar la comprensión de las amenazas/riesgos de seguridad cibernética y la conciencia de seguridad en toda nuestra organización

23% Continuidad empresarial segura sin interrupciones

23% Crear una fuerte cultura de "primero la seguridad" en nuestra organización



23% Abordar las nuevas amenazas de seguridad introducidas por la cloudificación

22% Minimice el trabajo manual y aligere la carga de trabajo del equipo de seguridad de TI

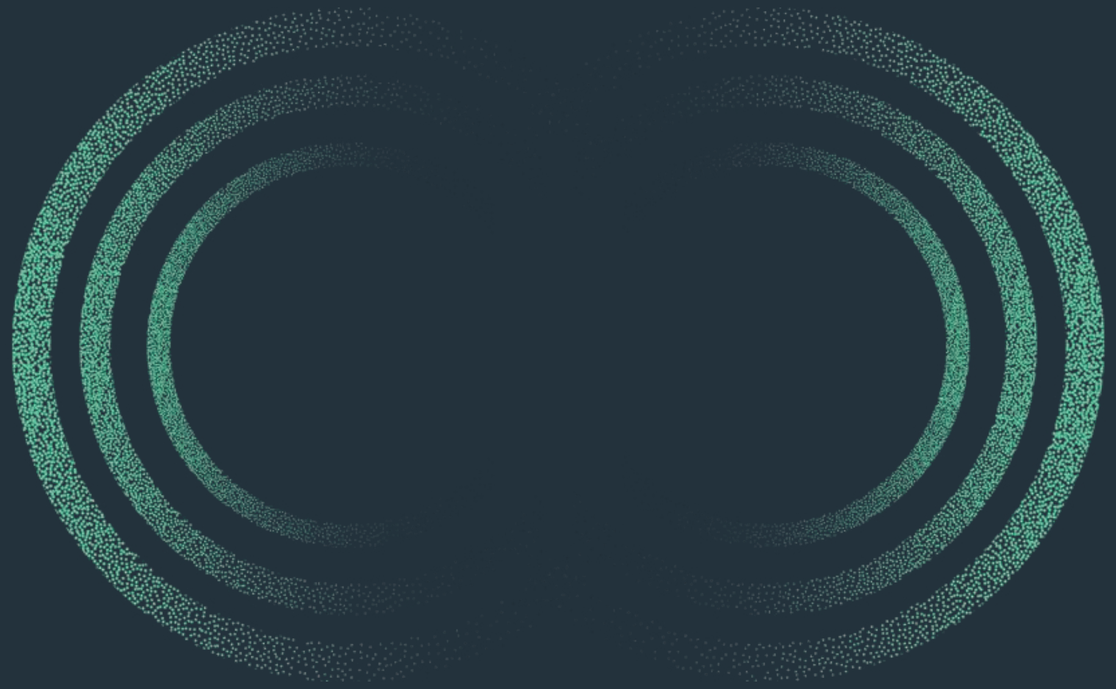
22% Aumente la flexibilidad para adaptar la seguridad de TI en un mundo incierto

22% Reduzca el costo y el impacto de los incidentes cibernéticos mediante medidas de recuperación efectivas

21% Asegúrese de que sus herramientas de seguridad se ajusten a los planes a largo plazo de su organización

"No es sorprendente que las personas estén más preocupadas por el desafío de asegurar a los trabajadores remotos. Hubo un cambio masivo en las formas de trabajar en 2020, y ha habido mucha orientación y asesoramiento en esta área para ayudar a las organizaciones a adaptarse. Eso ha significado proyectos a gran escala para muchas personas, lo que implica cambiar la arquitectura de TI (por ejemplo, migrar a la nube) y reeducar a los empleados. Pero si bien esto es obviamente una preocupación frecuente en este momento, espero que para cuando se repita esta encuesta en 2024/5, la mayoría de las organizaciones habrán llegado a un punto estable en el que se hayan adaptado y todos estén acostumbrados a las nuevas formas de trabajo."

- Peter Page, director de consultoría de soluciones de WithSecure



2. Gasto en seguridad

¿Cuánto debería gastar en seguridad?

Es una pregunta que se hacen miles de empresas en todo el mundo, pero ¿cuánto de su presupuesto de TI debe reservarse para la ciberseguridad?

Se espera que el mercado mundial de seguridad de la información tenga un valor de USD 174 700 millones para 2024. Esta es una estadística sorprendente que muestra la creciente importancia de la ciberseguridad a medida que el mundo continúa cambiando. Esto sugeriría que las empresas están reaccionando a la amenaza planteada invirtiendo más en su seguridad..

Debido a una serie de factores, como atacantes más sofisticados, el trabajo remoto continuo y la situación geopolítica global, ¿cuánta seguridad es suficiente y cuánto deben pagar las empresas para obtenerla?

La investigación de WithSecure reveló que el 87,9% de las empresas con sede en la UE planean aumentar su presupuesto de seguridad en los próximos 12 meses. Quizás lo más sorprendente fue que el 8,3% siente que está adecuadamente cubierto o buscará activamente reducir su gasto en ciberseguridad.

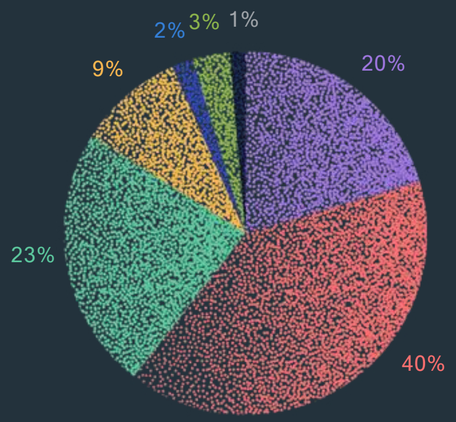
También parece haber una desconexión entre los grupos en cuanto a cómo será el presupuesto para el próximo año; mientras que los encuestados de los Decisores de TI y la Alta Dirección parecen estar en sintonía, los Influyentes de TI a veces tienen expectativas presupuestarias significativamente diferentes. La comunicación temprana y clara a sus partes interesadas sobre este tema es vital para evitar confusiones o tomas de decisiones de última hora.

