Microsoft Security

3 motivos para cambiar a la protección contra amenazas integrada

Índice

Introducción

La empresa promedio ahora usa más de 30 herramientas de seguridad diferentes, a menudo desarticuladas y "anexadas".

La seguridad se encuentra en un punto de inflexión. A medida que las organizaciones siguen abordando desafíos que van desde la escasez de talentos y el equilibrio de costos hasta enfrentar las presiones del trabajo híbrido, los ciberataques son cada vez más sofisticados.

Mientras tanto, el mercado de la seguridad está más fragmentado y complejo que nunca antes. La empresa promedio ahora usa más de 30 herramientas de seguridad diferentes, a menudo desarticuladas y "anexadas", que ofrecen una visibilidad limitada e información inadecuada a los centros de operaciones de seguridad (SOC).

Los líderes de seguridad y cumplimiento quieren comprender mejor los riesgos y amenazas más recientes, pero también necesitan saber qué funciona, qué no y dónde existen brechas.

Si bien el alcance de los desafíos de seguridad de hoy puede parecer abrumador, los CISO que buscan mejorar la eficiencia y eficacia de sus operaciones de seguridad tienen motivos para sentirse optimistas. La respuesta radica en un enfoque de la protección contra ciberamenazas integrado de extremo a extremo que ayudará a las organizaciones:

Motivo 1: Haga más con menos

Consolide soluciones puntuales y reduzca la sobrecarga de operaciones de seguridad (SecOps).

Motivo 2: Capacite a los equipos de SecOps para centrarse en tareas de alto valor

Use herramientas que aumenten la eficiencia y logre que incluso los analistas junior estén más capacitados que nunca.

Motivo 3: Incremente la productividad de los empleados

Proteja su organización de una manera que permita que sus empleados no teman mientras crean e innovan.

Este enfoque es posible al integrar una solución de detección y respuesta extendida (XDR) con un sistema de administración de eventos e información de seguridad (SIEM) nativo de la nube que utiliza inteligencia artificial (IA) y capacidades de automatización. La solución integrada puede ayudar a que su SOC se vuelva más predictivo, proactivo y preventivo contra los ataques en toda la empresa.

Motivo 1

Haga más con menos

Al consolidar las herramientas con la solución integrada de Microsoft, también le permite ahorrar al pagar solo por lo que usa.

Muchas organizaciones han abordado la incorporación de herramientas de seguridad enfocándose en las mejores soluciones puntuales. Lamentablemente, este enfoque puede hacer que sea más difícil para los profesionales de seguridad identificar y responder rápidamente a las amenazas. También puede terminar teniendo un impacto negativo en el gasto de TI y en la productividad del usuario final.

A medida que las organizaciones buscan hacer más con menos, un enfoque integrado, como SIEM y XDR de Microsoft, puede ayudar. Puede reducir la complejidad ya que consolida las herramientas individuales y, debido a que es una solución integrada nativa de la nube, también puede mejorar el rendimiento y la escala.

Al consolidar las herramientas con la solución integrada de Microsoft, también le permite ahorrar al pagar solo por lo que usa. También puede reducir la sobrecarga del equipo de SecOps necesaria para administrar las soluciones pues se aumenta la automatización y la integración.

> Comenzar el proceso de adopción de nuevas herramientas de seguridad es fácil porque uno espera que las brechas sean extensas. A partir de ese momento, pronto se dará cuenta de que las herramientas de diferentes proveedores pueden superponerse en sus mandatos. Esta superposición podría ser conveniente para los cheques y los saldos, **pero también podría representar un costo financiero considerable"**.
>
> **Jonathan Cassar**
> Director de tecnología, MITA

USD 1,6 millones

se ahorraron al año en la consolidación de proveedores

Microsoft encargó a Forrester Consulting que realizara un estudio Total Economic Impact™ (TEI) y examinara el potencial retorno de la inversión (ROI) que las empresas podrían obtener al implementar SIEM y XDR de Microsoft. A continuación, se presentan algunos de los hallazgos clave para una organización compuesta hipotética con 8000 empleados totales y 10 profesionales de seguridad:

