Serie de Reportes de
Ciberseguridad de Cisco 2020

cisco Seguridad

SIMPLIFICAR PARA **ASEGURAR**

Reduzca la complejidad al integrar su ecosistema de seguridad

Contenido

Introducción

Administrar la seguridad es complejo como resultado de las cambiantes amenazas, la necesidad de conservar el talento y un extenso panorama de proveedores. Hacer crecer su negocio de manera segura no solo implica adoptar nuevas tecnologías de seguridad para contrarrestar las nuevas amenazas. O mantenerse al día con los desafíos que plantean los nuevos procesos empresariales. Es como luchar contra Hidra de Lerna, el monstruo acuático con forma de serpiente de la mitología griega y romana, que se corta una cabeza y volverán a crecer dos más.

La sabiduría convencional implica que cada nuevo problema requiere una nueva solución. Sin embargo, esa nueva solución puede presentarle la difícil tarea de luchar contra dos nuevas cabezas de Hidra en lugar de una. De la misma manera, estratificar la nueva tecnología en cada nueva amenaza realmente lo hace menos seguro a medida que sus procesos se complejizan y sus herramientas son más interdependientes.

En otras palabras, si sigue buscando la tecnología exacta para resolver su problema de seguridad más reciente y más apremiante, es posible que esté multiplicando las brechas de seguridad que lo ralentizan en lugar de simplificar su entorno de seguridad para acelerar la detección y la respuesta.

La bestia que hay que domar

Como gerente de seguridad de CISO o de TI, está constantemente luchando contra exigencias implacables para proteger a su organización. Está protegiendo una fuerza laboral que necesita acceder a las aplicaciones y a los datos en cualquier dispositivo, en cualquier lugar y en cualquier momento. Está fortaleciendo un negocio cada vez más digitalizado para garantizar que cada parte del ecosistema sea segura, desde la red hasta la nube. Está garantizando que las cargas de trabajo estén protegidas dondequiera que se estén ejecutando, las 24 horas, todos los días. Desea que su organización genere titulares por los motivos adecuados, no los equivocados.

Y no hay duda de que los actores de las ciberamenazas están bien financiados y en constante innovación. Los eternos desafíos, como mantener un inventario preciso de usuarios, aplicaciones y dispositivos, nunca desaparecen. Intenta potenciar a los equipos para que se muevan rápidamente, consciente de encontrar un equilibrio entre acelerar el éxito y garantizar la confiabilidad de su seguridad. Entre las nuevas regulaciones, los mandatos de autoridades, los presupuestos estáticos, permitir una fuerza laboral remota segura y la alta rotación del talento de seguridad... el CISO nunca descansa.

Para empeorar las cosas, se ha visto obligado a utilizar soluciones puntuales individuales de un sector que está plagado de incompatibilidades, que ejecutan sus operaciones a través de docenas de herramientas y una cantidad de consolas con una integración inconsistente. Y esto, combinado con las puntuaciones insatisfechas de las necesidades de mantenimiento y parches, inevitablemente deja las vulnerabilidades en diferentes soluciones puntuales de toda la infraestructura de seguridad.

Con soluciones y proveedores dispares, parece un programa insuperable de mantener. Sin embargo, una plataforma de seguridad puede transformar su infraestructura de una serie de soluciones inconexas en un entorno totalmente integrado. Puede conectar la totalidad de su portafolio de seguridad y de su infraestructura de seguridad para establecer la cobertura en cada vector de amenazas y punto de acceso y desarrollar la seguridad de su organización para satisfacer las necesidades del futuro.

Una plataforma puede unificar sus tecnologías de seguridad para combinar visibilidad e identificar áreas para la automatización, la coordinación y el análisis. Y al hacerlo, puede liberar y potenciar a sus equipos de seguridad mientras toma decisiones basadas en datos oportunos y precisos para respaldar el éxito general de su empresa.

Las organizaciones digitales que buscan reducir la complejidad y administrar el riesgo de manera más eficiente aprovecharán una plataforma de seguridad integrada para la visibilidad e inteligencia unificadas, la eficiencia operativa y la seguridad simplificada.

Este enfoque permite que nuestro equipo de seguridad deje de ser integrador de productos y, en su lugar, se concentre en lo que más importa: proteger nuestras soluciones para ayudar a nuestros clientes a alcanzar sus objetivos con confianza.

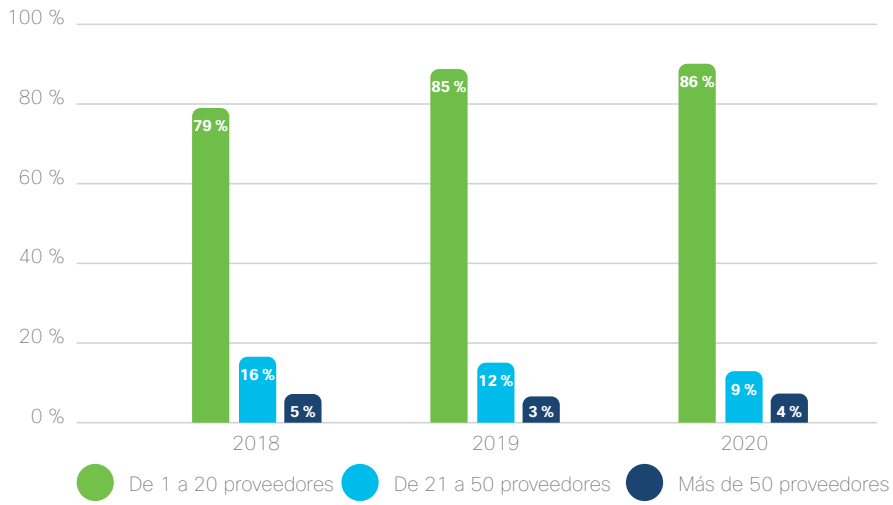
– Brad Arkin, vicepresidente sénior y director de Seguridad y Confianza, Cisco

Un estudio detallado de los proveedores de seguridad, los productos y su impacto

En cada Conferencia de RSA, cientos de proveedores de seguridad compiten por la notoriedad de los profesionales en seguridad y no faltan los proveedores que ofrecen soluciones puntuales que prometen victorias rápidas para combatir las amenazas. La realidad es que la mayoría de las organizaciones cuenta con infinidad de productos diseñados para abordar desafíos específicos, de hecho, más de lo que pueden administrar con tantas alertas que se generan. Pero la mayoría de los productos con parches conjuntos carecen de integraciones inmediatas que permita una práctica de seguridad optimizada y madura.