Teemu Myllykangas, director de gestión de productos B2B en WithSecureTM, está bien versado en esta área. *“Cuando le preguntas a una empresa si están gastando lo suficiente, les cuesta mucho responder. Si dicen que sí, entonces cualquier incumplimiento volverá a morderlos con fuerza, ya que la gente querrá saber cómo estaban incumplidos a pesar de la inversión que se suponía debía protegerlos. Si dicen que no, entonces esas mismas personas deberían preguntarse si están haciendo su trabajo correctamente y asegurando el negocio. No hay una respuesta fácil a esta pregunta: cualquiera que diga lo contrario está mintiendo o tratando de venderle aceite de serpiente”.*

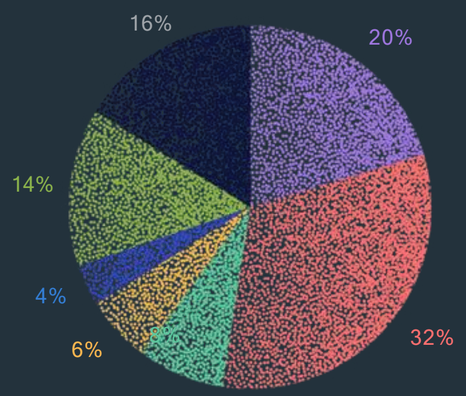
Dentro de la industria, generalmente se acepta que las empresas gastan entre el 3% y el 15% de su presupuesto en seguridad cada año. Cuando los clientes lo presionan sobre dónde deberían caer en esta categoría, Myllykangas se muestra cauteloso. “Siempre digo que debes comenzar con un mínimo absoluto del 5%. Ahora, eso es sin ninguna advertencia: cuanto más vital es la seguridad para el cliente, mayor es el porcentaje. Y viceversa. Por lo general, lo divido en tres pasos: comenzar con la evaluación de riesgos y modelado de amenazas para definir el ROI, decidir cómo usar ese dinero de una manera adecuada utilizando un marco de seguridad básico bien conocido; revise los números uno y dos anualmente para identificar el punto de rendimiento decreciente y administre su presupuesto”.

Intenciones presupuestarias de seguridad por rol

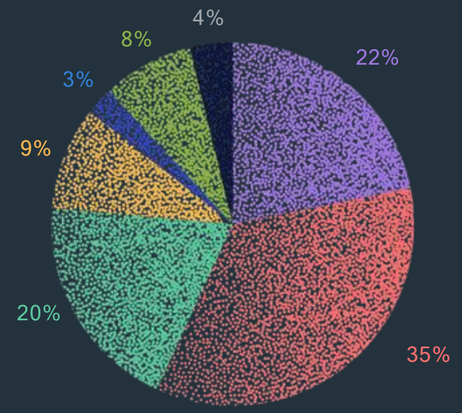
IT deciders



IT influencers



Top management



- En los próximos 12 meses nuestro presupuesto aumentará en un 1-5%
- En los próximos 12 meses nuestro presupuesto aumentará en un 6-10%
- En los próximos 12 meses nuestro presupuesto aumentará en un 11-15%
- En los próximos 12 meses nuestro presupuesto aumentará más de un 15%
- En los próximos 12 meses nuestro presupuesto disminuirá
- En los próximos 12 meses nuestro presupuesto no aumentará ni disminuirá
- No sé

La evaluación de riesgos es crucial

Es muy difícil crear una regla general para determinar la suficiencia del gasto en seguridad. Hay demasiadas variables. Como proporción del presupuesto de TI, puede haber una diferencia de hasta diez veces, según las circunstancias. Hace unos cinco años, el porcentaje de gasto en seguridad era de aproximadamente el 10 % del presupuesto de TI de una empresa, pero ha aumentado desde entonces. Las empresas para las que la seguridad es de vital importancia gastan entre un 12 % y un 15 % de su presupuesto de TI en seguridad", afirma Paul Brucciani, director de marketing de productos de WithSecure™.

La primera pregunta que debes hacerte es: ¿qué te amenaza? Entonces, si ocurriera el peor de los casos, ¿cuál sería la consecuencia? Debe averiguar qué es una expectativa de pérdida anual (ALE) y la probabilidad de que esto suceda.

Aquí es donde entra WithSecureTM, ya que una empresa generalmente no sabrá cuál es la respuesta a la pregunta. Con una experiencia significativa en respuesta a incidentes, podemos trazar el ALE contra los factores de riesgo y determinar cuánto debería gastar esa empresa en seguridad.

"Una vez que haya identificado su riesgo, debe determinar qué hacer con estos riesgos y hay tres opciones. Primero, puede transferir los riesgos, lo que implicaría, por ejemplo, tomar un seguro cibernético. En segundo lugar, puede reducir el riesgo utilizando controles, tecnologías y servicios de seguridad adecuados.

Finalmente, puedes simplemente aceptarlo, vivir con eso y lidiar con las cosas cuando sucedan", continúa Brucciani.

"Esencialmente, está viendo cuánto puede reducir el riesgo y, por lo tanto, hace un juicio de valor sobre cuánto de su presupuesto necesita reservar para la seguridad. Debe decidir cuánto riesgo está dispuesto a aceptar, su nivel de tolerancia al riesgo y si su empresa tiene la capacidad de absorberlo", según Brucciani.

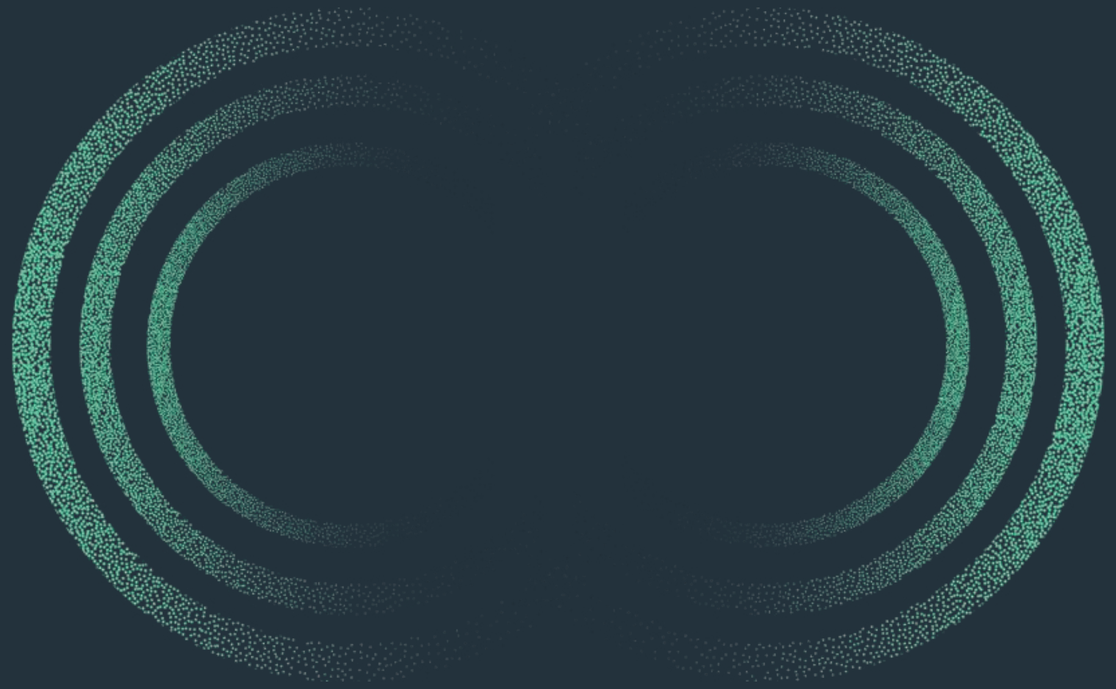
Estos son temas sobre los que el CFO debe decidir. Solo así podrá determinar presupuestos, montos de contingencia y cómo enfrentar los riesgos.

