Bitdefender®

GravityZone

GUÍA DE SOLUCIONES

Simplifique sus operaciones de seguridad y reduzca los riesgos

¿Y si todo lo que nos han dicho sobre la seguridad informática fuera incorrecto? ¿Y si añadir capas no hiciera que su organización estuviera más protegida, sino que aumentara su vulnerabilidad? La realidad es que muchos de nuestros sistemas se han vuelto tan complejos que ahora constituyen nuestras mayores debilidades.

Cada nueva herramienta de seguridad promete protección, pero también genera confusión y zonas ciegas. Los delincuentes informáticos no derriban nuestras murallas; se cuelan por las grietas que hemos creado. El Foro Económico Mundial lo confirma al decir: ““El ciberespacio es ahora más complejo y desafiante que nunca debido a los rápidos avances tecnológicos, la creciente sofisticación de los delincuentes informáticos y la profunda interconexión de las cadenas de suministro””.

El futuro de la seguridad informática no está en añadir más. Está en simplificar la seguridad, eliminar el ruido y centrarse en lo que realmente importa.

Por qué las amenazas digitales actuales son más difíciles de detectar y detener

Es una historia conocida: las amenazas para la seguridad informática evolucionan día a día, son cada vez más avanzadas y resultan más difíciles de combatir. Las organizaciones trabajan en entornos amplios e interconectados con miles de recursos. Cada nueva iniciativa empresarial incorpora más endpoints, flujos de datos y dependencias. Y aunque todo ello aporta valor, también introduce riesgos.

A medida que su entorno crece, la visibilidad de TI se fragmenta. Es casi imposible correlacionar datos de múltiples fuentes dispares. Su departamento de informática y seguridad, reducido, se esfuerza por atar cabos y puede pasar por alto puntos ciegos que los adversarios explotan rápidamente.

Al mismo tiempo, los atacantes han perfeccionado sus manuales de explotación. Los responsables de los ataques ya no dependen únicamente de la fuerza bruta ni del malware de día cero, sino que dominan las técnicas de tipo living-off-the-land, en las que combinan sus acciones maliciosas con herramientas y procesos legítimos que ya existen dentro de los sistemas de su organización.

Los atacantes encuentran mucho más sencillo llevar a cabo intromisiones, mientras que a los equipos de TI les resulta mucho más complicado detectarlas. Incluso ataques relativamente rudimentarios, cuando se realizan con precisión y sigilo, pueden tener consecuencias devastadoras si logran eludir las defensas durante el tiempo suficiente. Mientras tanto, los atacantes integran la automatización y la IA en sus conjuntos de herramientas, lo que amplifica su alcance y acelera la velocidad con la que identifican vulnerabilidades, explotan brechas y escalan campañas.

Este desafío se agrava porque las amenazas actuales rara vez se limitan a un único punto de ataque. Por diseño, son multifacéticas y golpean de manera simultánea varias capas de la empresa. Por ejemplo, los piratas informáticos pueden comenzar con un correo de phishing, pasar al escalamiento de privilegios, aprovechar recursos en la nube mal configurados y, finalmente, ejecutar un movimiento lateral a través de los endpoints. Cada etapa refuerza la siguiente y genera una cadena de eventos mucho más difícil de interrumpir una vez que está en marcha.

Esta filosofía multicapa implica que el impacto de un ataque ya no se limita a un solo sistema o departamento. Por ejemplo:

- El ransomware a menudo desactiva las copias de seguridad y, al mismo tiempo, extrae datos confidenciales para una doble extorsión
- Las campañas de business email compromise (BEC) pueden llegar mucho más allá de una bandeja de entrada comprometida y a menudo implican fraudes financieros o infiltración en la cadena de suministro.

Como los atacantes pueden explotar varios vectores simultáneamente, aumentan sus posibilidades de éxito y el riesgo de interrupción del negocio. El resultado es una tormenta perfecta: entornos empresariales cada vez más complejos que chocan con adversarios cada vez más eficientes. Y sin la visibilidad adecuada, la comprensión precisa y las capacidades de respuesta apropiadas, las organizaciones tienen dificultades para determinar la mejor forma de priorizar sus esfuerzos de protección.

