Enterprise Strategy Group | Getting to the bigger truth.™

DOCUMENTO SOBRE CONOCIMIENTOS DE INVESTIGACIÓN DE ESG

Hacia proveedores de ciberseguridad de clase empresarial y plataformas de productos integradas

Por Jon Oltsik, analista principal sénior y socio de ESG

Febrero de 2020

El presente Documento sobre conocimientos de investigación de ESG fue encargado por Cisco y se distribuye con licencia de ESG.

Contenido

Resumen ejecutivo

Al famoso físico Albert Einstein se le atribuye esta famosa cita: "La definición de locura es hacer lo mismo una y otra vez, y esperar resultados diferentes".

Según la investigación de ESG, Einstein podría haber estado hablando de ciberseguridad empresarial. Muchas organizaciones continúan abordando los desafíos de seguridad cibernética con cambios tácticos limitados, como agregar un nuevo control de seguridad de red o forzar el ajuste de algún tipo de herramienta de análisis de backend. En este escenario, cualquier mejora en la eficacia de la seguridad a menudo se ve compensada por la complejidad técnica y el gasto general operativo. Esto también puede conducir a un aumento del riesgo cibernético, incidentes de seguridad y costosas filtraciones de datos.

Afortunadamente, las organizaciones están profundizando, buscando las causas raíz de sus problemas y luego explorando nuevos tipos de soluciones de ciberseguridad. En este Documento sobre conocimientos de investigación de ESG, se llega a la siguiente conclusión:

- Las herramientas de puntos de seguridad representan un problema fundamental. Los profesionales de la ciberseguridad han mantenido durante mucho tiempo una creencia cultural en los beneficios de los mejores productos de seguridad. Desafortunadamente, esto ha conducido a silos de las mejores herramientas de seguridad en todas partes: productos individuales sólidos y una infraestructura de seguridad colectiva desconectada. Los escasos profesionales de la seguridad se ven obligados a monitorear y administrar la seguridad producto por producto y utilizar sus conocimientos, habilidades e intuición para reconstruir una imagen de seguridad integral, una situación operativamente desafiante. Los CISO no pueden salir de esta situación debido a la escasez global de habilidades en ciberseguridad. Dada la escala, el alcance y la sofisticación de las amenazas cibernéticas, un enfoque fragmentado basado en herramientas puntuales se ha convertido en una desventaja.
- Las organizaciones consolidan proveedores e integran tecnologías. Para abordar esta situación, las organizaciones consolidan activamente proveedores de seguridad e integran productos de seguridad. ¿Cuáles son los objetivos? Mejorar la prevención/detección de amenazas, optimizar las operaciones, impulsar un tiempo de resolución más rápido y recibir un mayor apoyo de los proveedores. La investigación apunta a una dirección clara: las organizaciones empresariales gastarán más dinero con menos proveedores. Este cambio ya está sucediendo y será aún más significativo en el futuro.
- Los proveedores líderes responden a los requisitos del lado de la demanda. Para abordar los requisitos de los clientes, los proveedores líderes integran productos, abren interfaces, impulsan los estándares de la industria y crean ecosistemas de socios. ESG cree que algunos líderes se separarán del resto para convertirse en proveedores de ciberseguridad de clase empresarial, al ofrecer plataformas tecnológicas para la prevención, detección y respuesta de amenazas en áreas como seguridad de aplicaciones, terminales, redes y nube. Las mejores plataformas también contarán con análisis avanzado, inteligencia de amenazas de clase mundial, automatización de procesos de operaciones de seguridad y una interfaz de usuario/experiencia de usuario común. La competencia de plataformas de tecnología de ciberseguridad será feroz. Los líderes en este espacio tendrán ofertas fuertes, hojas de ruta sólidas para el futuro y capacidades de servicios para ayudar a los clientes a tener éxito.

Las plataformas de tecnología de ciberseguridad tienen el potencial de simplificar y automatizar las operaciones de seguridad, devolviendo tiempo a los equipos de seguridad abrumados. De esta manera, los CISO pueden enfocarse en habilitar procesos comerciales seguros en lugar de simplemente bloquear ciberataques.

Errores de las herramientas del punto de seguridad

Según una investigación reciente de ESG, el 76 % de las organizaciones afirman que la detección de amenazas y la respuesta es más difícil hoy que hace 2 años.[1] Esta dificultad creciente se debe a cambios externos e internos. Externamente, los profesionales de seguridad deben abordar un panorama de amenazas dinámico y sofisticado mientras monitorean y mantienen la seguridad en una creciente superficie de ataque (es decir, nube, IoT, móvil, SaaS, etc.) impulsada por nuevas iniciativas de TI, como la transformación digital. Estas condiciones están fuera del control (es decir, es algo externo) del equipo de seguridad. Internamente, muchos CISO abordan los desafíos de la seguridad cibernética con una dependencia en procesos informales manuales, un equipo de seguridad cibernética con poco personal y un ejército de herramientas puntuales dispares de una variedad de proveedores.