No simplemente relacionado con los costos

Es importante señalar que asegurar su empresa va mucho más allá del costo. Existen numerosos factores y la investigación de WithSecure ha demostrado exactamente este punto. Solo el 13,2% de los encuestados en la encuesta de WithSecure dijo que el precio más bajo es el aspecto más crítico al seleccionar un proveedor. Por el contrario, más de una quinta parte (21,8 %) cree que el soporte 24/7 es el aspecto más crítico, y otro 16,7 % busca confiar en un proveedor.

Si bien no existe una bala de plata cuando se trata de decidir cuánto debe gastar en seguridad, WithSecure™ puede proporcionar un camino lógico y defendible que puede tomar para garantizar que su empresa esté tan bien protegida como sea posible. Además, si bien el precio es y siempre será un problema importante, la seguridad va mucho más allá del resultado final.

WithSecure™ Elements puede ayudarlo a reducir el riesgo, la complejidad y la ineficiencia. Combina poderosas capacidades de seguridad predictiva, preventiva y receptiva, todo administrado y monitoreado a través de un único centro de seguridad.



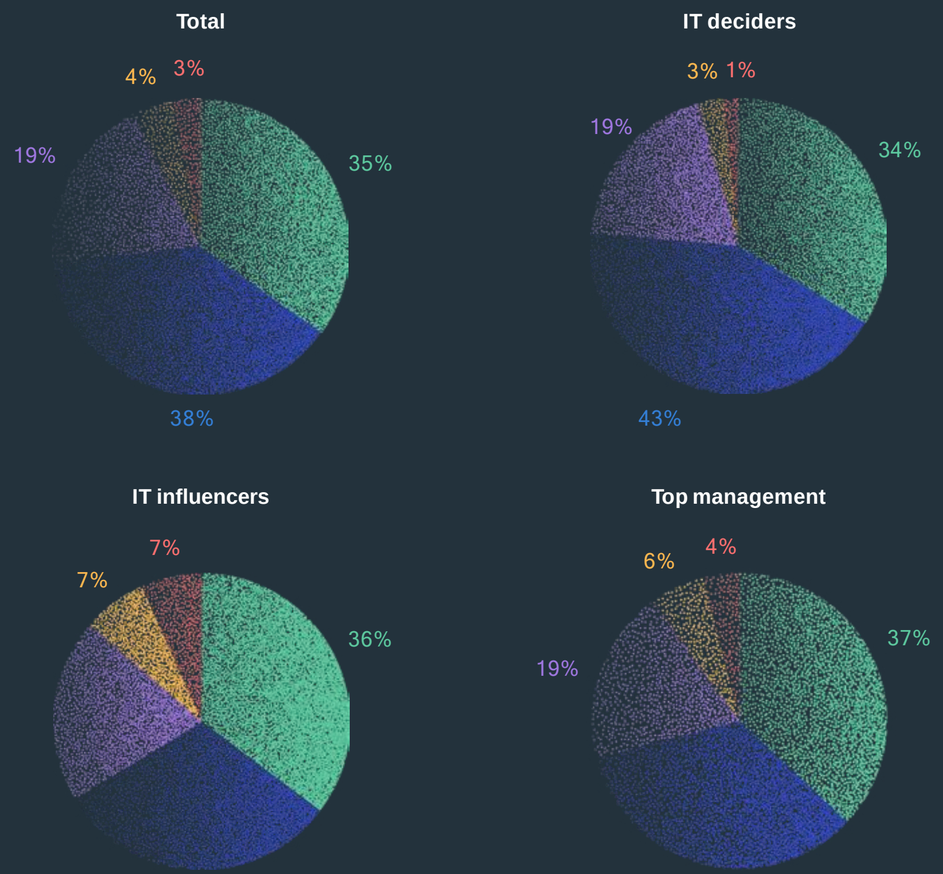
3. Datos residencia

¿Sabes dónde están tus datos?

A la gente realmente le importa dónde se almacenan y procesan sus datos.

Los resultados de nuestra encuesta Pulse 2023 destacan un gran interés en dónde se almacenan y procesan los datos. Casi el 73 % de los encuestados dijo que sus datos deben procesarse dentro del mismo país o región donde opera. Menos de una quinta parte dijo que esto no tenía importancia.

¿Qué importancia tiene la ubicación geográfica para el procesamiento de datos en su función?



- Los datos deben ser procesados dentro del mismo país que nuestras operaciones.
- Los datos deben procesarse dentro de la misma región (p. ej., UE, América del Norte, APAC) como nuestras operaciones
- No tiene importancia dónde procesamos los datos de nuestros clientes finales, siempre que se cumplan todos los requisitos legales y de cumplimiento pertinentes.
- No procesamos datos para clientes finales.
- No sé

Dónde guardas los datos

Cuando se desglosaron estas respuestas, surgió una desconexión. El 42,8 % de los decisores de TI ven el procesamiento regional como un requisito, en comparación con solo el 30,9 % de los influyentes de TI. Esta respuesta sugiere que la cuestión del procesamiento regional o nacional no está bien definida, o que diferentes grupos tienen diferentes prioridades.

Los tamaños específicos de las empresas (500-999 y más de 5000 empleados) prefieren el procesamiento regional, y más encuestados están de acuerdo en que no es importante dónde terminan los datos del cliente.

Este sentimiento varía según el tamaño de la empresa: los encuestados de organizaciones más grandes tenían más probabilidades de decir que pensaban que los datos debían procesarse en la región que de pensar que no tenían importancia.