Más herramientas = más ruido

Los entornos empresariales extremadamente complejos de hoy en día han sometido a los equipos de seguridad a una presión sin precedentes. Cada nuevo dispositivo, aplicación o servicio en la nube aporta su propio conjunto de alertas, registros y vulnerabilidades. Para mantenerse al día, la mayoría de las organizaciones han incorporado una serie de herramientas de seguridad:

- Detección y respuesta en los endpoints
- Cortafuegos
- Protección de la identidad
- Seguridad en la nube y SaaS
- Gestión de vulnerabilidades
- Y un largo etcétera

Sin duda, cada herramienta cumple una función específica. No obstante, intentar unirlas improvisadamente para formar una defensa cohesionada suele generar más problemas de los que resuelve. ¿Por qué?

- **Datos dispares:** Cada plataforma genera sus propios formatos de datos, lógicas de alertas y paneles. Su equipo de seguridad se ve obligado a invertir gran parte de su tiempo en reconciliar esquemas inconsistentes y eventos duplicados en lugar de centrarse en las amenazas de mayor prioridad.
- **Redundancias y ruido:** La funcionalidad superpuesta entre herramientas provoca que un mismo evento genere múltiples alertas, lo que abruma a los analistas, consume tiempo y debilita la confianza en el proceso global de detección.
- **Desafíos de integración:** La integración entre herramientas rara vez resulta fluida. Las API cambian, los conectores fallan y el ajuste de las reglas de correlación exige un esfuerzo de ingeniería continuo que muchos equipos simplemente no pueden mantener.

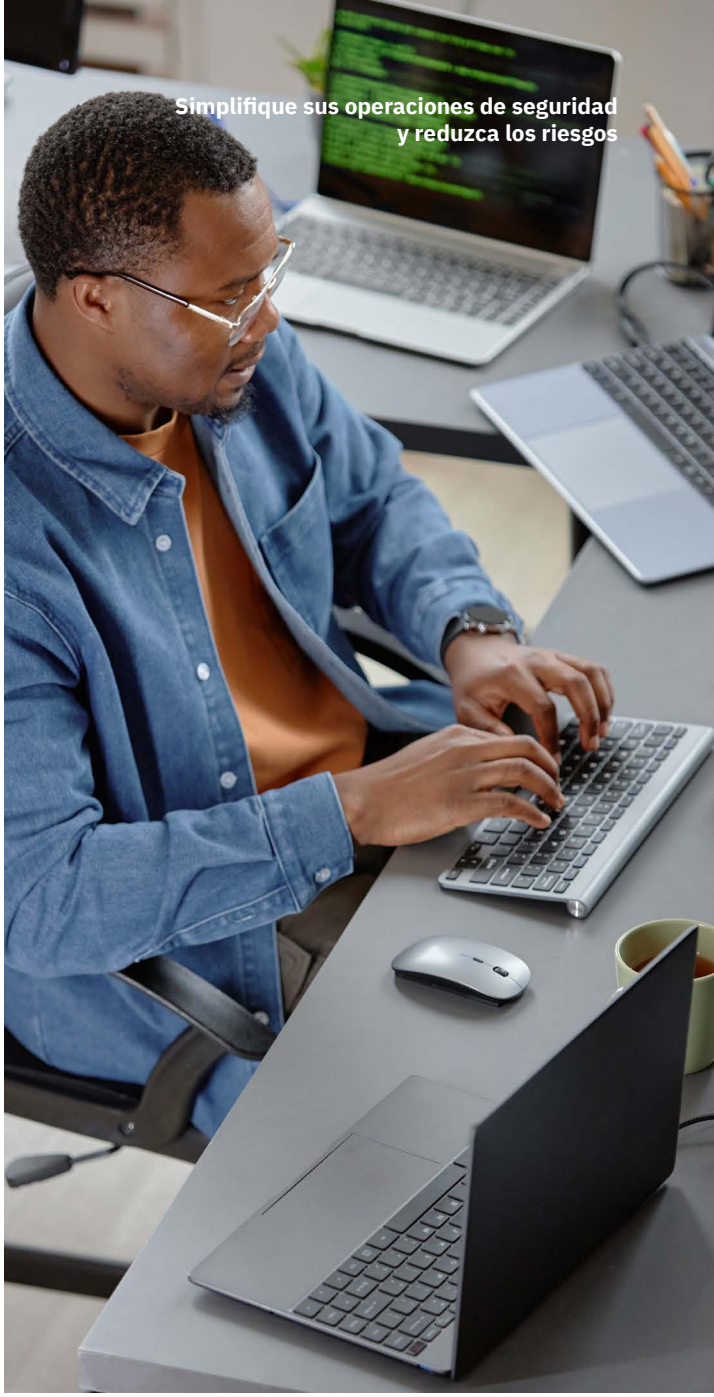
A medida que crece el arsenal de seguridad, disminuye la visibilidad general. La encuesta sobre seguridad en la nube híbrida de Gigamon de 2024 reveló que el 41 % de los CISO estaban preocupados por la proliferación de herramientas y por las brechas de visibilidad y seguridad que generan debido a la falta de integración simplificada y a las dificultades para administrar cada solución. En lugar de contar con una visión unificada, los analistas deben desplazarse por múltiples consolas, cada una con una perspectiva parcial del entorno. Esta visibilidad fragmentada ralentiza la investigación. Los equipos se ven obligados a cambiar de plataforma para reconstruir la secuencia de un ataque, lo que incrementa tanto el tiempo medio de detección (MTTD) como el de respuesta (MTTR).