Este último punto se ilustra en una investigación reciente de ESG: el 31 % de las organizaciones usa más de 50 productos de seguridad diferentes, mientras que el 60 % usa más de 25[2]. La administración de una amplia variedad de herramientas de seguridad crea numerosos desafíos como (ver Figura 1):

- Monitoreo y seguridad de diferentes infraestructuras. El 40 % de los encuestados dijo que necesita diferentes entornos de infraestructura (de seguridad) que luego son administrados por equipos separados, lo que genera ineficiencias operativas. Por ejemplo, el personal de SOC puede monitorear la seguridad de aplicaciones, endpoints, redes y nube con diferentes equipos y herramientas, lo que dificulta la comparación de datos o la coordinación de acciones en diferentes entornos de infraestructura de TI. Estos silos de seguridad pueden obstaculizar las operaciones eficientes en una infraestructura de TI de nube híbrida moderna.

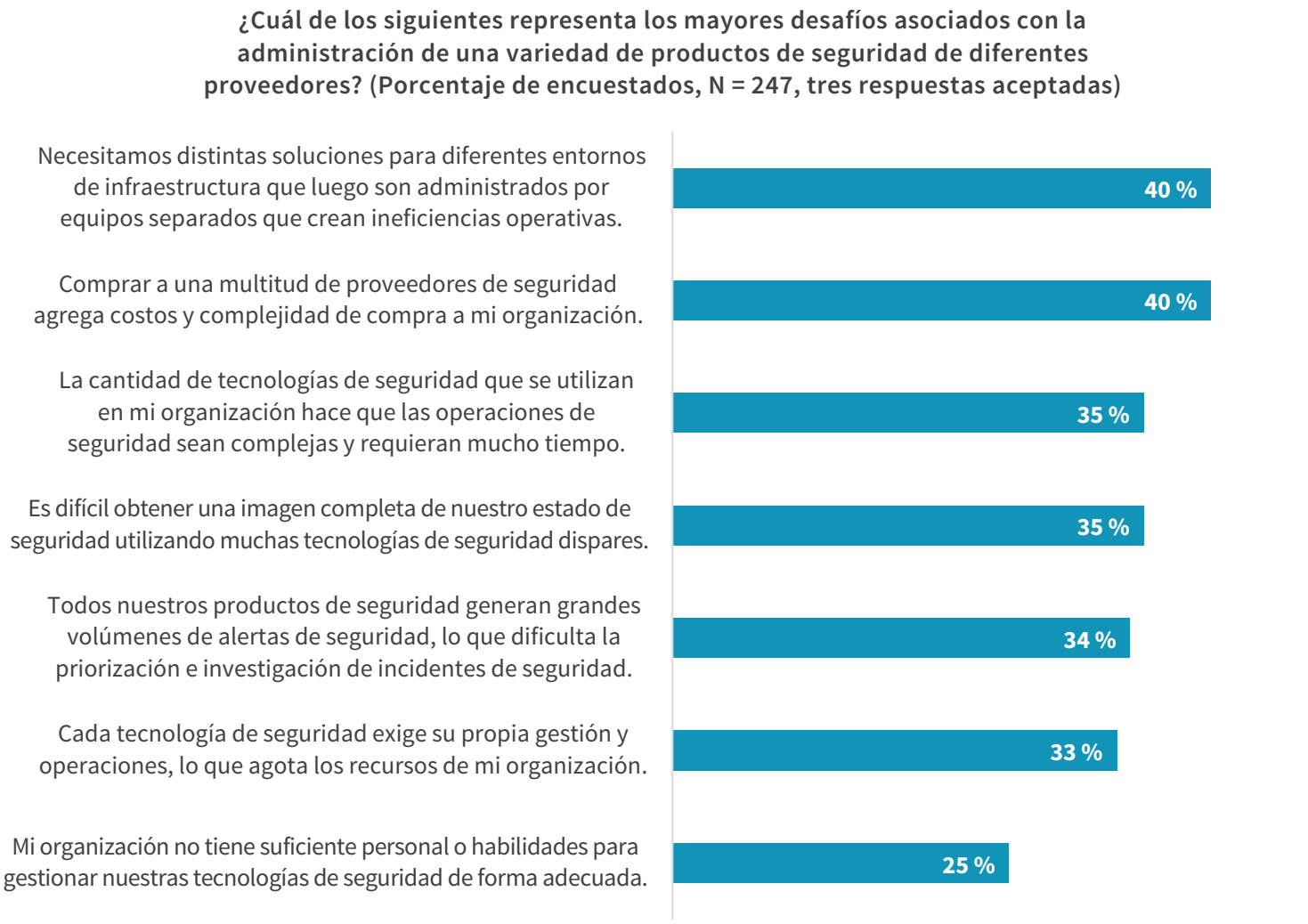
- Complejidad adquisitiva. Los equipos de seguridad se contratan para prevenir, detectar y responder a incidentes de seguridad, no para administrar proveedores y contratos de servicio. Desafortunadamente, el 40 % de los profesionales de la seguridad dicen que comprar a una multitud de proveedores de seguridad agrega costos y complejidad de compra a su organización. Dado que los CISO no se miden en función de la competencia en compras, estos son gastos generales que no necesitan.