La encuesta de parámetros de CISO de Cisco de 2020 de 2800 administradores de seguridad reveló que la tendencia a reducir la complejidad a través de la consolidación de proveedores continúa y se mantiene estable con el 86 % de las organizaciones que utilizan entre 1 y 20 proveedores, pero solo el 13 % utilizó más de 20 proveedores este año (Figura 1).

Figura 1. Número de proveedores de seguridad (es decir, marcas, fabricantes, etc.) diferentes que se utilizan en los entornos de seguridad de los encuestados. N=2800.



Fuente: Estudio de parámetros de CISO de Cisco de 2020 Todos los porcentajes están redondeados.

Hemos observado un aumento uniforme año tras año en el porcentaje de encuestados de la encuesta de parámetros de CISO que clasifican el trabajo con varios productos de seguridad como algo exigente o muy exigente, lo que asciende de 74 % en 2018 a 80 % en 2020.

Si aborda su infraestructura de seguridad sin un enfoque de plataforma, las integraciones de producto a producto dan lugar a una expansión de soluciones puntuales diseñadas y respaldadas por diferentes proveedores. Esto crea una visibilidad fragmentada y flujos de trabajo manuales en toda la infraestructura de seguridad, lo que limita el valor de cada solución.

¿No sería útil si su infraestructura de seguridad fuera mayor que la suma de sus partes?

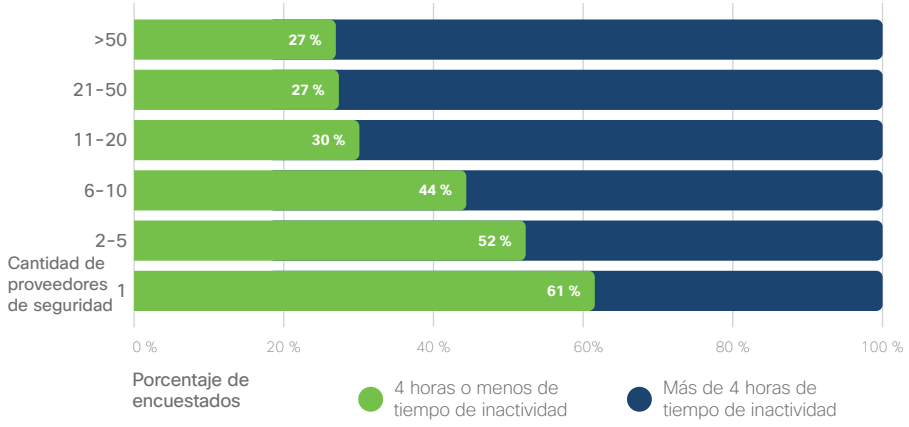
Exposición al fracaso: los datos no mienten

La dependencia de demasiadas consolas reduce la eficacia operativa y, no es de sorprender, agrega más riesgo de error humano. El uso de herramientas inconexas hace que sea cada vez más difícil establecer una amplia visibilidad en toda la superficie de ataque. Esto puede reducir la eficacia de la seguridad, que a menudo se mide por el tiempo de permanencia (la duración del período de tiempo que un agente de amenazas tiene dentro de un sistema para moverse lateralmente y realizar reconocimiento o exfiltrado de datos).

La falta de integración expone una debilidad de seguridad crítica en la capacidad de una organización para responder rápidamente a las amenazas y lograr tiempos de permanencia más bajos. Por lo tanto, la visibilidad en contexto se vuelve mucho más significativa.

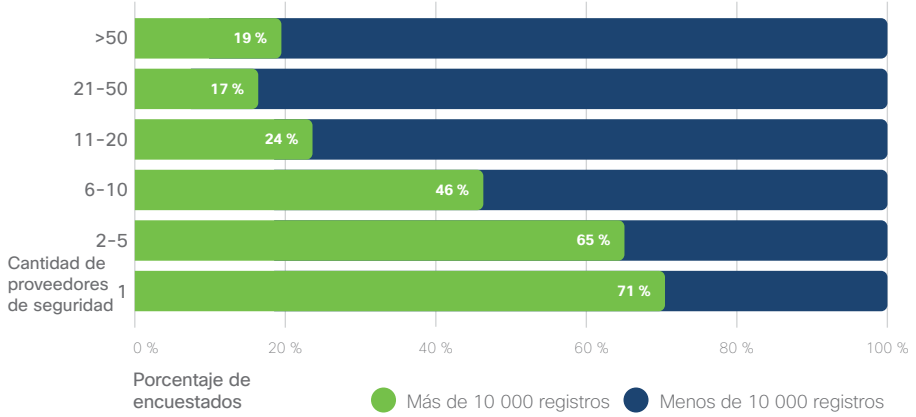
Nuestra encuesta de parámetros de CISO de Cisco de 2020 también destacó cómo la complejidad de proveedores y productos puede degradar significativamente la eficacia de una organización para minimizar el tiempo de inactividad en la respuesta a un ciberataque. Encontramos una correlación entre la cantidad de proveedores y productos en un entorno, y el tiempo de inactividad resultante, los registros afectados y el impacto financiero de un ataque. Como se muestra en las figuras 2, 3 y 4, las personas con menos proveedores experimentaron un menor impacto de un ataque.

Figura 2. Para la mayor intrusión del año pasado, los encuestados de seguridad informaron tener **menos horas de tiempo de inactividad del sistema** cuando tenían menos proveedores. N=2490.