Para afrontar esta situación, muchas empresas recurren a las plataformas de administración de eventos e información de seguridad (SIEM) y las de orquestación, automatización y respuesta de seguridad (SOAR) para centralizar los datos y automatizar los flujos de trabajo. Sin embargo, las SIEM y las SOAR generan sus propias complejidades, como los elevados costes de ingesta de registros, la fragilidad de las reglas de detección y la necesidad de contar con ingenieros especializados que las ajusten y mantengan.

En el informe “State of SIEM Detection Risk” de CardinalOps de 2025 se constató que, a pesar de ingerir cientos de fuentes de registros, los SIEM suelen cubrir solo una fracción de las técnicas conocidas de los adversarios, lo que deja brechas peligrosas. Las organizaciones siguen “sin observar un aumento proporcional en la cobertura” cuando invierten en SIEM para consolidar la proliferación de sus herramientas.

Entonces ¿cuál es la respuesta? Sin duda, la solución no consiste en añadir más herramientas, sino en adoptar un enfoque integrado que reduzca la complejidad y, al mismo tiempo, mejore la cobertura y los resultados.

Bitdefender



Simplifique sus operaciones de seguridad y reduzca los riesgos

Unificar herramientas para simplificar la seguridad

Con las amenazas en aumento, las herramientas fragmentadas y los equipos reducidos bajo presión, la seguridad informática exige hoy un enfoque cuidadoso y bien planificado. Añadir más productos para endpoints solo multiplica la carga de integración y amplifica el ruido de datos. Lo que su equipo de seguridad necesita es una plataforma unificada que simplifique las operaciones, mejore la visibilidad, automatice la detección y la respuesta, y proporcione la experiencia adecuada bajo demanda.

Hablar el mismo idioma

Una plataforma de seguridad unificada reúne todo el espectro de herramientas y capacidades bajo un mismo techo, garantizando que todas hablen el mismo idioma. En lugar de consolas dispares y datos aislados, las organizaciones pueden administrar la seguridad de endpoints, identidades, nube, red y aplicaciones SaaS desde un único entorno integrado.

Esta consolidación aporta lo siguiente:

- → Reduce la redundancia
- → Recorta los gastos operativos
- → Garantiza que las alertas, los registros y la telemetría fluyan a una capa de inteligencia central donde se puedan correlacionar y analizar en tiempo real

¿El resultado? Operaciones de seguridad simplificadas, con capacidades de detección y respuesta de mayor fidelidad en toda su superficie de ataque.

Prevención, protección, detección y respuesta unificadas

Una plataforma de seguridad unificada refuerza las defensas de la organización al integrar prevención, protección, detección y respuesta en un único sistema conectado. En lugar de tratar estas áreas como funciones separadas, la plataforma correlaciona de manera continua la telemetría de endpoints, identidades, cargas de trabajo en la nube, redes y aplicaciones SaaS. Esto permite identificar con prontitud vulnerabilidades, configuraciones erróneas o actividades anómalas antes de que los atacantes puedan explotarlas, lo que reduce la probabilidad de que los ataques profundicen en el entorno.