- Operaciones de seguridad complejas y que requieren mucho tiempo. En otro informe reciente de investigación de ESG, el 75 % de las organizaciones afirman que la escasez global de habilidades en ciberseguridad ha afectado sus operaciones de seguridad.[3] Lamentablemente, el impacto de la escasez de habilidades en ciberseguridad se agrava cuando muy pocos empleados se enfrentan a un exceso de herramientas de puntos de seguridad. Como indica la investigación, el 35 % dice que administrar una variedad de productos de seguridad conduce a operaciones de seguridad complejas y que requieren mucho tiempo. En otras palabras, la detección y respuesta de amenazas tardan mucho más de lo óptimo, lo que genera niveles más altos de riesgo cibernético, incidentes de seguridad y filtraciones de datos.

- Evaluación del panorama general a través de una serie de imágenes pequeñas. El 35 % de los encuestados dice que administrar una variedad de productos de seguridad dificulta obtener una imagen completa de su estado de seguridad. Nuevamente, esto hace que sea problemático comprender el riesgo cibernético o rastrear un ataque a través de la cadena de eliminación cuando un sistema comprometido escanea la red para robar contraseñas de administrador, descargar cargas útiles de malware o comunicarse con un servidor de comando y control (C2) para instrucciones. Comprender la totalidad de este tipo de actividad maliciosa requeriría tiempo y esfuerzo por parte de analistas de SOC altamente capacitados que reunieran análisis de varias tecnologías de seguridad diferentes.

[1] Fuente: Resultados de la encuesta maestra de ESG, *Panorama de respuesta y detección de amenazas,* abril de 2019.
[2] Fuente: Resultados de la encuesta maestra de ESG, *Encuesta de opinión de proveedores de ciberseguridad de clase empresarial*, febrero de 2020. Todas las referencias y gráficos de investigación de ESG en este documento de información de investigación se han tomado de este conjunto de resultados de la encuesta maestra, a menos que se indique lo contrario.
[3] Fuente: Informe de investigación de ESG/ISSA, *La vida y los tiempos de los profesionales de ciberseguridad 2018,* mayo de 2019.

Figura 1. Desafíos asociados con la administración de una variedad de productos de seguridad



Fuente: Enterprise Strategy Group

Las organizaciones están cambiando el comportamiento de compra de productos de seguridad

En los últimos años, muchos CISO reconocieron que una infraestructura de seguridad basada en herramientas puntuales es insostenible: los problemas asociados con la falta de integración y los gastos generales operativos superan los beneficios propios de las herramientas individuales. Como resultado, las organizaciones han cambiado su enfoque para comprar, implementar y operar productos de seguridad.

Si bien las estrategias de compra, implementación y operaciones están evolucionando, los profesionales de la seguridad aún exigen excelencia de los productos de seguridad individuales. Esta actitud se muestra claramente en la Figura 2. Cuando se les pidió que identificaran las consideraciones de productos de seguridad más importantes, el 41 % de los encuestados optaron por la capacidad de un producto para prevenir/detectar amenazas. Por lo tanto, una arquitectura de tecnología de seguridad debe tener como base las mejores herramientas de prevención y detección de amenazas.

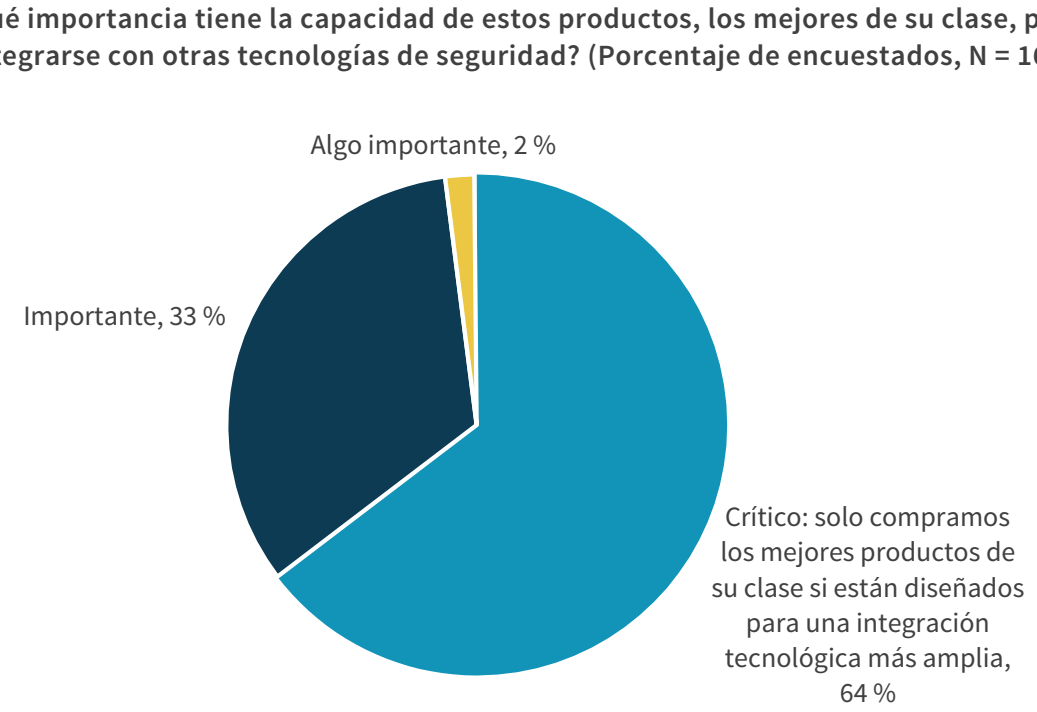
Figura 2. Consideraciones importantes sobre la tecnología de ciberseguridad