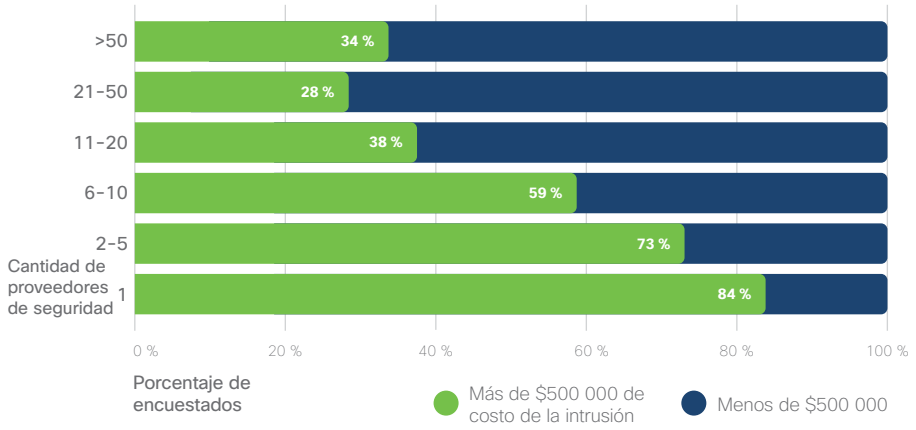
Fuente: Estudio de parámetros de CISO de Cisco de 2020. Todos los porcentajes están redondeados.

Figura 3. Para la mayor infracción del año pasado, los encuestados de seguridad informaron haber tenido **menos registros afectados** cuando tenían menos proveedores. N=2490.



Fuente: Estudio de parámetros de CISO de Cisco de 2020. Todos los porcentajes están redondeados.

Figura 4. Para la mayor infracción del año pasado, los encuestados de seguridad informaron tener **menos impacto financiero** cuando tenían menos proveedores. N=2490.



Fuente: Estudio de parámetros de CISO de Cisco de 2020. Todos los porcentajes están redondeados.

El impacto en la administración de alertas

Dado que las soluciones de varios proveedores tienen múltiples integraciones de punto a punto, si existe alguna integración, no comparten eficazmente el contexto y el análisis para identificar indicadores de riesgo. Además, tienen una oportunidad limitada para enriquecer y priorizar alertas y presentar alertas de alto valor de maneras concisas. Lo que complica más las cosas es que esto genera poca o ninguna conexión entre ver la alerta y actuar en consecuencia.

En nuestra encuesta de parámetros de CISO de Cisco de 2020, los profesionales de seguridad informaron que solo pueden investigar el 51 % de sus alertas de seguridad. De las alertas investigadas, el 50 % de las alertas legítimas no se corrigen.

Este enfoque de varios proveedores (en lugar de un enfoque integrado) hace que continúe el desafío constante de una cantidad abrumadora de alertas. En nuestro estudio, el 96 % de aquellos que sufren la fatiga por alertas dijo que administrar un entorno de varios proveedores es un desafío. Por ende, mientras los profesionales de seguridad intentan abordar la dispersión de los proveedores y las consecuencias, su gestión no se ha vuelto más fácil y necesita más mejoras a fin de optimizar los recursos.

Asesoramiento de primera línea del liderazgo de seguridad de Cisco

La seguridad ha evolucionado en la última década

Ahora se lucha por sobrevivir las 24 horas, todos los días y la seguridad ha evolucionado en tres dimensiones. Una de ellas es la **relevancia empresarial** que ha demostrado ser un acelerador increíble para abogar por la seguridad. La seguridad se está integrando esencialmente en la estructura de la manera en que las empresas operan con mayores niveles de escrutinio en toda la organización, desde la sala de juntas hasta el personal ejecutivo y las operaciones de las diversas unidades de negocios.

La segunda es la **tecnología**, que es una moneda de dos caras. El primer lado de la moneda es la **arquitectura** en evolución impulsada por la migración a la nube y la proliferación de la movilidad en aplicaciones y dispositivos. El otro lado es la aparición de **plataformas** que permiten a los proveedores intercambiar datos de amenazas en tiempo real, como las plataformas de respuesta a amenazas y los intercambios de datos abiertos, como Cisco pxGrid.

La tercera dimensión la conforman los **datos**, porque nadie ve el planeta entero. En el pasado, el impulso hacia la arquitectura de seguridad correcta se ha visto desafiado por la falta de una plataforma que pueda integrar y aprovechar el poder de tantos datos para satisfacer el panorama de ataques en evolución, la infraestructura y la falta de destrezas.

Asesoramiento para la planificación de los CISO de la integración de su arquitectura

Desarrolle un plan y determine lo que intenta lograr mediante la creación de un ecosistema integrado relevante para su empresa. Para mí, es esencialmente cómo se diseña algo, cómo se construirá y cómo se extenderá y podrá desarrollarse, además de validar, para lograr la arquitectura correcta.

En primer lugar, comience con la idea y **desarrolle estrategias** para las funcionalidades distintivas que desea aprovechar su organización. En segundo lugar, sepa **qué resultados está midiendo** antes de comenzar a construir algo. También es fundamental **asociarse con proveedores** que entienden su estrategia y pueden destacar posibles puntos ciegos y **oportunidades de integración** que puede haber perdido.

Métricas necesarias para realizar el seguimiento del éxito en sus operaciones de SOC

Durante mucho tiempo, el sector ha utilizado "¿Ha incumplido?" como métrica para el éxito. Con mi equipo, recalco las métricas en torno a **la visibilidad y el control**. Es imperativo definir qué resultados necesita lograr, ya sea menos incumplimientos, un menor tiempo de detección (MTTD) y corrección (MTTR), una reducción del costo de contención o mayor eficacia. Las métricas que informe al directorio deben estar **vinculadas a estos resultados a nivel empresarial** impulsados por el programa de seguridad subyacente.