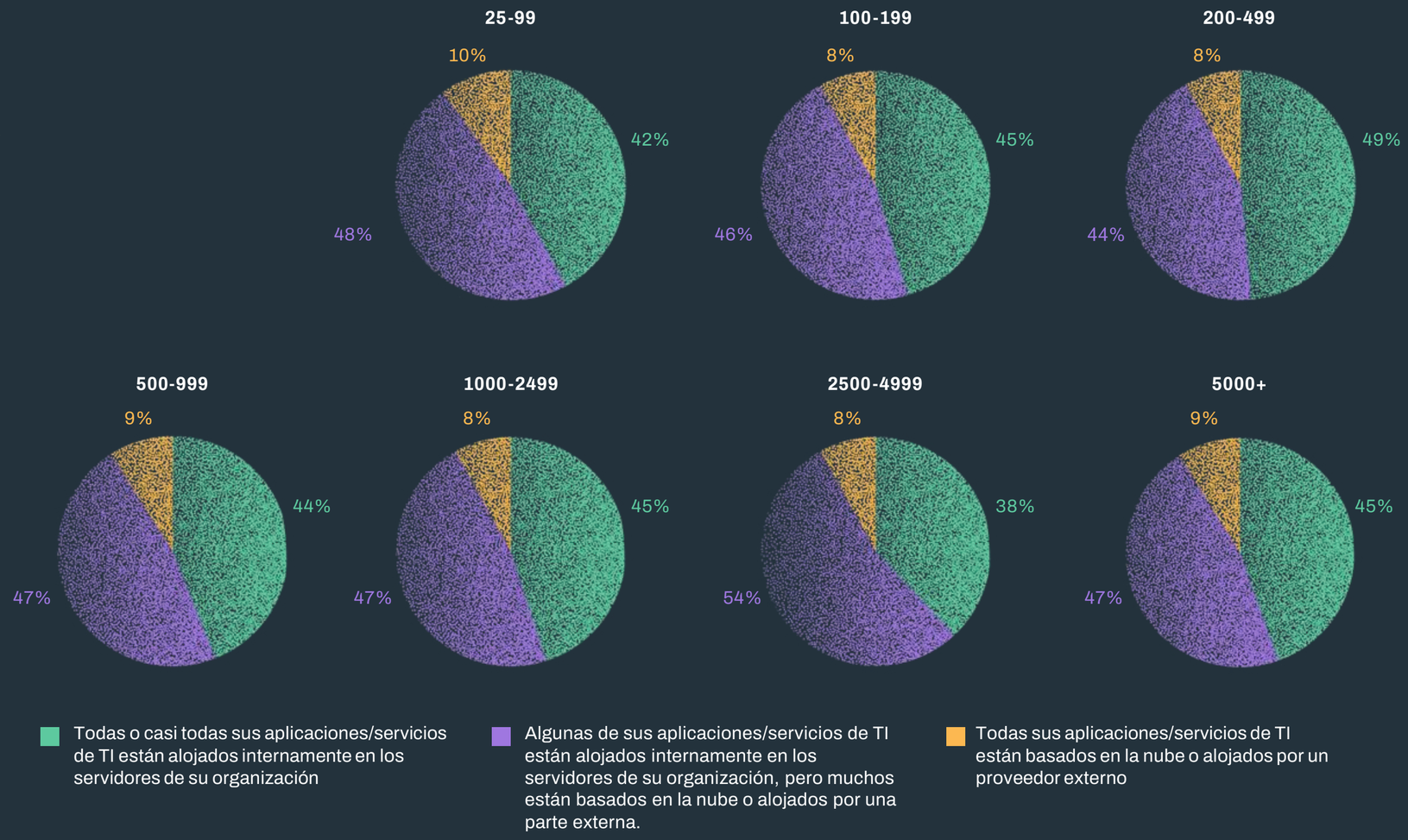
La preferencia por una fuerte residencia de datos puede ser el resultado de una agitación y un cambio significativos, tanto en términos de reglas como de eventos físicos. La soberanía de los datos, las reglas por las cuales los países individuales manejan los datos dentro de sus fronteras, se ha enfrentado entre fuerzas que compiten, incluida la globalización de la informática y el procesamiento de datos, la regulación regional, la geopolítica, la guerra y la agitación política y el consiguiente deseo de reducir el riesgo. Todo esto se suma a un enfoque profundo en dónde se encuentran los datos de uno y hacia dónde se mueven o a través de ellos.

Dónde procesas los datos

Aquí es donde se vuelve un poco contradictorio: constantemente nos dicen Cloud Changes Everything™, pero no parece influir en las actitudes de nuestros encuestados.

Independientemente de si las aplicaciones tenían más o menos probabilidades de estar alojadas internamente o en la nube en una organización, las actitudes seguían siendo las mismas. Las organizaciones de más de 2500 empleados (y las organizaciones de América del Norte) eran ligeramente más propensas a alojar aplicaciones en el sitio, mientras que los daneses, suecos,
Los alemanes y los encuestados del Reino Unido tenían más probabilidades de estar más en la nube que en las instalaciones. Burbujeando entre el 12,1 % y el 6,2 % estaban esos tipos extraños con visión de futuro que hacían todo en la nube.