¿Cuáles de las siguientes consideraciones de productos son más importantes para su organización al comprar tecnologías de ciberseguridad? (Porcentaje de encuestados, N = 247, se muestra el porcentaje clasificado como # 1)

Fuente: Enterprise Strategy Group

Sin embargo, más allá de la mejor prevención/detección de amenazas, los profesionales de la seguridad quieren ir más allá de los silos de herramientas de puntos desconectados hacia una arquitectura de tecnología de seguridad integrada. Este deseo se ilustra claramente en la Figura 3. El 64 % de los encuestados dicen que es fundamental que los productos de seguridad se integren con otras tecnologías de seguridad, mientras que otro 33 % dice que es importante que los mejores productos se integren con otras tecnologías de seguridad. Claramente, los CISO lo quieren todo: una base de herramientas de seguridad de primera clase e interoperabilidad entre tecnologías.

Figura 3. Importancia de la integración entre productos y tecnologías de seguridad



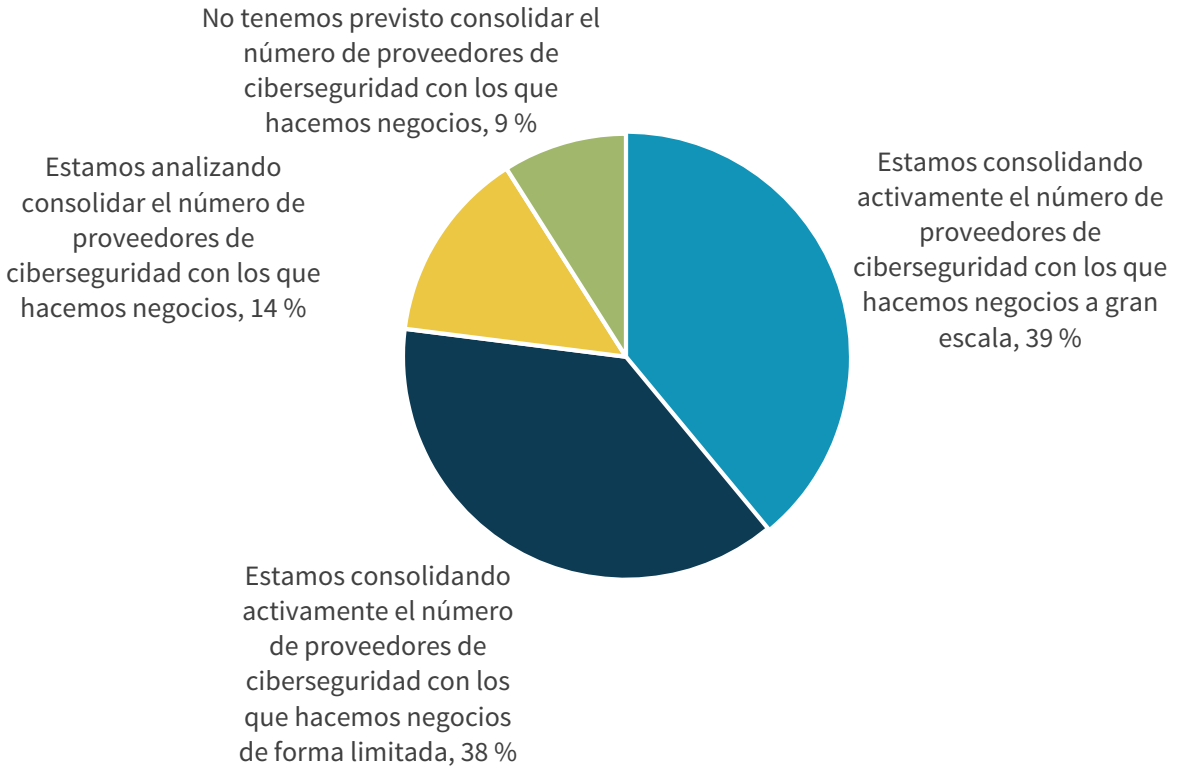
Fuente: Enterprise Strategy Group

Consolidación de proveedores de ciberseguridad

Dada la tendencia hacia la integración de productos, no es sorprendente entonces que las empresas se inclinen a comprar más productos y tecnologías de menos proveedores. ¿Por qué? Los proveedores de tecnología de ciberseguridad de clase empresarial pueden hacer gran parte del trabajo mediante la estrecha integración de sus mejores productos en arquitecturas de tecnología escalables e interoperables. Con base en esta tendencia de la industria, muchas organizaciones adoptan un enfoque activo para la consolidación de proveedores. La investigación de ESG indica que el 39 % de las organizaciones están consolidando activamente la cantidad de proveedores de ciberseguridad con los que hacen negocios a gran escala, mientras que otro 38 % está consolidando activamente la cantidad de proveedores de ciberseguridad con los que hacen negocios de forma limitada (consulte la Figura 4).