Cómo las integraciones eficaces han impulsado el SOC de Cisco

Por supuesto, es genial obtener la mejor de su clase, pero no siempre es necesario alcanzar rápidamente los resultados de seguridad deseados. Además de usar nuestros propios productos de seguridad en Cisco, históricamente también hemos utilizado productos de seguridad que no son de Cisco. Actualmente, estamos usando el paquete completo de productos de Cisco. **Y, a pesar de que nuestro presupuesto se redujo tres veces en los últimos tres años, hemos logrado reducir nuestro MTTD a ocho horas.**

Lo hicimos posible gracias a una plataforma integrada impulsada por la automatización y la inteligencia de datos que ha permitido que mi personal se **concentre en los incidentes más críticos y la búsqueda de amenazas**, lo que mejora la productividad de los recursos. Es fundamental contar con una solución consolidada con capacidades de automatización, respaldada por una plataforma que funcione bien con sus necesidades de análisis de datos y la capacidad de llenar brechas en los flujos de trabajo de SecOps existentes. En Cisco, construimos eficiencia en el sistema, lo que ha generado el ROI y derribó el costo total.

Reinvención de la seguridad

Un día en la vida...

Pasemos un día en la vida de un analista de SOC. Si tienen cubiertas todas las bases, revisan un número cada vez mayor de alertas de diferentes soluciones. Se esfuerzan por seguirle el ritmo al volumen de alertas y están haciendo todo lo posible para priorizar y abordar las más críticas.

Correlacionan la información de varias fuentes para crear un panorama completo de cada amenaza potencial. Clasifican y asignan prioridades, trabajando con sus equipos de operaciones de red y de TI. Desarrollan cuadernos de estrategias para ayudarlos a repetir estas actividades de manera uniforme.

Realizan todas estas tareas complejas con un tremendo sentido de urgencia. Su objetivo es formular rápidamente una estrategia de respuesta adecuada basada en el reconocimiento situacional y el impacto de amenazas, el alcance potencial del riesgo y el daño potencial que puede surgir.

Este proceso manual a menudo es propenso a errores y requiere mucho tiempo, lo que exige que un analista de SOC rote en varias consolas rápidamente. Con toda la multitarea de los analistas del SOC para clasificar las alertas de numerosas soluciones puntuales, existe la probabilidad de que se pasen por alto amenazas de alta gravedad.

Y hete aquí que contratar a más expertos para administrar estas alertas no ayuda. La capacidad de respuesta también se ve afectada por la dependencia de ITOps y NetOps en SecOps y los obstáculos que estos equipos crean para el otro. Las organizaciones necesitan ayuda para mitigar la escasez de talento uniendo a las personas, los procesos y la tecnología en una experiencia más simple y uniforme. Y aquí, las integraciones son clave.

> Los cambios positivos en la transformación digital han puesto de manifiesto que las tecnologías de seguridad en los silos contribuyen a una mayor complejidad. Nuestros equipos pierden tiempo valioso conectando los puntos e integrando todas estas herramientas que no funcionan entre sí.
>
> – Michael Degroote, asesor de infraestructura, Mohawk Industries

Más enfoque, menos ruido

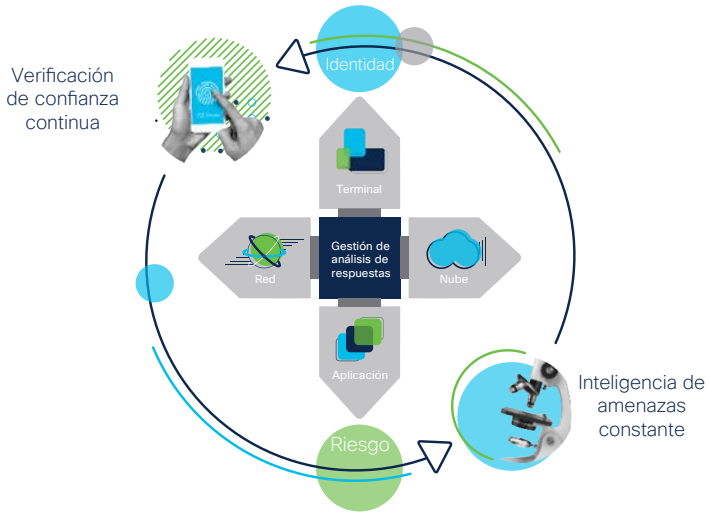
La mayoría de los CISO se levantan cada mañana para mejorar la eficiencia, optimizar sus recursos, aumentar la madurez e impulsar la colaboración en todas sus operaciones. Todo esto mientras administran las amenazas. Es mucho pedir y es difícil de lograr con tanto alboroto en torno a la ciberseguridad. Analicemos los componentes principales de la seguridad.

Cuando se trata de administrar las amenazas, hay muchas áreas de integración que las plataformas de seguridad pueden aprovechar, por ejemplo:

- **Seguridad de red:** firewalls y confianza cero en el lugar de trabajo
- **Protección de usuarios y terminales:** confianza cero de la fuerza laboral con la seguridad de terminales, móviles y correo electrónico
- **Perímetro de la nube:** un amplio conjunto de funciones de visibilidad, control y seguridad como servicio en la nube
- **Seguridad de las aplicaciones:** confianza cero de las cargas de trabajo con microsegmentación
- **Inteligencia de amenazas:** análisis de malware y fuentes
- **Verificación de confianza:** autenticación de usuarios y evaluación de la posición del dispositivo
- **Análisis de seguridad:** recopilación, categorización y análisis de datos en tiempo real para detectar anomalías y amenazas avanzadas
- **Servicios de seguridad:** detección y respuesta administradas

Para lograr la cobertura de seguridad en esta larga lista, sería necesaria una amplia gama de productos de seguridad. Pero tenga en cuenta que esto puede lograrse con un enfoque de plataforma, lo que proporciona una verificación continua de la confianza y una inteligencia de amenazas constante.

Figura 5. Transforme su infraestructura de una serie de soluciones inconexas en un entorno totalmente integrado con integraciones de back-end en mejores experiencias de interfaz.



Esto no puede suceder de la noche a la mañana. Pero para avanzar hacia este enfoque integrado, puede comenzar enumerando sus prioridades, desafíos y flujos de trabajo.

Para comenzar, dedique algún tiempo a responder a estas preguntas básicas:

- ¿Cuáles son los desafíos de mi infraestructura de seguridad existente?
- ¿Los cambios empresariales requerirán que agregue o reemplace mis inversiones en seguridad?
- ¿Cómo puedo impulsar mi madurez de seguridad con mis recursos existentes?
- ¿Cuáles son mis prioridades para obtener el máximo valor de cualquier inversión en seguridad?
- ¿Qué contexto se comparte entre los equipos y las herramientas en nuestros flujos de trabajo?

