Microsoft Security

Tres razones para cambiar a la protección contra amenazas integrada

Índice

Introducción

La empresa promedio ahora utiliza más de 30 herramientas de seguridad diferentes, a menudo desconectadas y «añadidas a la fuerza».

La seguridad está en un punto de inflexión. Los ciberataques son cada vez más sofisticados mientras las organizaciones siguen afrontando desafíos que van desde la escasez de talento y el equilibrio de costes hasta lidiar con las presiones del trabajo híbrido.

Mientras tanto, el mercado de la seguridad está más fragmentado y es más complejo que nunca. La empresa promedio ahora utiliza más de 30 herramientas de seguridad diferentes, a menudo desconectadas y «añadidas a la fuerza», lo que limita la visibilidad y proporciona conocimientos inadecuados a los centros de operaciones de seguridad (SOC).

Los líderes de seguridad y cumplimiento desean conocer mejor los últimos riesgos y amenazas, pero también necesitan saber lo que funciona, lo que no y dónde hay deficiencias.

Aunque el alcance de los desafíos de seguridad actuales puede parecer abrumador, hay motivos de optimismo para los directores de seguridad de la información que pretendan mejorar la eficiencia y la eficacia de sus operaciones de seguridad. La respuesta radica en un enfoque integral e integrado sobre la protección contra ciberamenazas que ayude a las organizaciones a:

Razón 1. Hacer más con menos.

Consolida las soluciones puntuales y reduce la sobrecarga de operaciones de seguridad (SecOps).

Razón 2. Permitir que SecOps se centre en tareas de alto valor

Utiliza herramientas que aumenten la eficiencia y capaciten como nunca antes incluso a los analistas júnior.

Razón 3. Aumentar la productividad de los empleados

Protege tu organización de forma que permita a tus empleados disipar los temores cuando crean e innovan.

Este enfoque es posible integrando una solución de detección y respuesta extendidas (XDR) con un sistema de administración de eventos e información de seguridad (SIEM) nativo del cloud que utilice funciones de inteligencia artificial (IA) y automatización. La solución integrada puede ayudar a tu SOC a adoptar una actitud más predictiva, proactiva y preventiva ante los ataques de toda la empresa.

Razón 1

Hacer más con menos

Al consolidar las herramientas con la solución integrada de Microsoft, también puedes ahorrar, ya que solo pagas por lo que usas.

Muchas organizaciones han abordado la compra de herramientas de seguridad centrándose en las mejores soluciones puntuales. Lamentablemente, ese enfoque puede hacer que sea más difícil para los profesionales de seguridad identificar y responder rápidamente a las amenazas. También puede terminar teniendo consecuencias negativas en el gasto de TI y en la productividad de los usuarios finales.

Cuando las organizaciones quieren hacer más con menos, un enfoque integrado como SIEM y XDR de Microsoft puede ser de ayuda. Puede reducir la complejidad gracias a la consolidación de herramientas individuales y, como es nativa del cloud, una solución integrada puede mejorar también el rendimiento y la escala.

Al consolidar las herramientas con la solución integrada de Microsoft, también puedes ahorrar, ya que solo pagas por lo que usas. Asimismo, puedes reducir la sobrecarga de SecOps para administrar soluciones gracias a una mayor automatización e integración.

> Iniciar el proceso de adopción de nuevas herramientas de seguridad es sencillo, porque esperas encontrar grandes deficiencias. A partir de ahí, pronto te das cuenta de que las herramientas de diferentes proveedores pueden solaparse cuando se ejecutan. Este solapamiento podría ser deseable para los cheques y los saldos, **pero también puede tener un coste financiero elevado**».
>
> **Jonathan Cassar**
> Director de tecnología, MITA

1,6 millones de USD

ahorrados anualmente al consolidar los proveedores

Microsoft encargó la realización de un estudio de Total Economic Impact™ (TEI) a Forrester Consulting para conocer el rendimiento de la inversión (ROI) potencial que las empresas pueden conseguir al implementar una solución SIEM y XDR de Microsoft. Estas fueron algunas de las principales conclusiones de una organización compuesta hipotética con un total de 8000 empleados y 10 profesionales de seguridad:

- **Ahorro de casi 1,6 millones de USD al año al consolidar los proveedores**. La inversión en SIEM y XDR de Microsoft permite a la organización compuesta reducir el coste de su solución SIEM anterior (560 000 USD), la infraestructura on-premises asociada (más de 360 000 USD), tres soluciones puntuales XDR (192 000 USD) y el coste continuo de mano de obra para administrar estas soluciones (480 000 USD).
- **Reducción del riesgo de una infracción importante en un 60 %.** Con flujos de trabajo de investigación y respuesta de seguridad más eficientes, una mejor automatización de las respuestas de seguridad y una mayor capacidad para proteger todos los entornos informáticos, incluida la protección multicloud, la organización compuesta reduce el riesgo de infracciones con un impacto anual valorado en un ahorro de 1,6 millones de USD.
- **Generación de un ROI del 207 %.** Las entrevistas con los representantes y los análisis financieros revelaron que una organización compuesta obtiene beneficios de 17,68 millones de USD en tres años frente a los costes de 5,76 millones de USD, lo que representa un valor actual neto (VAN) de 11,92 millones de USD.