Figura 4. Tendencias de consolidación de proveedores de ciberseguridad

¿Cuál de las siguientes afirmaciones con respecto a la consolidación de proveedores de ciberseguridad con los que su organización realiza negocios es más precisa? (Porcentaje de encuestados, N = 247)



Fuente: Enterprise Strategy Group

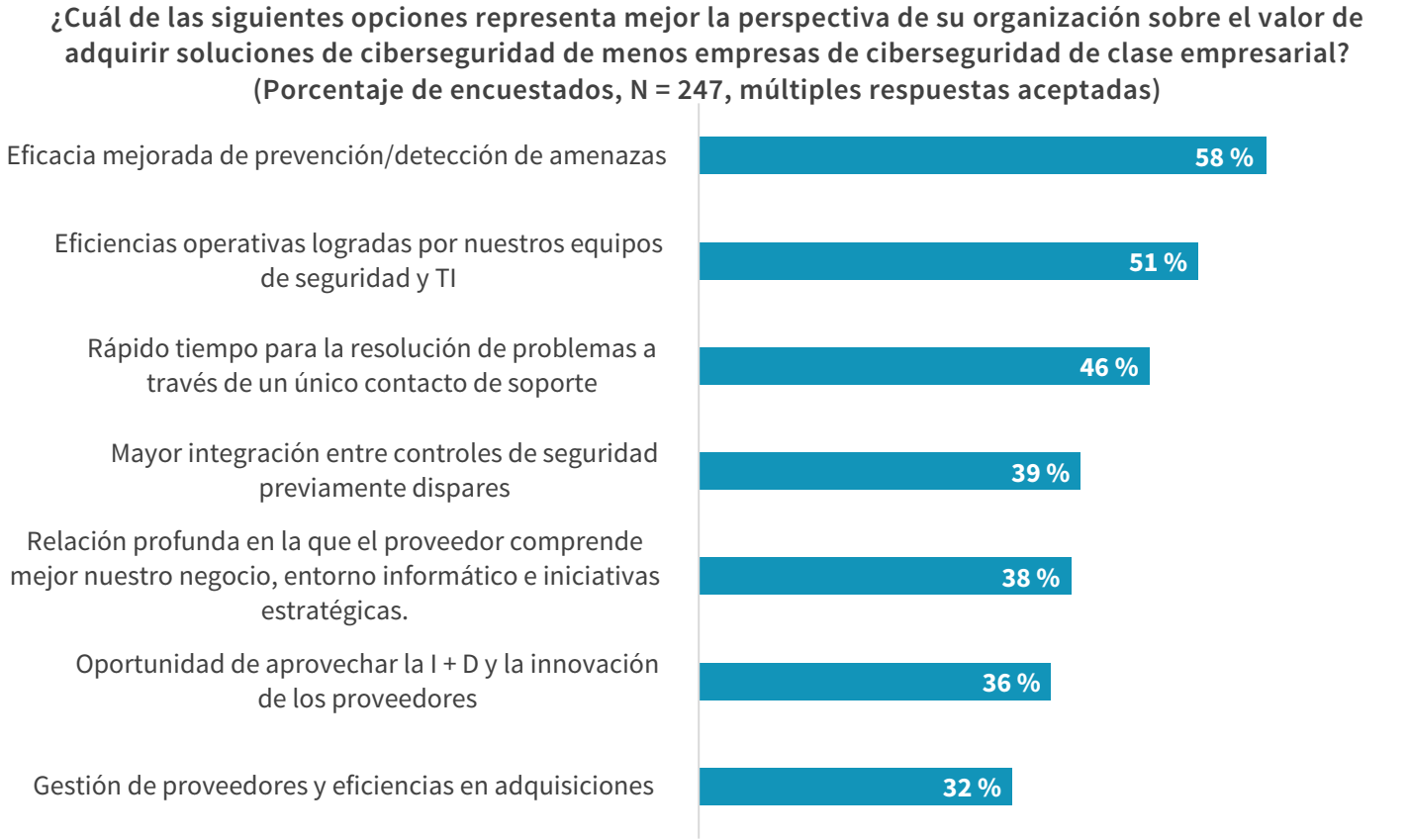
La investigación también indica que los profesionales de la ciberseguridad tienen expectativas claras sobre el valor de comprar más tecnologías de seguridad de menos proveedores. Por ejemplo (vea la Figura 5):

- El 58 % apunta a una mayor eficacia en la prevención/detección de amenazas. La idea aquí es que las herramientas individuales interoperarán, compartiendo datos, alertas e inteligencia de amenazas pertinente. De esta manera, una plataforma de seguridad integrada puede mejorar la fidelidad de las alertas al tiempo que enriquece y contextualiza la telemetría de seguridad. Esto puede ayudar a los equipos de SOC a minimizar el trabajo sin salida de perseguir falsos positivos mientras agilizan las tareas de operaciones de seguridad asociadas con las investigaciones forenses.

- El 51 % dice que espera eficiencias operativas realizadas por sus equipos de seguridad y TI. Las sólidas prácticas de ciberseguridad dependen de comunicaciones y colaboraciones efectivas entre el SOC y los equipos de operaciones de red/TI. Los encuestados creen que la coordinación de las operaciones de seguridad/TI se puede mejorar si ambos equipos trabajan con datos agregados, alertas enriquecidas y herramientas de administración comunes.