Responder detalladamente estas preguntas le proporcionará una comprensión sólida de los desafíos de seguridad que deben resolverse y en qué orden. Esto también sirve como un plan para identificar lo que tiene, lo que necesita para alcanzar sus objetivos, por qué lo necesita y lo que ganará al realizar estos cambios. El siguiente paso es desarrollar estrategias para cada funcionalidad que su organización necesita tener.

Una vez que haya alcanzado una comprensión clara de todos estos aspectos, entonces puede buscar soluciones que satisfagan específicamente esas necesidades, atento a explorar soluciones **que funcionen juntas de manera integral en su ecosistema de seguridad e infraestructura general**.

La mera adquisición de las mejores herramientas que operan aisladamente sin una plataforma de seguridad subyacente se ha convertido en una opción cada vez menos viable. Cualquier herramienta con una funcionalidad muy buena (y una que se integre fácilmente con otras herramientas) probablemente sea más valiosa y eficaz que una herramienta con todo tipo de accesorios.

La adquisición de esta manera le permite comenzar el trabajo de definición de flujos de trabajo entre herramientas a un nivel más avanzado. Una plataforma que ofrezca la definición de flujo de trabajo e integración en su núcleo tiene un impacto significativo en sus esfuerzos por aumentar la madurez de la seguridad.

El punto aquí es que antes de buscar soluciones de seguridad, sepa lo que intenta lograr y cómo se alinea (o admite) sus objetivos comerciales. Determine cómo trabajarán las soluciones en conjunto para minimizar el ruido de demasiadas alertas y reducir el mantenimiento manual para el que no posee recursos.

Integración desde una plataforma de seguridad

Sin duda, ninguna solución de seguridad única puede proteger organizaciones completas. Y ningún panel único puede solucionar la necesidad de un dominio de seguridad para una mayor visibilidad. El éxito depende de comprender las relaciones entre las tecnologías que vinculan los sistemas y el uso de este conocimiento para crear una mayor sinergia entre ellos. Suena más fácil decirlo que hacerlo: ¿cómo se traduce esta visión?

Un enfoque de plataforma para la seguridad hace hincapié en la importancia de la apertura: la capacidad de conectar su infraestructura de seguridad existente a una plataforma abierta e integrada con una interoperabilidad inmediata. Su empresa debe tener la libertad de explorar nuevas soluciones sin tener que preocuparse por gastar sus recursos en integrarlas más adelante.

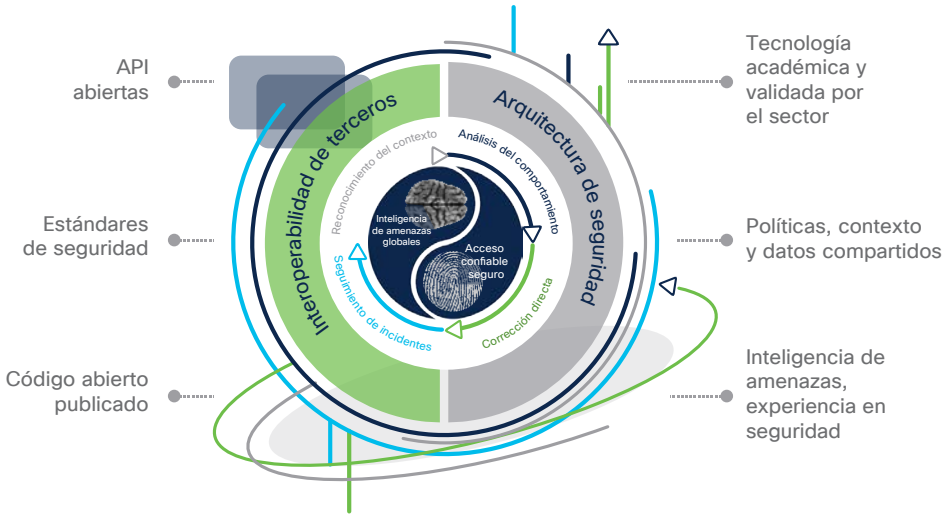
Por ejemplo, la alianza técnica de seguridad de Cisco facilita las integraciones de productos abiertos y de varios proveedores con más de 170 partners tecnológicos para mejorar la eficacia de la seguridad a través de la automatización y la simplicidad operativa. Nuestra integración a través de una plataforma de seguridad está diseñada para brindar a nuestros clientes un enfoque eficaz para garantizar el acceso, la respuesta ante amenazas y la administración de políticas.

Mientras trabajamos en el lado de la red, de la seguridad, de la identidad, del acceso, entre otros, no estamos cerrados. Puede incorporar tecnología de cualquier producto de seguridad (Cisco o de otro tipo) para crear un entorno de seguridad integrado.

Tenga en cuenta cuatro pilares de habilitación en un entorno de este tipo. Usted puede:

- Saber qué datos se comparten para acelerar el tiempo de detección
- Ejecutar cambios automatizados de políticas para acelerar la respuesta
- Brindar un reconocimiento contextual para integrar controles granulares en toda la arquitectura de seguridad
- Armonizar sus políticas de seguridad e impulsar resultados más sólidos con la colaboración de SecOps, NetOps e ITOps

Figura 6. Crear una base para su pila de seguridad con interoperabilidad integrada que le garantice que experimente todo el potencial de sus productos.



Este enfoque modular a la seguridad le permite contar con puntos de acceso para aprovechar la integración entre las tecnologías existentes, a la vez que garantiza un acceso más rápido a las nuevas tecnologías sin compensaciones de integración. Puede crearlo ahora con lo que tiene.

Quizás ya haya desarrollado el portafolio más potente de productos de seguridad y haya agregado la interoperabilidad incorporada. Ahora, con este enfoque, está conectando todo esto a una plataforma que garantiza que su experiencia alcance todo el potencial de sus productos, con la apertura y la interoperabilidad integrada como los beneficios más destacados.