Razón 2

Permitir que SecOps se centre en tareas de alto valor

Es fundamental integrar los sistemas SIEM y XDR para cotejar las alertas, priorizar las amenazas más importantes y coordinar la acción en toda la empresa.

Los equipos de SecOps se ven abrumados por la cantidad de señales que tienen que analizar, incluidas muchas señales de baja fidelidad que son difíciles, si no imposibles, de detectar manualmente y mitigar. Conforme aumentan las amenazas, es difícil para un SOC ya sobrecargado mantenerse al día, especialmente cuando hay que analizar datos de varias soluciones puntuales. La asignación de más recursos para cubrir las carencias no es la respuesta, ya que encontrar profesionales de seguridad con la cualificación suficiente es un desafío continuo.

Por eso es fundamental integrar los sistemas SIEM y XDR para cotejar las alertas, priorizar las amenazas más importantes y coordinar la acción en toda la empresa, con IA y automatización avanzadas para detectar y corregir proactivamente las amenazas.

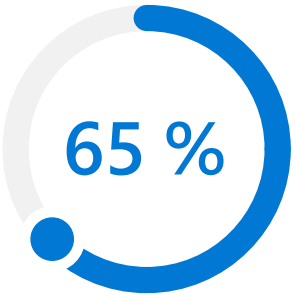
Debe tenerse en cuenta que, por ejemplo, una única señal de bajo nivel podría no llamar demasiado la atención de una solución SIEM tradicional. Con la IA, sin embargo, una solución SIEM nativa del cloud puede comparar automáticamente esa señal con las señales de otras fuentes en toda la organización, cotejando varios conjuntos de datos para encontrar ataques en varias etapas.

Los sistemas SIEM y XDR integrados liberan recursos de SecOps, al tiempo que proporcionan más capacidades y confianza a incluso los analistas júnior.

A continuación, el sistema normaliza, analiza y coteja los datos, al tiempo que proporciona un contexto sobre la forma en que el ciberataque ha penetrado en la infraestructura, además de la línea cronológica de su propagación. Esto permite a los equipos de SOC ver la infracción desde una única consola y abordarla eficazmente.

> Muchos directores de seguridad de la información no se dan cuenta **de la sobrecarga que imponen a sus equipos con 20 paneles diferentes** o soluciones puntuales, y los costes anuales que esto conlleva... Hemos eliminado la fatiga de tener que lidiar con un montón de herramientas al recurrir a un solo proveedor».
>
> **Terence Jackson**
> Director de seguridad de la información y privacidad, Thycotic

Una organización no debería necesitar amplios conocimientos para aprovechar el valor de una solución de seguridad. Los sistemas SIEM y XDR integrados liberan recursos de SecOps, al tiempo que proporcionan más capacidades y confianza a incluso los analistas júnior.



El enfoque integrado de SIEM y XDR de Microsoft redujo el tiempo para investigar las amenazas en un 65 %.

El estudio Total Economic Impact™ (TEI) de Forrester encargado por Microsoft revela este tipo de eficiencia en SecOps en su organización compuesta:

- **Reducción del tiempo de investigación de las amenazas en un 65 % y reducción del tiempo de respuesta a las amenazas en un 88 %.** El enfoque integrado de SIEM y XDR de Microsoft para la investigación y respuesta a las amenazas de seguridad aumenta la eficacia de estos flujos de trabajo para los profesionales de seguridad de la organización compuesta. Ya no necesitan emplear varias herramientas para identificar las amenazas, mientras que las características de automatización de seguridad mejoran aún más los flujos de trabajo de respuesta.

- **Reducción del tiempo para crear un nuevo libro de trabajo en un 90 % y del tiempo para incorporar nuevos profesionales de seguridad en un 91 %.** El enfoque integrado de SIEM y XDR de Microsoft también mejora la eficacia de los flujos de trabajo de los nuevos profesionales de seguridad. Como los registros de SIEM se integran en todo el conjunto de soluciones, la creación de libros de trabajo está casi automatizada, mientras que un inicio de sesión único permite a los nuevos profesionales de seguridad incorporarse casi 16 semanas más rápido.