- El 46 % afirma que espera un tiempo más rápido para la resolución de problemas a través de un solo contacto de soporte. Casi la mitad (46 %) de los encuestados creen que el trabajo de los analistas de SOC será más fácil cuando tengan un solo proveedor con el que trabajar para el soporte de la plataforma. Esto tiene sentido: en lugar de ajustar varios productos individuales, los equipos de SOC pueden personalizar los conjuntos de reglas y centralizar los ajustes de configuración. Los proveedores líderes también pueden beneficiarse aquí al dedicar personal de campo capacitado medido en hacer que sus clientes tengan el mayor éxito posible.

Figura 5. Valor asociado con la consolidación de proveedores de ciberseguridad



Fuente: Enterprise Strategy Group

Hacia proveedores de ciberseguridad de clase empresarial

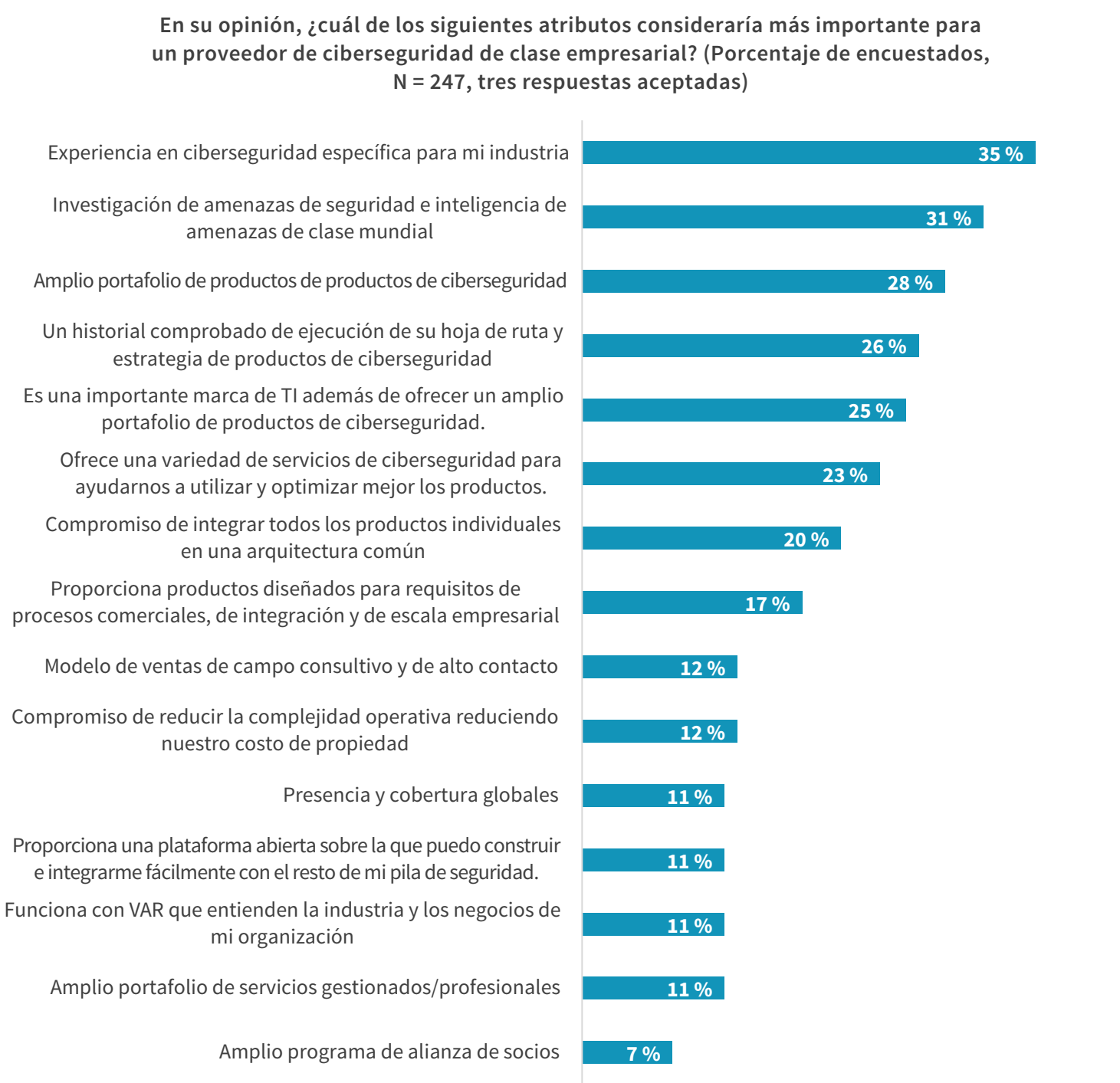
Hoy en día, la industria está formada por miles de proveedores individuales, muchos de los cuales ofrecen una herramienta de un solo punto. A medida que las grandes organizaciones integren tecnologías de seguridad y consoliden proveedores, la industria cambiará en consecuencia y dará lugar al surgimiento de un puñado de proveedores de ciberseguridad de clase empresarial. ESG define el término proveedor de ciberseguridad de clase empresarial como aquellos proveedores de ciberseguridad que ofrecen una amplia gama de productos y/o servicios de ciberseguridad diseñados para escalar, integrar y dar soporte a los requisitos de procesos comerciales de una gran organización.