- **Se ahorraron casi USD 1,6 millones al año en la consolidación de proveedores**. La inversión en SIEM y XDR de Microsoft permite al compuesto reducir el costo de su SIEM anterior (USD 560 000), la infraestructura local asociada (más de USD 360 000), tres soluciones de puntos de XDR (USD 192 000) y el costo del trabajo continuo para administrarlos (USD 480 000).
- **Se redujo el riesgo de una filtración de material en un 60 %.** Gracias a los flujos de trabajo de investigación y respuesta de seguridad más eficientes, una mejor automatización de las respuestas de seguridad y la mayor capacidad para proteger a todos los entornos informáticos, incluida la protección multinube, el compuesto redujo el riesgo de filtraciones con un impacto anual que representa un ahorro de USD 1,6 millones.
- **Se generó un ROI del 207 %.** Las entrevistas representativas y el análisis financiero detectaron que una organización compuesta experimenta beneficios de USD 17,68 millones en tres años frente a los costos de USD 5,76 millones, lo que suma un valor actual neto (NPV) de USD 11,92 millones.

Motivo 2

Capacite a los equipos de SecOps para centrarse en tareas de alto valor

Resulta fundamental integrar SIEM y XDR para correlacionar alertas, priorizar las amenazas más grandes y coordinar la acción en toda la empresa.

Los equipos de SecOps se ven abrumados por la cantidad de señales que tienen que analizar, lo que incluye una gran cantidad de señales de baja fidelidad que son difíciles, si no imposibles, de detectar manualmente y mitigar. A medida que aumentan las amenazas, es difícil para un SOC sobrecargado mantenerse al día, en especial cuando intenta analizar los datos de varias soluciones puntuales. La asignación de más recursos para cerrar las brechas no es la respuesta, puesto que encontrar suficientes profesionales de seguridad calificados es un desafío constante.

Por esta razón es fundamental integrar SIEM y XDR para correlacionar las alertas, priorizar las amenazas más importantes y coordinar la acción en toda la empresa, con IA y automatización avanzadas para detectar y corregir de modo proactivo las amenazas.

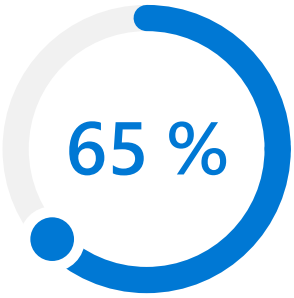
Considere, por ejemplo, que es posible que una señal de bajo nivel no capte mucha atención de un SIEM tradicional. Sin embargo, con el uso de la IA, un SIEM nativo puede comparar automáticamente esa señal con señales de otros orígenes en toda la organización, correlacionando varios conjuntos de datos para descubrir ataques de varias etapas.

Los SIEM y XDR integrados liberan recursos de SecOps y, al mismo tiempo, empoderan incluso a los analistas junior con más capacidades y confianza.

Luego, el sistema normaliza, analiza y correlaciona los datos, a la vez que se proporciona contexto sobre la manera en que el ciberataque ingresó a la infraestructura, junto con la cronología de su propagación. Esto permite a los equipos de SOC visualizar la vulneración, desde una sola consola, y abordarla con eficacia.

> Muchos CISO no se dan cuenta de la **sobrecarga que imponen a sus equipos con 20 paneles diferentes** o soluciones puntuales, y los costos anuales asociados... Hemos eliminado mucha fatiga de herramientas con un solo proveedor".
>
> **Terence Jackson**
> Director de Seguridad de la Información y Privacidad, Thycotic

Una organización no debería necesitar una tremenda experiencia para descubrir el valor de una solución de seguridad. Los SIEM y XDR integrados liberan recursos de SecOps y, al mismo tiempo, empoderan incluso a los analistas junior con más capacidades y confianza.



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

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

- **Se redujo el tiempo para investigar las amenazas en un 65 % y disminuyó el tiempo para responder a las amenazas en un 88 %.** El enfoque integrado de SIEM y XDR de Microsoft para la investigación y respuesta de amenazas de seguridad hace que estos flujos de trabajo sean más eficientes para los profesionales de seguridad de la organización compuesta. Ya no necesitan pasar por varias herramientas para identificar las amenazas, mientras que las características de automatización de seguridad mejoran aún más los flujos de trabajo de respuesta.