Razón 3

Aumentar la productividad de los empleados

Una solución SIEM y XDR integrada puede ayudar a tu organización a aumentar la productividad de los usuarios finales.

Además de hacer más con menos y aumentar la eficacia de SecOps, una solución SIEM y XDR integrada puede ayudar a tu organización a aumentar la productividad de los usuarios finales.

Como los equipos de SecOps saben, cuando las medidas de seguridad son complejas, los empleados usan atajos. Por tanto, cuando las experiencias de los usuarios finales entorpecen en lugar de contribuir a la productividad de los empleados, la organización puede sufrir más riesgos de seguridad y tener que afrontar mayores costes. Las contraseñas poco seguras o perdidas, el acceso inseguro mediante dispositivos personales o el intercambio sin restricciones de datos confidenciales son solo algunos de los desafíos.

> [En el pasado] usábamos instrumentos contundentes cuando alguien sospechaba que había un problema. Lo apagábamos todo y cerrábamos el acceso, lo que afectaba negativamente a nuestro negocio. Y ese impacto era evidente porque las cosas dejaban de funcionar temporalmente. En Microsoft Sentinel tenemos un bisturí con el que podemos reaccionar quirúrgicamente a lo que está sucediendo. **Por lo general, la empresa ni siquiera sabe cuándo estamos respondiendo a una amenaza**, y esa es una medida muy importante de nuestro éxito».
>
> **Rick Gehringer**
> Director de información, Wedgewood

Casi
68 000

La solución SIEM y XDR de Microsoft mejoró la productividad de otros empleados en casi un total de 68 000 horas al año.

Un enfoque integrado de SIEM y XDR te ayuda a ofrecer experiencias de usuario fluidas que permiten que tus empleados sean productivos y estén protegidos en todas las facetas de sus experiencias cotidianas. Puede reducir el impacto negativo en la productividad, como tener que desactivar servicios o aislarlos y después volver a crear una imagen de las máquinas. Pero las soluciones SIEM y XDR integradas también pueden crear nuevas oportunidades para aumentar la productividad de los usuarios finales, por ejemplo, con un mayor soporte de seguridad en régimen de autoservicio, mejores paneles e informes y más capacidad de respuesta y tiempos de arranque más rápidos, ya que son menos los agentes de seguridad que hay que ejecutar.

En el estudio Total Economic Impact™ (TEI) de Forrester encargado por Microsoft, la hipotética organización compuesta con un total de 8000 empleados registró un aumento en la productividad de los empleados gracias a la implementación de una solución SIEM y XDR de Microsoft:

- **Mejora de la productividad de otros empleados en casi un total de 68 000 horas al año.** La solución SIEM y XDR de Microsoft evita que los procesos de seguridad ineficientes repercutan negativamente en otros empleados. Por ejemplo, la organización compuesta ahorra 4000 horas al año gracias a la nueva capacidad de los profesionales de TI de autogestionar las actualizaciones y recomendaciones de seguridad. También permite solucionar los problemas de seguridad en remoto en las máquinas de los empleados y reduce el número de agentes de seguridad que se ejecutan en ellas, lo que supone un ahorro de casi 64 000 horas al año en productividad de los usuarios finales.

La seguridad se ha convertido en un factor esencial para el éxito tecnológico. Es por eso que las organizaciones necesitan medidas de seguridad que proporcionen la mayor resiliencia posible a los ataques modernos, para proteger y permitir la productividad y la innovación que impulsan el crecimiento.

Obtén protección contra ciberamenazas integrada con SIEM y XDR

Esta integración de productos líderes del sector ofrece prevención, detección y respuesta ante ciberamenazas en una única solución completa.

Microsoft ofrece la primera y única solución SIEM y XDR integrada, que proporciona visibilidad integral de todos los clouds y plataformas. Esta integración de productos líderes del sector ofrece prevención, detección y respuesta ante ciberamenazas en una única solución completa.