Con base en esta definición general, ESG pidió a los profesionales de la ciberseguridad que identificaran los atributos más importantes de un proveedor de ciberseguridad de clase empresarial (consulte la Figura 6). Entre ellos se encuentran:

- Experiencia en ciberseguridad específica de la industria. Las aplicaciones de transformación digital, la proliferación de dispositivos IoT y las crecientes regulaciones están cambiando las tecnologías de ciberseguridad de servicios horizontales a aplicaciones industriales verticales. Esta transición se refleja en los datos de ESG, ya que el 35 % de los encuestados cree que la experiencia en ciberseguridad centrada en la industria es uno de los atributos más importantes para los proveedores de ciberseguridad de clase empresarial.
- Investigación e inteligencia de amenazas de clase mundial. Los equipos de operaciones de seguridad necesitan inteligencia en tiempo real sobre el panorama de amenazas para las investigaciones forenses y la búsqueda de amenazas. Por lo tanto, la investigación e inteligencia de amenazas de seguridad de clase mundial es un atributo principal para los proveedores de ciberseguridad de clase empresarial.
- Una amplia cartera de productos de ciberseguridad. Como se dijo anteriormente, los CISO quieren comprar más productos de menos proveedores. Los proveedores de ciberseguridad de clase empresarial pueden cumplir con este requisito al ofrecer una amplia cartera de productos a los clientes. No es de extrañar entonces por qué el 28 % de los encuestados consideran que este es un atributo importante de los proveedores de ciberseguridad de clase empresarial.

- Un registro probado de seguimiento de las ejecuciones. Más de una cuarta parte (26 %) cree que los proveedores de ciberseguridad de clase empresarial deben tener la capacidad de ejecutar sus estrategias y hojas de ruta de productos. En otras palabras, los CISO quieren trabajar con proveedores vistos como "apuestas seguras" a largo plazo.

Figura 6. Atributos más importantes de un proveedor de ciberseguridad de clase empresarial



Fuente: Enterprise Strategy Group

Los proveedores de tecnología de ciberseguridad de clase empresarial con estos atributos son muy atractivos para las organizaciones empresariales. De hecho, el 80 % de las organizaciones indicaron que considerarían comprar una cantidad significativa de sus tecnologías de seguridad a un único proveedor de ciberseguridad de clase empresarial.

El auge de las plataformas tecnológicas de ciberseguridad

En 2020, los proveedores de ciberseguridad de clase empresarial competirán por negocios ofreciendo plataformas de tecnología de ciberseguridad. ESG define este término como:

> *Un conjunto de productos estrechamente integrado ofrecido por un solo proveedor con capacidades de integración de productos de terceros a través de API, estándares de la industria y ecosistemas de partners.*

Las tan anticipadas "guerras de plataformas" de ciberseguridad conducirán a una competencia feroz, una hipérbole de la industria y confusión entre los usuarios. Sin embargo, los profesionales de la ciberseguridad tienen una idea clara de lo que quieren de una plataforma de ciberseguridad. Los cinco atributos principales de la plataforma incluyen:

1. Cobertura de seguridad en los principales vectores de amenazas y puntos de acceso. La mayoría de los ataques cibernéticos todavía se basan en dos vectores de amenazas principales: el correo electrónico y la web. Por lo tanto, las plataformas de ciberseguridad deben incluir monitoreo y controles diseñados para bloquear y/o alertar sobre actividades sospechosas/maliciosas en estos canales comunes.

2. Análisis. Las plataformas de ciberseguridad deben estar respaldadas por análisis avanzados para el análisis de comportamiento, análisis de archivos y calificación de riesgos. ¿El objetivo? Eliminar los falsos positivos y proporcionar alertas procesables y de alta fidelidad.

3. Integración de inteligencia de amenazas. Como se mencionó anteriormente, los analistas de SOC quieren inteligencia de amenazas en tiempo real para poder comparar actividades anómalas con lo que está sucediendo "en la naturaleza".

4. Cobertura amplia. En lugar de comprar herramientas dispares, los CISO quieren plataformas de ciberseguridad que abarquen aplicaciones, terminales, redes y nubes.

5. Prevención, detección y respuesta. Las plataformas deben poder reducir la superficie de ataque y bloquear fácilmente las amenazas conocidas. Las plataformas líderes proporcionarán análisis avanzados para la detección de amenazas y un banco de trabajo de operaciones de seguridad, runbooks y capacidades de automatización para la respuesta a incidentes.

Figura 7. Atributos más importantes de una plataforma tecnológica de ciberseguridad

¿Cuáles son los atributos más importantes de una "plataforma" de ciberseguridad? (Porcentaje de encuestados, N = 247, tres respuestas aceptadas)

Fuente: Enterprise Strategy Group

La transición a las plataformas de ciberseguridad no es una visión lejana. En verdad, los requisitos de ciberseguridad de hoy exigen acción, por lo que el cambio a las plataformas de ciberseguridad ya está en marcha. Por ejemplo, el 38 % de las organizaciones ya han comprado varios productos de un solo proveedor en lugar de los mejores productos de varios proveedores, el 34 % ha utilizado software de código abierto como una capa de integración entre productos independientes y el 34 % ha impulsado varios proveedores de productos de tecnología de ciberseguridad para trabajar juntos en la integración de productos.