- **Se redujo el tiempo para crear un nuevo libro en un 90 % y el tiempo para incorporar a los nuevos profesionales de seguridad en un 91 %.** El enfoque integrado de SIEM y XDR de Microsoft hace que los flujos de trabajo profesionales de seguridad adicionales también sean más eficientes. Como los registros de SIEM están integrados en todo el conjunto de soluciones, la creación de libros está casi automatizada, y un único inicio de sesión permite a los nuevos profesionales de la seguridad incorporarse casi 16 semanas más rápido.

Motivo 3

Incremente la productividad de los empleados

Una solución de SIEM y XDR integrada puede ayudar a su organización a mejorar la productividad para los usuarios finales.

Además de hacer más con menos y aumentar la eficiencia de los equipos de SecOps, una solución de SIEM y XDR integrada puede ayudar a su organización a mejorar la productividad para los usuarios finales.

Como saben los equipos de SecOps, cuando la seguridad es compleja, la gente busca soluciones alternativas. Por lo tanto, cuando las experiencias de los usuarios finales obstaculizan la productividad de los empleados en lugar de ayudarla, la organización puede quedar expuesta a más riesgos de seguridad y costos más altos. Las contraseñas débiles o perdidas, el acceso no seguro a través de dispositivos personales o el uso compartido ilimitado de datos confidenciales son solo algunos de los desafíos.

> [En el pasado] usábamos instrumentos contundentes cuando alguien sospechaba de un problema. Cerrábamos todo y cancelábamos el acceso, lo que afectaba negativamente a nuestro negocio. Y era muy evidente para todos 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, el negocio 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

SIEM y XDR de Microsoft mejoraron la productividad de otros empleados en un total de casi 68 000 horas totales anuales.

Un enfoque de SIEM y XDR integrado le ayuda a ofrecer experiencias de usuario perfectas que mantienen a sus empleados productivos y seguros en todas las facetas de sus experiencias cotidianas. Puede reducir los impactos negativos en la productividad, como tener que desactivar los servicios o aislar y luego volver a diseñar las máquinas. Sin embargo, SIEM y XDR integrados también pueden crear nuevas oportunidades para las ganancias en la productividad de los usuarios finales, como contar con más soporte de seguridad de autoservicio, mejores paneles e informes, y más capacidad de respuesta y tiempos de arranque más rápidos debido a que se ejecutan menos agentes de seguridad.

En el estudio de Forrester Total Economic Impact™ (TEI) encargado por Microsoft, la organización compuesta hipotética con 8000 empleados totales mostró un aumento en la productividad de los empleados mediante la implementación de SIEM y XDR de Microsoft:

- **Se mejoró la productividad de otros empleados en un total de casi 68 000 horas totales anuales.** SIEM y XDR de Microsoft evitan los impactos negativos en otros empleados a partir de procesos de seguridad ineficientes. Por ejemplo, el compuesto ahorra 4000 horas al año gracias a la nueva capacidad de los profesionales de TI para ofrecer autoservicio con respecto a las actualizaciones y recomendaciones de seguridad. También permite la solución remota de problemas basadas en la seguridad en las máquinas de los empleados y reduce la cantidad de agentes de seguridad que se ejecutan en ellas, lo que ahorra casi 64 000 horas al año en productividad del usuario final.

La seguridad se ha convertido en un facilitador esencial del éxito tecnológico. Por ello las organizaciones necesitan medidas de seguridad que creen la mayor resiliencia posible contra los ataques modernos, para proteger y permitir la productividad y la innovación que impulsan el crecimiento.

Obtenga protección contra ciberamenazas integrada con SIEM y XDR

Esta integración de productos líderes en la industria brinda prevención, detección y respuesta frente a ciberamenazas en una única solución integral.

Microsoft ofrece la primera y única solución integrada de SIEM y XDR, que proporciona visibilidad de extremo a extremo en todas las nubes y plataformas. Esta integración de productos líderes en la industria brinda prevención, detección y respuesta frente a ciberamenazas en una única solución integral.