Entorno de TI por tamaño de empresa

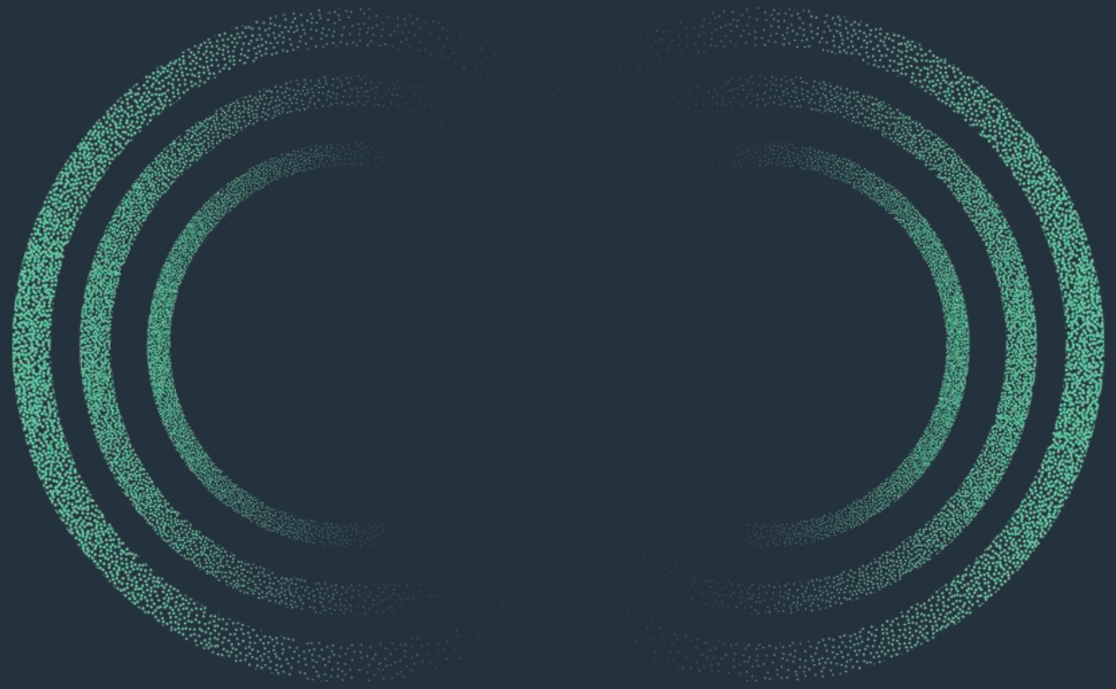


Conclusiones y Recomendaciones

La residencia es importante, algo que nuestros clientes de Countercept MDR expresaron tanto el año pasado que presentamos una versión de Countercept solo para Europa para cumplir con sus requisitos. Las palancas y los impulsores de este deseo son complejos, pero es interesante que haya un amplio consenso entre los encuestados de todas las tendencias.

En última instancia, depende de las organizaciones individuales cumplir con los requisitos reglamentarios y garantizar que sus clientes estén bien atendidos. Los aspectos prácticos de esto pueden ser complejos, por decir lo menos.
Abandonar la nube y cambiar al almacenamiento y procesamiento de datos en las instalaciones conlleva sus propios gastos generales de cumplimiento, seguridad y técnicos. El consejo de nuestros consultores es seguir los requisitos reglamentarios nacionales de protección de datos en primera instancia y luego agregar las inquietudes y los requisitos de los clientes.

La única área que puede requerir una acción significativa es la comunicación interna: entre los tipos de Decisores de TI y los influyentes más estratégicos y la alta dirección, existe cierta desconexión en torno al procesamiento de datos regionales. Comprender las diferencias entre los requisitos nacionales y regionales, y por qué estas diferencias de opiniones parecen existir en las organizaciones, deben ser un área de investigación inmediata para los lectores.



4. Cambiando la seguridad cibernética vendedores

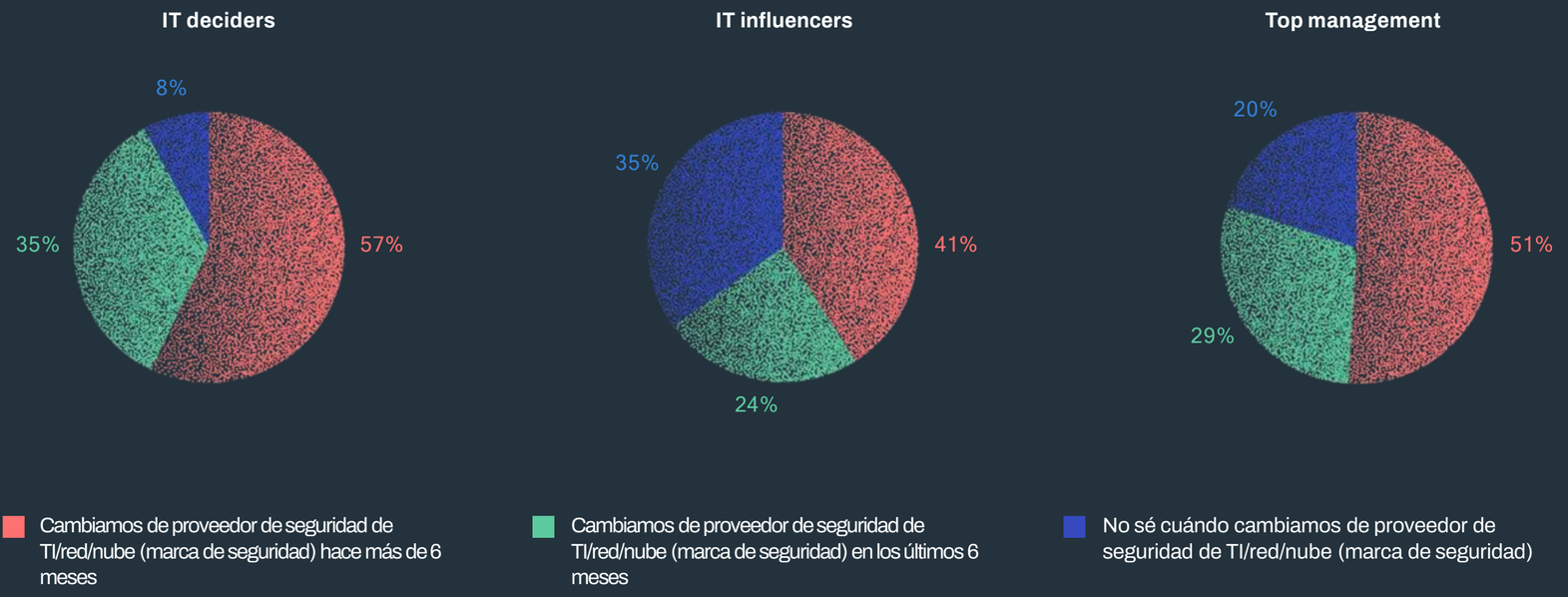
El cambio de proveedor es la constante

Todo es cambio para las organizaciones de seguridad, o mejor dicho, para sus proveedores.

Nuestra encuesta muestra que casi un tercio (31,9 %) había cambiado de proveedor de seguridad en los últimos seis meses, mientras que el 32 % esperaba cambiar de proveedor o solución de seguridad de TI en los próximos seis meses.