Los CISO continuarán impulsando a los proveedores en la consolidación de productos y alentándolos a buscar estándares, integración de productos heterogéneos y cooperación industrial. Los proveedores de ciberseguridad de clase empresarial deben anticipar estas demandas y asumir una posición de liderazgo hacia la facilitación. Los líderes de la industria ofrecerán plataformas de tecnología de ciberseguridad abiertas integrales que pueden ayudar a las organizaciones a mejorar la eficacia de la seguridad mientras optimizan las operaciones.

Cisco SecureX

Cisco anunció recientemente una plataforma de ciberseguridad llamada SecureX. Cisco SecureX conecta la amplia gama del portafolio de seguridad integrada de Cisco y la infraestructura de seguridad del cliente. Esta integración está destinada a ayudar a los clientes a obtener más valor de los productos de Cisco y la infraestructura de seguridad existente mediante la coordinación de defensas (es decir, terminal, red, nube, etc.), centralizando la visibilidad y el análisis, y habilitando la automatización para la prevención, detección y respuesta de amenazas. SecureX también está construido con una UI/UX consistente que sigue al usuario a través de Cisco Security para compartir contexto entre productos y equipos. Esto debería ayudar a los equipos de seguridad a reunirse en torno a informes y paneles comunes, eliminando la necesidad de alternar entre múltiples soluciones.

En general, Cisco SecureX proporciona muchos de los atributos importantes de la plataforma destacados en la investigación de ESG. Cisco también tiene una hoja de ruta agresiva para el avance de SecureX. Los CISO deben evaluar SecureX en todas las capacidades actuales y futuras. Piense en SecureX como un viaje en lugar de un destino. También vale la pena señalar que Cisco no cobra extra por SecureX ni pide a los clientes que reemplacen o incorporen nuevas tecnologías. Más bien, SecureX se ofrece como una experiencia integrada en todo el portafolio de seguridad de Cisco.

La verdad más grande

Dado el estado actual de la ciberseguridad, la mayoría de los CISO se dan cuenta de que no pueden proteger a sus organizaciones dependiendo de herramientas puntuales desconectadas, procesos informales o manuales, y una escasez de habilidades en ciberseguridad. Una forma de salir de este embrollo es a través de la integración de tecnología que permite que las herramientas independientes compartan datos, correlacionen alertas y habiliten flujos de trabajo comunes para operaciones de seguridad.

Las plataformas de tecnología de ciberseguridad pueden abordar la complejidad de la integración con suites de productos interoperables llave en mano. Los de los principales proveedores de ciberseguridad de clase empresarial mejorarán las plataformas de tecnología de ciberseguridad con inteligencia de amenazas de clase mundial, características/funcionalidad de la industria y escalabilidad, capacidad de administración y soporte de calidad empresarial. Además, la funcionalidad de las plataformas de tecnología de ciberseguridad puede tener un impacto inmediato en la madurez organizacional. En pocas palabras, el equipo de ciberseguridad puede ser más productivo y concentrarse en proteger los activos y procesos críticos para el negocio.

Para evitar confusiones al evaluar las plataformas de tecnología de ciberseguridad, los CISO deberían:

- Evaluar los desafíos actuales en personas, procesos y tecnología. Las plataformas líderes deben ir más allá de la tecnología y ayudar a las organizaciones a aumentar la productividad del personal mientras optimizan las operaciones. Los CISO deben buscar los cuellos de botella actuales que afectan áreas como la capacitación de los empleados, MTTD/MTTR y la automatización de procesos. Esta evaluación debería ayudar a generar una lista de requisitos de plataforma más allá de la integración de tecnología.
- Incluya operaciones de red y TI en las solicitudes de información y evaluaciones de productos. Recuerde que la seguridad es una actividad colectiva que depende de una sólida comunicación y colaboración entre los equipos de seguridad y de operaciones de red/TI. Los CISO inteligentes trabajarán con sus pares de TI para descubrir los desafíos actuales y luego buscarán soluciones en RFI, evaluaciones de productos y pruebas/pilotaje que ambos grupos puedan utilizar de manera efectiva.

- Planificar a largo plazo. Las plataformas de tecnología de ciberseguridad probablemente crecerán orgánicamente, integrando más categorías de productos y capacidades con el tiempo. Por lo tanto, la investigación de plataformas debería ir más allá de lo que está disponible en la actualidad. Los CISO deben presionar a los proveedores para que establezcan una hoja de ruta de 24 a 36 meses. Los proveedores líderes deben tener planes integrales, pero también deben estar dispuestos a trabajar con los clientes a medida que surjan nuevos requisitos. En el lado empresarial, los CISO deben crear métricas para que puedan evaluar el progreso y crear programas para la mejora continua a medida que implementan plataformas de tecnología de ciberseguridad de manera más amplia a través de fases.

- Comunicarse con la comunidad. Nota para los CISO: no está solo; casi todas las demás organizaciones empresariales están pasando por una transición similar. Los CISO deben buscar orientación de otras organizaciones industriales de tamaño similar. De esta manera, las organizaciones pueden trabajar juntas para presionar a los proveedores sobre algunos matices específicos de la industria que se pueden agregar a las plataformas de tecnología de ciberseguridad con el tiempo.

Enterprise Strategy Group es una compañía de análisis, investigación, validación y estrategia de TI que proporciona inteligencia de mercado e información procesable a la comunidad global de TI.

www.esg-global.com

contact@esg-global.com

508.482.0188