SIEM y XDR de Microsoft aprovecha el poder de la IA y la automatización, así como las inversiones profundas y continuas en la detección y el análisis de ciberamenazas, con información experta y visibilidad de 43 000 billones de señales cada día. Con la integración en estos productos, los equipos de SOC están equipados con más contexto que nunca para detectar y resolver las ciberamenazas críticas más rápido:

Microsoft Sentinel

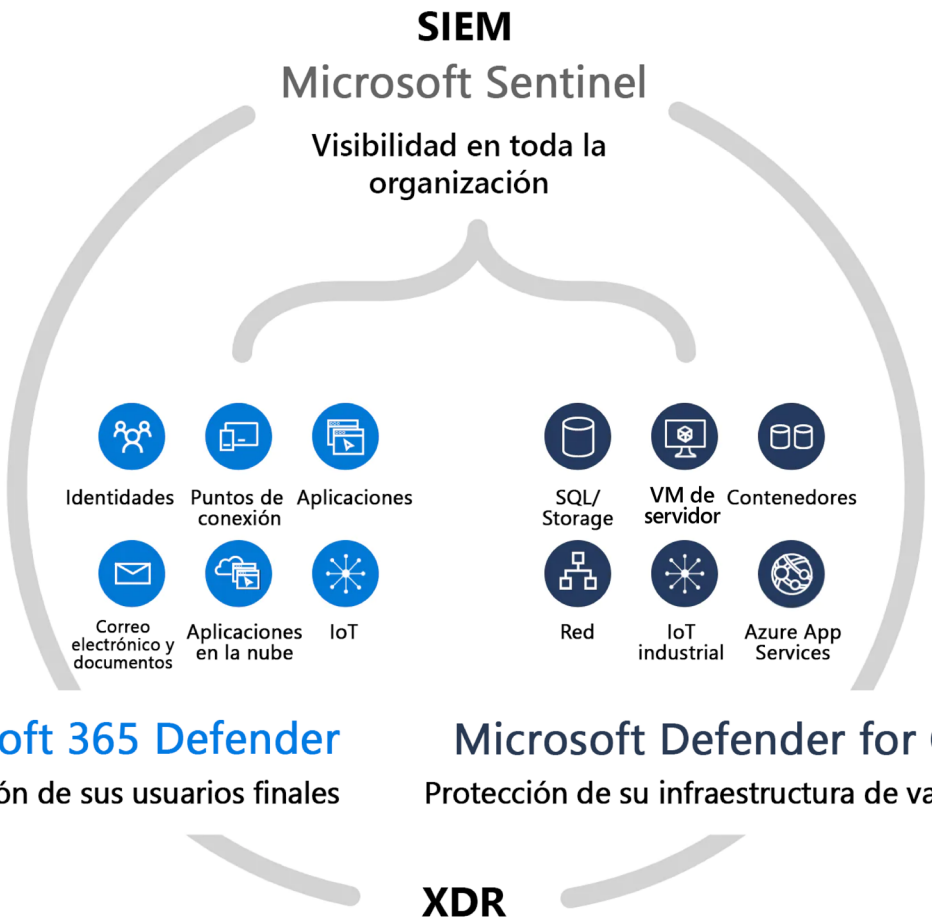
Obtenga una vista panorámica de la empresa con el SIEM nativo de la nube de Microsoft. Agregue datos de seguridad de prácticamente cualquier fuente y aplique IA para separar el ruido de los eventos legítimos, correlacionar las alertas en cadenas de ciberataques complejas y acelerar la respuesta frente a ciberamenazas con orquestación y automatización integradas.

Microsoft Defender XDR

Evite y detecte ciberataques en todas sus identidades, puntos de conexión, aplicaciones, correo electrónico, datos y aplicaciones en la nube con capacidades de XDR. Investigue y responda a los ciberataques con la mejor protección lista para usar. Detecte amenazas y coordine fácilmente su respuesta desde un solo panel.

Microsoft Defender for Cloud

Proteja sus cargas de trabajo de nube híbrida y multinube con las capacidades de XDR integradas. Proteja sus servidores, almacenamiento, bases de datos, contenedores y mucho más. Céntrese en lo que más importa con las alertas priorizadas.



No anexe la seguridad. Intégrela.

Ponga las herramientas y la inteligencia correctas en manos de las personas adecuadas. Defiéndase de los ataques modernos con una solución de extremo a extremo integrada y nativa de la nube.

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

Microsoft Security