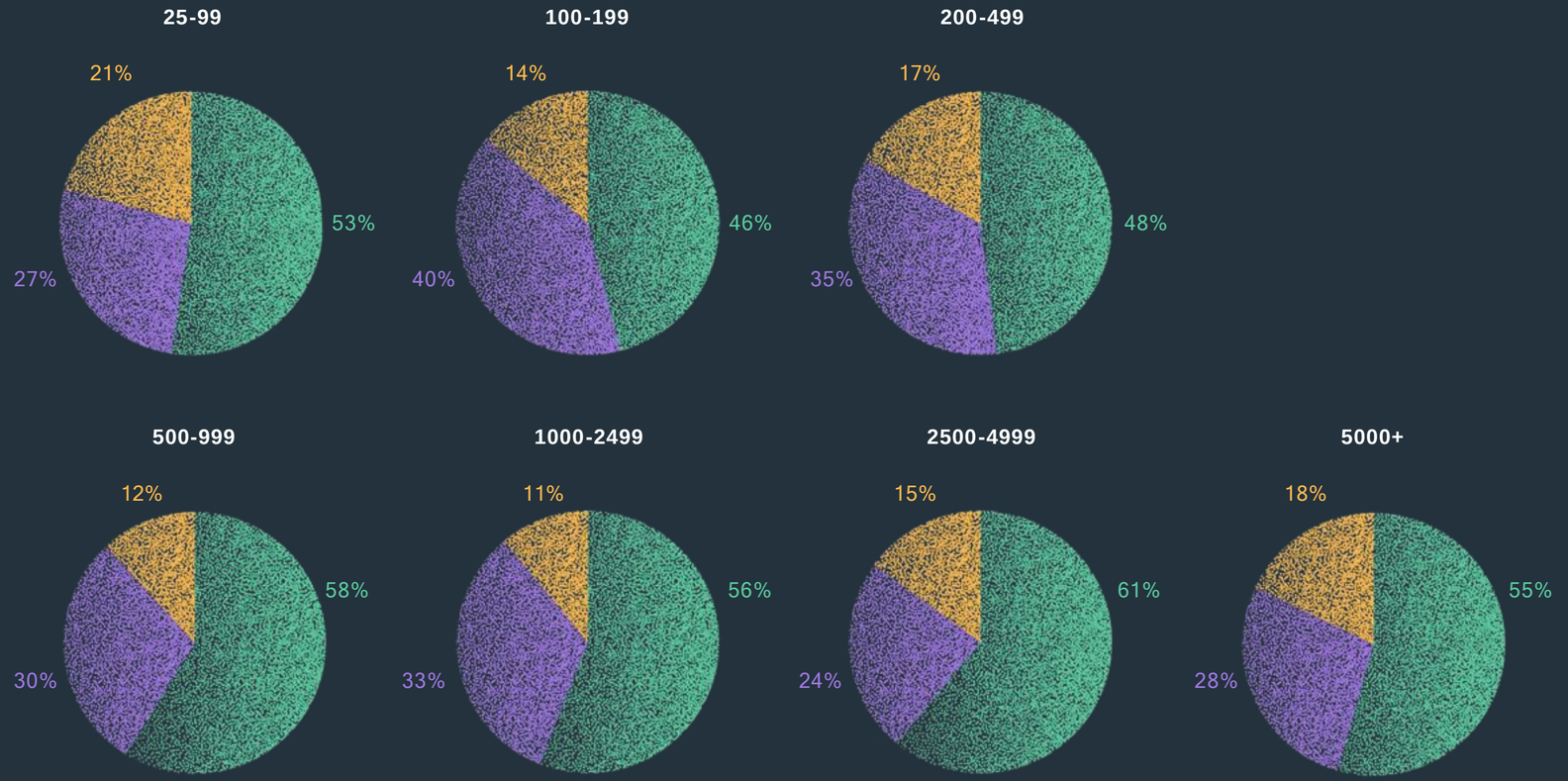
Los encuestados en los sectores de finanzas y seguros y servicios de TI y tecnología tenían más probabilidades de haber cambiado de proveedor hace más de seis meses (59,4 % y 58,4 % respectivamente) y más probabilidades de esperar cambiar en los próximos seis meses, a un ritmo del 45% y 41,1% respectivamente.

Intenciones y criterios de cambio de proveedor de marca por tipo de rol



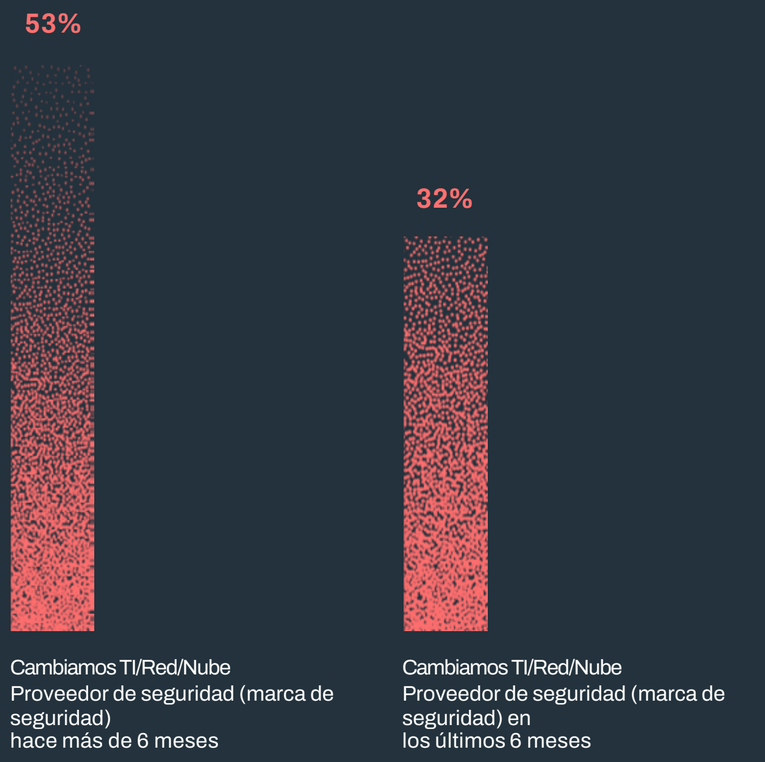
Mirar esto desde la perspectiva del tamaño de la empresa (n=1800) sugiere mucho más movimiento en las pequeñas y medianas empresas que en las organizaciones más grandes.