La plataforma adecuada no solo lo ayudará a mejorar su seguridad en los usuarios, las aplicaciones y los dispositivos, sino que lo ayudará a medir y probar el éxito. Una plataforma debe ofrecer automatización y análisis integrados que ayuden en la administración de políticas y dispositivos, la detección de amenazas desconocidas y la coordinación de la respuesta y el cambio de políticas. Este nuevo enfoque está bien posicionado para resolver el problema de la seguridad y transformar la seguridad de compleja a uniforme.

Cuantificar los beneficios

La adopción del enfoque de plataforma crea mejoras cuantificables para su empresa. Estas mejoras incluyen numerosos beneficios; a continuación se describen los más importantes:

Eficiencias operativas: incorporar inteligencia de amenazas, automatizar el enriquecimiento y mejorar la respuesta ante incidentes y la coordinación de políticas para responder más eficazmente a las amenazas en evolución y proteger los nuevos emprendimientos empresariales.

- **Reducir el ruido de alertas** con el reconocimiento contextual y las correlaciones para comprender más profundamente qué alertas necesitan atención urgente. Reducir el tiempo por alerta requerido para la investigación forense, ya que los flujos de trabajo se integran y automatizan a través de los cuadernos de estrategias.
- **Reducir la huella de los proveedores** en su ecosistema garantizando que los partners de seguridad estratégica puedan ofrecer nuevas funcionalidades como componentes puedan integrar fácilmente.
- **Obtener un acceso más rápido** a esas funcionalidades para los equipos de seguridad y TI, que se ofrecen de manera más eficiente que si fueran componentes autónomos.

Innovación: trabajar con menos proveedores pero que sean más fuertes y que se hayan ganado una reputación de ofrecer servicios y funcionalidades más innovadores al mercado que mejor se dirijan a las arquitecturas y amenazas en evolución. Una plataforma abierta que le permita desarrollar flujos de trabajo que automatizan sus cuadernos de estrategias personalizados puede impulsar la innovación para su seguridad.

Potenciar recursos a través de la automatización: una plataforma integrada impulsada por la automatización puede ayudar a abordar los desafíos de la escasez de talento, lo que le permite usar sus recursos limitados de SOC para una coordinación más estratégica. Esto puede ayudar a mejorar la retención de los empleados y ayudar a un analista del SOC de nivel 1 a realizar investigaciones más complejas para que su equipo tenga más tiempo de enfocarse en lo más importante.

Reducir la complejidad: muchos dispositivos y soluciones de seguridad no pueden integrarse en la plataforma de seguridad más amplia debido a la falta de modularidad de diseño. Busque soluciones basadas en la nube y basadas en la API que puedan permitir una rápida respuesta y corrección. Su plataforma de seguridad debe permitir una expansión simplificada de las funcionalidades de seguridad en función de las necesidades emergentes.

Racionalizar el retorno de la inversión (ROI): la transición a una plataforma de seguridad integrada frente a recurrir a proveedores de seguridad dispares puede mostrar con mayor facilidad un impacto en los KPI, lo que impulsa la productividad de los recursos y las métricas de respuesta, como MTTD, MTTR y los tiempos de evolución de incidentes. Esto le brinda pruebas concretas definitivas para correlacionarse con los costos del incumplimiento. Con herramientas dispares, es difícil obtener métricas clave que realmente proporcionen medidas de rendimiento y eficiencia.

Reducir el riesgo: evaluar los datos más importantes y cubrir los riesgos de los asistentes en esos datos en todo el ecosistema de la solución mediante el aprovechamiento de la inteligencia de amenazas agregada, el análisis de comportamiento avanzado, la coordinación, la automatización y la búsqueda continua de amenazas.

Medir el éxito: las métricas son una excelente manera de comprender la desconexión entre la prevención, la detección y las operaciones de IR. La capacidad de realizar un seguimiento de métricas tales como el tiempo de permanencia, la relación de protección, los falsos positivos de incidentes, la relación entre los incidentes identificados por el usuario y los incidentes identificados por el SOC, entre otros, proporciona una instantánea de la vulnerabilidad. La eficacia táctica de SecOps le permite ocuparse de las brechas y diseñar un mejor programa de seguridad.

Preguntas para comenzar

Con tantas opciones y tantas direcciones en las que ir, comencemos con 10 preguntas críticas que los profesionales de seguridad deben tener en cuenta al analizar productos y soluciones de proveedores.

1. **¿Cuál es el costo total de propiedad y los beneficios de ROI que puedo obtener de la consolidación de proveedores e integración de mi portafolio existente?**
2. **¿Nuestra plataforma está unificada para la investigación de amenazas, la administración de seguridad y la respuesta ante incidentes?**
3. **¿Cómo se integra esta nueva tecnología con nuestro ecosistema existente? ¿Mejorará la eficacia de la seguridad y la eficacia operativa?**
4. **¿Nuestro programa de inteligencia de amenazas nos permite tomar decisiones más rápidas y más definitivas?**
5. **¿Cómo evaluaremos la apertura de nuestras soluciones a la integración con terceros? ¿Cómo funciona esto junto con nuestras tecnologías existentes de SIEM?**
6. **¿Este proveedor (o producto) permite que nuestro equipo acelere las funciones clave de seguridad: detección, investigación y corrección a través de una consola unificada?**
7. **¿Nuestras tecnologías existentes generan y conservan el contexto en el conjunto de herramientas? ¿Se integran de manera nativa con otras herramientas de ese mismo proveedor?**
8. **¿Nuestra plataforma aprovecha la automatización para simplificar los flujos de trabajo manuales? ¿Estos flujos de trabajo nos permiten hacer de NetOps e ITOps una extensión de los equipos de SecOps?**
9. **¿Nuestro equipo ha analizado los intercambios de integración mientras evalúa los productos para comprender si necesitamos las características adicionales a expensas de la integración?**
10. **¿La mano de obra actual de SOC lo apoyará? ¿Necesitamos contratar analistas adicionales o podemos capacitar al equipo existente?**

Estrategias fundamentales de nuestros asesores de CISO

Estas son nuestras recomendaciones prácticas basadas en nuestra investigación original y prácticas comprobadas de consultoría con los clientes:

1. Considere la integración como una parte clave de su decisión de compra.

La expansión de proveedores en un entorno de seguridad típico provoca una complejidad innecesaria y flujos de trabajo ineficientes. Para empeorar las cosas, la escasez crónica de talento dificulta la adopción completa de soluciones existentes, lo que aumenta la exposición. Una táctica para mitigar estos desafíos es adoptar una plataforma abierta basada en el portafolio que permita que sus soluciones funcionen en conjunto.