La solución SIEM y XDR de Microsoft aprovecha la eficacia de la IA y la automatización, así como las inversiones cuantiosas y continuas en detección y análisis de ciberamenazas, con conocimientos especializados y visibilidad de 43 billones de señales cada día. Gracias a la integración de estos productos, los equipos de SOC están mejor equipados que nunca para buscar y resolver las ciberamenazas críticas más rápidamente:

Microsoft Sentinel

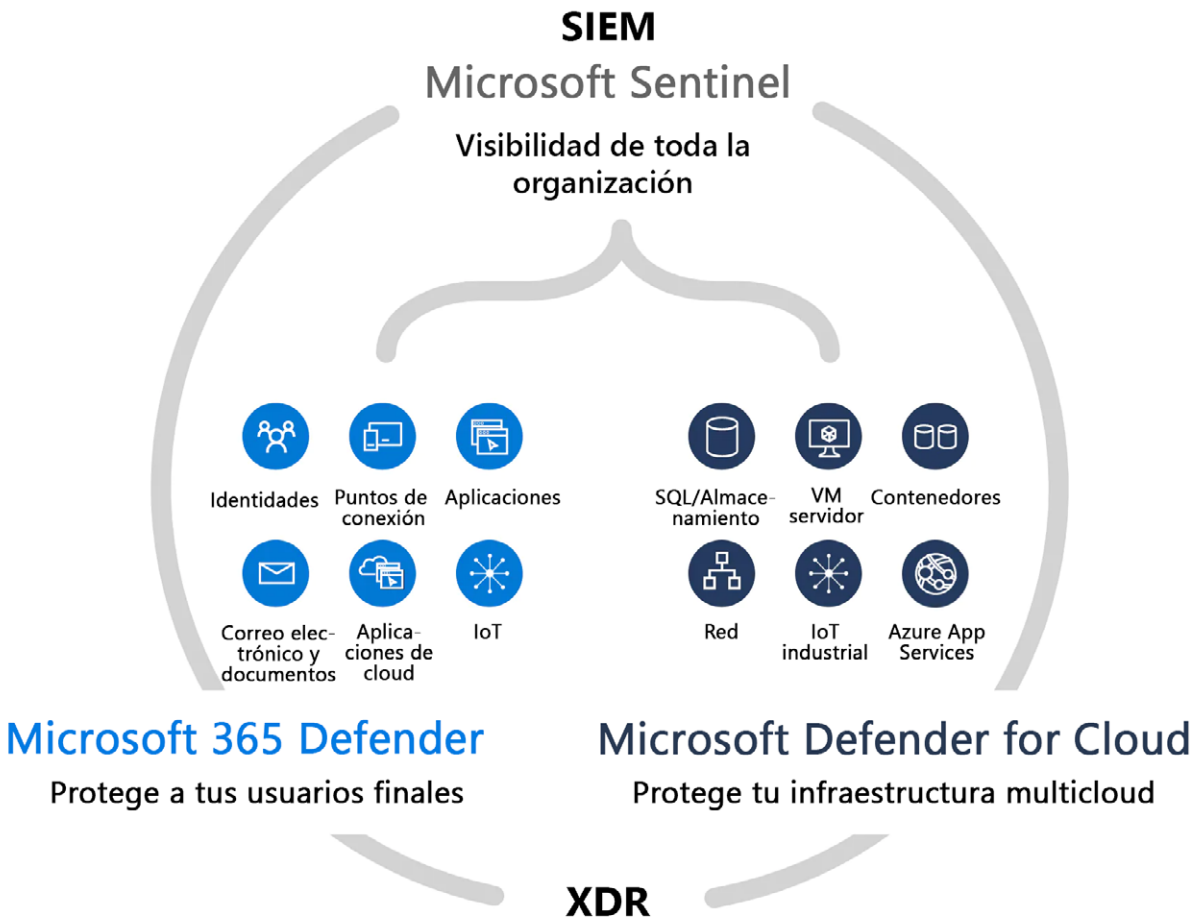
Obtén una vista general de toda la empresa con la solución SIEM nativa del cloud de Microsoft. Agrega datos de seguridad de prácticamente cualquier fuente y aplica la IA para separar el ruido de los eventos legítimos, cotejar alertas en cadenas de ciberataque complejas y acelerar la respuesta ante las ciberamenazas con orquestación y automatización integradas.

Microsoft Defender XDR

Evita y detecta ciberataques en tus identidades, puntos de conexión, aplicaciones, correo electrónico, datos y aplicaciones en el cloud con funciones XDR. Investiga y responde a los ciberataques con la mejor protección de su clase incluida de serie. Busca amenazas y coordina fácilmente tu respuesta desde un único panel.

Microsoft Defender for Cloud

Protege tus cargas de trabajo en los distintos cloud y en el cloud híbrido con funciones de XDR integradas. Protege tus servidores, almacenamiento, bases de datos, contenedores, etc. Céntrate en lo importante con alertas priorizadas.



No acumules soluciones de seguridad. Intégralas.

Pon las herramientas y los conocimientos adecuados en manos de las personas correctas. Defiéndete de los ataques modernos con una solución completa, nativa del cloud e integrada.

Obtén más información sobre la protección contra ciberamenazas integrada con las soluciones SIEM y XDR de Microsoft >

Microsoft Security