Intenciones y criterios de cambio de proveedor de marca según el tamaño de la empresa

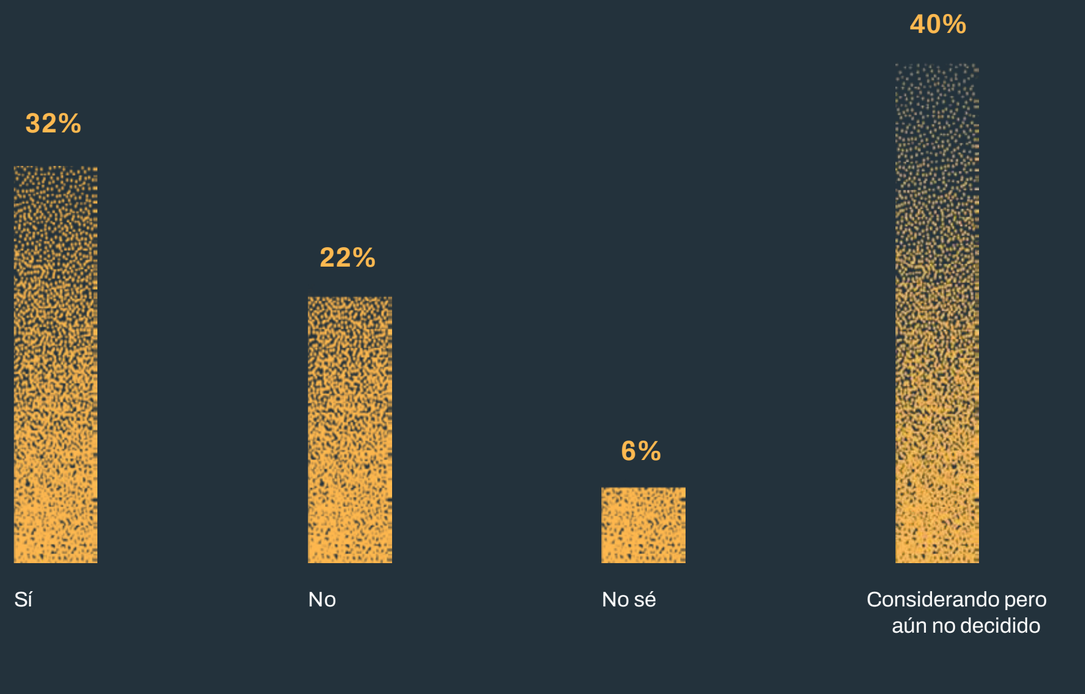


Si bien "todo cambio" puede ser la norma para muchas organizaciones, saltando entre diferentes proveedores de forma continua, este proceso es complicado y requiere mucho tiempo. Le pedimos al jefe de consultoría de soluciones de WithSecure, Peter Page, que nos diera su opinión sobre cómo las empresas abordan el cambio de proveedor. También exploramos la clave para generar y mantener la confianza entre los proveedores y sus clientes.

Con respecto a un cambio de proveedor de seguridad de TI/red/nube (marca de seguridad)



¿Su empresa planea cambiar su proveedor de seguridad de TI comercial en los próximos 6 meses?



¿Qué es lo que más temen los clientes de los proyectos de transición?

Los recursos finitos o limitados son enemigos familiares, y hacen que el esfuerzo necesario para cambiar de un proveedor a otro sea un esfuerzo abrumador para muchas organizaciones. Simplemente: a veces es demasiado esfuerzo deshacerse de un proveedor de bajo rendimiento. Este ya no es el caso, a juzgar por lo que nos dijeron nuestros encuestados.

“Los equipos de seguridad a menudo no son las personas que implementan nuevos servicios”, dice Page. “Deben apelar al proyecto equipos de administración (y) TI para implementar el software, tienen que confiar en el equipo de redes, ya que el cambio que están realizando está afectando a más partes del negocio de las que son responsables, y tienen que obtener la aceptación de todas las diferentes partes interesadas”.

¿La llegada de los servicios en la nube facilita el cambio?

Hemos hablado antes sobre las cambiantes necesidades y desafíos de seguridad de la nube. Cambiar de proveedor es cada vez más fácil, pero no por la naturaleza de la nube: los usuarios se sienten más cómodos cambiando entre servicios en la nube, como lo harían entre servicios locales.

Para Page, todo se reduce a las personas: “Ahora hay un gran grupo de talentos que tienen habilidades para desarrollar, implementar y asegurar la nube. Los proveedores de seguridad también deben tener esa capacidad. Pero a medida que cambia su perímetro, cambia su servicio de seguridad, y está ayudando a los clientes a comprender ese riesgo y ahí es donde entran cosas como la gestión de la postura de seguridad en la nube”.

¿Por qué la duración de los contratos es cada vez más corta?

Es probable que los contratos más cortos sean el resultado de dos factores: el estado de los productos y servicios en el mercado de la seguridad cibernética y la tendencia hacia plazos más cortos para los directores de seguridad de la información (CISO). Estos gerentes senior de seguridad de TI generalmente pasan menos de dos años en una organización antes de continuar.

A medida que van y vienen nuevos CISO, esto puede impulsar un patrón de requisitos y decisiones en constante cambio y es probable que contribuya en parte a esta inestabilidad en el mercado y al consiguiente cambio regular de proveedores.

"También hay un impulso constante hacia esta 'cosa nueva' o la siguiente mejor, y esa es la forma en que el mercado está impulsando los comportamientos", dice Page. “A veces, los recursos que se invierten en comprar lo último y lo mejor pueden gastarse mejor en lo básico, o en ajustar lo que ya tiene”.

“Debido a la cantidad de ruido en el mercado, es difícil entender cuál es el mejor enfoque. Un CISO que se comprometa con un servicio costoso de varios años debe estar seguro de que obtener los resultados que necesitan, y los resultados que su directorio está buscando”.

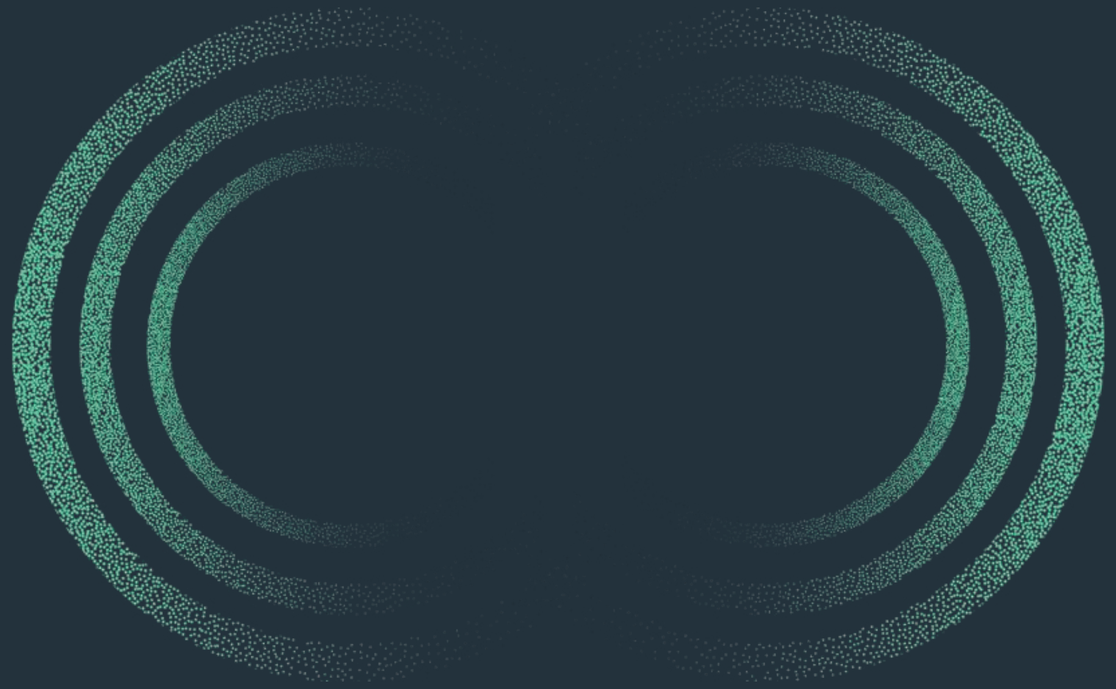
¿Se está volviendo más difícil o más fácil para los CISO tomar la decisión de hacer la transición?