Este tipo de enfoque de plataforma es único de dos maneras. En primer lugar, integra de manera nativa las soluciones de back-end del portafolio con una interfaz unificada. En segundo lugar, permite que otras tecnologías de los proveedores se integren sin inconvenientes con esa interfaz.

Cuando la carga de la integración se traslada principalmente al proveedor, termina aprovechando las inversiones existentes, basándose en lo que tiene y creando una base sólida para las necesidades futuras.

2. Alinee NetOps, ITOps y SecOps.

Los equipos de red, TI y seguridad tradicionalmente han trabajado en silos, pero su dependencia mutua para resolver problemas provoca obstáculos. Puede unificar a sus equipos con flujos de trabajo de colaboración y contexto compartido para permitir a ITOps corregir problemas con alertas significativas y permitir que NetOps apliquen políticas de manera más uniforme. Esto reduce la carga de SecOps y mejora la productividad de los tres equipos.

Lograr este nivel de colaboración no es fácil, pero es posible con el enfoque adecuado. Una plataforma integrada puede ayudar, siempre y cuando ofrezca una vista adaptable y unificada, lo que permite a cada equipo ver las alertas, las métricas y el contexto que son más significativos para ellos sin afectar a los demás.

3. Guíe su toma de decisiones con un modelo de madurez de la seguridad.

Con las presiones de los presupuestos ajustados, la escasez crónica de personal y un panorama de amenazas en constante cambio, es fácil caer en un modo reactivo de seguridad. Sin embargo, en este paradigma reactivo, sus inversiones solo pueden ayudarlo a mantener el statu quo en lugar de darle la libertad para madurar su organización de seguridad.

Elija un modelo de madurez de seguridad y sea proactivo sobre su trayectoria. Hay muchos para elegir, pero la mayoría de los modelos reflejan la visibilidad unificada en los puntos de control, la automatización entre entornos y las métricas claras de seguridad. Si bien es posible lograr estos resultados a través de integraciones manuales de SIEM/SOAR, todas son funciones nativas de una plataforma de seguridad integrada.

4. Ofrezca a su gente una vista para enfocarse, no veinte.

Sus equipos de seguridad están constantemente rotando entre diferentes consolas e interfaces, lo que los ralentiza y genera alertas contradictorias.

Deles una visión unificada mediante la integración de su infraestructura de seguridad. Esto optimiza los flujos de trabajo y maximiza el valor de sus inversiones. También permite que sus equipos actúen sobre alertas, armonicen políticas, respondan a las amenazas y aprendan las mejores prácticas, lo que libera valor con mayor rapidez con una experiencia más simple y uniforme.

5. Utilice la automatización dondequiera que pueda para hacer que sus equipos sean más eficientes.

Es probable que sus equipos pierdan mucho tiempo en procesos manuales y repetitivos: esto es ineficiente y deja espacio para el error humano. Con una plataforma, puede utilizar la automatización para manejar muchas tareas, como compartir el contexto de amenazas y confianza, y adaptar el acceso a la red o las aplicaciones para los terminales comprometidos.

Por ejemplo, podría utilizar estas funcionalidades en conjunto para evitar que los dispositivos en mal estado accedan a datos confidenciales. En primer lugar, utilice la solución de acceso seguro para identificar los terminales infectados o no seguros. Luego, utilice la automatización para cambiar la política de autenticación de dicho dispositivo en todo el entorno hasta que se corrija la amenaza.

Al bloquear el acceso para los dispositivos no confiables, puede responder a las amenazas con mayor rapidez y evitar las intrusiones en los datos sin interponerse en el camino de los negocios.

Caso de éxito: Istanbul Grand Airport (IGA)

La creación de una red segura y escalable desde cero con la integración en su núcleo.

Resumen

Industria: transporte

Ubicación: Estambul, Turquía

Desafío

- Construir una base de TI segura para el aeropuerto de mayor crecimiento del mundo
- Garantizar la flexibilidad y la escalabilidad de la red a través de tres fases de construcción
- Proporcionar visibilidad de todas las partes de la infraestructura de TI del aeropuerto
- Ofrecer capacidades eficaces de investigación y búsqueda de amenazas

Solución

IGA consolidó su portafolio de seguridad con los objetivos siguientes:

- Reducir la complejidad a través de la consolidación de proveedores
- Mejorar la seguridad de terminales
- Aumentar la visibilidad de la red y la inteligencia procesable
- Lograr una mejor detección de amenazas

Para proteger completamente el aeropuerto de mayor crecimiento del mundo, IGA implementó la solución de seguridad de terminales de Cisco. Con una plataforma integrada de seguridad completa de Cisco, IGA ahora confía en que los datos del cliente y del negocio se protegerán y asegurarán.

Resultados

- Escalabilidad en la administración con API flexibles
- Seguridad eficaz en toda la infraestructura de TI de IGA, desde la red, la web y el correo electrónico hasta el terminal
- Plataforma integrada que permite a IGA ver una amenaza una vez y bloquearla en todas partes en su entorno, lo que reduce la carga de trabajo administrativa y el tiempo de corrección
- Visibilidad mejorada y capacidades de búsqueda de amenazas para evitar que los ataques ingresen a la red del IGA

Aprenda más.

Estábamos analizando las características de integración, visibilidad e implementación de los productos y Cisco era el único proveedor que nos lo podía ofrecer.

– Emrah Bayarcelik, director de seguridad de Istanbul Grand Airport

La seguridad de Cisco ofrece simplicidad

La seguridad de Cisco continúa construyendo una experiencia simplificada para nuestros clientes: seguridad que ayuda a reducir la complejidad, fortalecer las operaciones y permite que los equipos dediquen más tiempo a iniciativas de mayor valor.