“Solía ser difícil para un CISO obtener la aceptación de la junta para gastar mucho en seguridad cibernética. Ahora es más fácil: la junta directiva, el CFO y el CEO están viendo filtraciones e infecciones de ransomware en las organizaciones y pueden apreciar el impacto financiero y de resultados.

“Pero, debido al estado del mercado, hay tantas formas diferentes en que los CISO pueden abordar el problema: ¿Dónde gastan su dinero? ¿Internalizan o subcontratan? ¿Qué pasa con MDR versus EDR versus SIEM versus algo más? Entonces, es casi como 'análisis-parálisis'. Hay demasiadas opciones, y eso significa que pasan mucho tiempo haciendo RFI, hablando con los proveedores; se convierte en un trabajo de tiempo completo solo para hacer eso”.

El tiempo es la esencia

A pesar del ruido en el mercado actual de ciberseguridad, Page infiere que, por el bien de la seguridad, cualquier decisión es mejor que ninguna: “Si vas de la nada a algo, entonces tomar una decisión es importante porque no tienes visibilidad o cobertura. de tu patrimonio, Pero en los servicios gestionados, la finalización del contrato es la fecha límite. La pregunta es: ¿qué tan pronto comienza a hablar con proveedores alternativos? A los CISO les va bien cuando miran 12 meses antes de la fecha de finalización de su contrato y comienzan a pensar en sus opciones, y ahí es donde vemos los mejores resultados”.



4. Cambiando la seguridad cibernética vendedores

La encuesta de este año toma bastante tiempo para digerir. Está claro que quienes toman las decisiones sobre ciberseguridad tienen opiniones y expectativas diversas. Clasificar los datos para encontrar lo que es procesable, en lugar de lo que es meramente interesante, es complicado. Dicho esto, estas son las ideas que creemos que son más relevantes. Algunos, inevitablemente, ya son claros para los lectores informados, pero vale la pena repetirlos, y nuestros datos también respaldan estas inferencias.

1) Las prioridades percibidas pueden no ser las que marcan la mayor diferencia en la postura de seguridad. Compruebe qué prácticas y competencias le faltan a su organización y compárelas con las prioridades percibidas. Busque discrepancias.

2) El gasto en seguridad es una cuestión de opinión. Nuestra encuesta mostró una gran diferencia en las percepciones de los presupuestos de seguridad para el próximo año, y las expectativas desalineadas son una receta para
confusión, conflicto y toma de decisiones precipitada. Asegurar que haya claridad, y que, si el presupuesto aún no se confirma o indica, cada parte interesada sepa qué nivel de presupuesto les permitirá cambiar, comprar o lograr, es una receta para la toma de decisiones tranquila y serena.

3) La residencia de datos es un tema candente y es absolutamente imperativo para más del 70 % de nuestros encuestados. Pero es igualmente importante considerar las implicaciones de deshacerse de una aplicación basada en la nube que no puede garantizar la residencia de una alternativa; ¿Una solución local o interna será tan segura u ofrecerá la capacidad que necesita?

4) Cuando venga a cambiar de proveedor, decida temprano. Es notable que las transiciones exitosas parecen comenzar al menos 12 meses antes del vencimiento o la renovación del contrato, y decidir es, bueno, probablemente la mejor decisión que se puede tomar primero. No se deje atrapar por la parálisis del análisis.

Finalmente: nuestros datos mostraron un acuerdo y consenso significativos entre los grupos encuestados, algo que apunta a una buena armonía organizacional. Sin embargo, también hay puntos en los datos donde las opiniones de los que toman las decisiones, las personas influyentes y la gerencia divergieron significativamente. Son estas áreas las que deberían preocuparnos a todos, y donde la comunicación clara y abierta será la herramienta más eficaz para el próximo año.

Metodología

El estudio de investigación de mercado B2B 2022 de WithSecure llegó a 3072 encuestados (2098 de Europa) a través de una encuesta en línea durante mayo de 2022 en 12 países, incluidos nueve países europeos: Reino Unido, Francia, Alemania, Bélgica, Países Bajos, Dinamarca, Finlandia, Noruega, Suecia, así como, así como Estados Unidos, Canadá y Japón. Todos los encuestados son tomadores de decisiones de seguridad de TI/red/nube y personas influyentes para la compra de productos y servicios de seguridad de TI/red/nube en sus organizaciones.

Quiénes somos

WithSecure™, formerly F-Secure Business, es el socio confiable de la seguridad cibernética. Proveedores de servicios de TI, MSSP y empresas – junto con las instituciones financieras más grandes, los fabricantes y miles de los proveedores de tecnología y comunicaciones más avanzados del mundo – confíen en nosotros para la seguridad cibernética basada en resultados que protege y habilita sus operaciones. Nuestra protección impulsada por IA protege los puntos finales y la colaboración en la nube, y nuestra detección y respuesta inteligentes están impulsadas por expertos que identifican los riesgos comerciales mediante la búsqueda proactiva de amenazas y el enfrentamiento de ataques en vivo. Nuestros consultores se asocian con empresas y desafíos tecnológicos para desarrollar resiliencia a través de consejos de seguridad basados en evidencia. Con más de 30 años de experiencia en la creación de tecnología que cumple con los objetivos comerciales, hemos construido nuestra cartera para crecer con nuestros socios a través de modelos comerciales flexibles.

WithSecure™ Corporation se fundó en 1988 y cotiza en NASDAQ OMX Helsinki Ltd.

W / T H®
secure