En el centro de nuestra plataforma de seguridad, Cisco SecureX, es una idea simple: las soluciones de seguridad deben estar diseñadas para actuar como un solo equipo. Deben aprender el uno del otro. Deben escuchar y responder como una unidad coordinada. Cuando esto sucede, la seguridad se vuelve sistemática y más eficaz. Con nuestro diseño de plataforma, hemos hecho posible lo siguiente:

- **Proteger su empresa con confianza:** satisfaga sus necesidades de seguridad de hoy y de mañana con la plataforma de seguridad más amplia y más integrada que protege sus diversos puntos de acceso de diversos vectores de amenazas.
- **Automatizar los flujos de trabajo de seguridad:** aumente la eficiencia y la precisión de sus recursos existentes a través de la automatización para impulsar su madurez de seguridad y mantenerse a la vanguardia de un panorama de amenazas en constante cambio.
- **Colaborar mejor que nunca:** comparta el contexto entre SecOps, ITOps y NetOps para armonizar las políticas de seguridad e impulsar resultados más sólidos en los flujos de trabajo que convierten a la seguridad de un bloqueador en un habilitador.
- **Reducir la complejidad y maximizar los beneficios:** impulse el potencial de sus inversiones en seguridad de Cisco, pruebe otros componentes del portafolio de Cisco a través de pruebas gratuitas y conéctese con su infraestructura de seguridad existente a través de la interoperabilidad inmediata.

La seguridad de Cisco le brinda una oportunidad única para combinar la totalidad de nuestro portafolio con toda su infraestructura de seguridad para una experiencia uniforme. Esto unifica la visibilidad, permite la automatización y fortalece la seguridad en toda la red, el terminal, la nube y las aplicaciones. El entorno permite que su personal automatice la detección de amenazas y la respuesta, así como la administración de políticas de red e implemente el acceso de confianza cero para impulsar una visibilidad más profunda y controles más fuertes de políticas. El resultado es una seguridad simplificada e incorporada en las soluciones que ya posee.

Imagine eliminar los puntos de fricción entre las operaciones de seguridad individuales y los flujos de trabajo. O que permitan un desarrollo y una implementación más rápidos de nuevas funcionalidades para ayudar a los equipos de seguridad a implementar tecnologías con mayor rapidez y superar a los adversarios en línea.

Cada producto de seguridad de Cisco está respaldado por la inteligencia de amenazas de Talos líder del sector para bloquear más amenazas y hacer que las organizaciones sean más seguras. Utilizamos la verificación de confianza como base para garantizar que solo las personas adecuadas obtengan acceso. El análisis de comportamiento y el aprendizaje automático aumentan todos nuestros esfuerzos de seguridad, por lo que las soluciones se adaptan y se convierten en más eficaces en tiempo real.

Todo esto se admite mediante respuestas automatizadas a amenazas avanzadas que le permiten optimizar las operaciones con la administración integrada de amenazas y seguridad en todo el portafolio. Y, por último, todos nuestros productos están diseñados para trabajar con las tecnologías que no son de Cisco que tiene para las respuestas de seguridad integradas. No más sillas giratorias, alertas contradictorias o administración de políticas inconsistente.

Figura 7. Los beneficios del enfoque de plataforma de Cisco SecureX.

La integración es un elemento esencial para nuestra estrategia de la plataforma, que ofrece automatización y visibilidad reales en todos los principales vectores de amenazas al tiempo que reduce su tiempo de respuesta a los eventos de seguridad.

Obtenga más información en cisco.com/go/secure.

Tener todas las herramientas de Cisco tan bien integradas realmente nos brinda protección profunda y en capas. Contar con una plataforma de seguridad más integral realmente nos ha ayudado a avanzar más hacia nuestro objetivo final en poco tiempo.

- Don Bryant, CISO, Universidad de Carolina del Norte en Pembroke

Acerca de nuestros expertos

La seguridad de Cisco cuenta con un consejo de asesoría CISO formada por antiguos CISO que poseen una gran cantidad de conocimientos sobre ciberseguridad con antecedentes en una variedad de sectores. Además de proporcionar su información, orientación y experiencia para informar las recomendaciones que ofrecemos en la serie de informes sobre ciberseguridad, también respaldan a nuestros vendedores, partners y clientes en cuestiones como la protección de la transformación digital al cumplimiento, la privacidad, el monitoreo y la visibilidad, la confianza cero y la inteligencia de amenazas. Si desea hablar con un miembro de nuestro equipo de asesoría CISO, comuníquese con asktheciso@external.cisco.com.

Acerca de la serie de reportes de ciberseguridad de Cisco

Durante la última década, Cisco ha publicado una gran cantidad de información crucial de seguridad e inteligencia de amenazas para profesionales de seguridad interesados en el estado de la ciberseguridad global. Estos informes exhaustivos proporcionan explicaciones detalladas de los panoramas de amenazas y las consecuencias para las organizaciones, así como los procedimientos recomendados para defenderse frente a los efectos adversos de las vulneraciones de datos.

El Departamento de Seguridad de Cisco realiza una serie de publicaciones basadas en investigaciones e impulsadas por datos bajo el banner " Serie de reportes de ciberseguridad de Cisco". Hemos ampliado la cantidad de títulos a fin de incluir diversos informes para profesionales de seguridad con intereses diferentes. Invocando la amplitud y profundidad de conocimientos de los investigadores de amenazas e innovadores en el sector de seguridad, los informes de la serie de este año incluyen el Reporte de Privacidad de Datos, Reporte CISO Benchmark, Reporte para PYMes y otros que serán publicados a lo largo del año.

Para obtener más información y acceder a todos los informes de la serie, visite: www.cisco.com/mx/securityreports.

Sede central en América
Cisco Systems Inc
San José, CA

Sede central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV
Ámsterdam, Países Bajos

Publicado en junio de 2020 RPT_06_2020

cisco Seguridad

Seguridad

El puente a lo posible