La prevención y la protección se optimizan aún más gracias a la aplicación unificada de políticas y a la gestión de vulnerabilidades. Los controles de seguridad, las políticas de acceso y las configuraciones de referencia pueden aplicarse coherentemente en todo el entorno desde una única consola. Cuando se introducen actualizaciones en la lógica de detección o en los canales de inteligencia, estas se distribuyen simultáneamente, lo que garantiza que las defensas se mantengan al día y sincronizadas, además de mejorar la cobertura y reducir la complejidad de mantener controles de ciberseguridad adecuados.

Esta consolidación de herramientas también mejora la visibilidad y facilita la comprensión de la superficie de ataque. Los analistas pueden identificar rápidamente qué activos tienen más probabilidades de ser atacados, priorizar los esfuerzos de reparación en función del riesgo real para el negocio y aprovechar el contexto correlacionado para acelerar las acciones de respuesta. Esta conexión integral, desde la prevención hasta la respuesta, garantiza que las amenazas se detengan antes, que las investigaciones se simplifiquen y que la reparación se ejecute con mayor rapidez y confianza.

Automatización simplificada y más eficiente

Dado que todas las herramientas están interconectadas, la detección y la respuesta ante las amenazas pueden automatizarse y optimizarse, lo que transforma procesos que antes eran manuales y propensos a errores en flujos de trabajo fluidos y fiables. La plataforma correlaciona automáticamente datos, eventos y alertas, con lo cual genera detecciones de alta fidelidad y pone en marcha automáticamente acciones de respuesta.

En lugar de que los analistas pierdan un tiempo valioso pasando de una consola a otra, clasificando alertas superpuestas o intentando integraciones personalizadas, reciben alertas priorizadas y enriquecidas con contexto. La automatización, además, aporta un enorme retorno de la inversión: el informe sobre costes de una filtración de datos de 2024 de IBM puso de manifiesto que las organizaciones con automatización de la seguridad plenamente implementada contienen las brechas 74 días más rápido y ahorran alrededor de un 31 % en los costes que estas conllevan en comparación con aquellas que adolecen de una automatización mínima o inexistente.

Con la automatización, su equipo de seguridad puede detectar amenazas con mayor rapidez (reducir el MTTD), validar incidentes con más confianza y responder más eficazmente a lo largo de toda la cadena de ataque. Esto incluye enriquecer las alertas con inteligencia sobre amenazas, vincular la actividad con las técnicas de MITRE ATT&CK, contener activos comprometidos y generar automáticamente informes listos para las auditorías. La diferencia es transformadora para equipos reducidos y con recursos limitados: los analistas se liberan del trabajo repetitivo de la priorización y pueden centrarse en la búsqueda proactiva de amenazas, la planificación de la resiliencia y las mejoras estratégicas de la seguridad.

La automatización acelera la detección y la respuesta, al tiempo que simplifica las operaciones de seguridad, reduce la complejidad y permite que los equipos reducidos trabajen más eficazmente.

Cómo reforzar su equipo con apoyo especializado

La tecnología por sí sola no puede mantener a salvo a una organización; los equipos también necesitan servicios que refuercen sus conocimientos y aumenten su capacidad. Por ejemplo, colaborar con un proveedor de detección y respuesta administradas (MDR) puede potenciar su seguridad ofreciéndole monitorización permanentemente disponible, detección de amenazas avanzadas y respuesta ante incidentes dirigida por expertos.

Con la MDR, su organización obtiene acceso inmediato a analistas experimentados, buscadores de amenazas y expertos forenses que validan alertas, investigan incidentes y coordinan la respuesta, lo que reduce el tiempo medio de detección y reparación. Al combinarse con inteligencia sobre amenazas continua, monitorización de la Internet oscura y protección de marca, la MDR garantiza que incluso los equipos más reducidos dispongan de visibilidad y protección de nivel corporativo.

No obstante, las plataformas unificadas deben ir más allá de la detección y la respuesta y ofrecer servicios preventivos y de asesoría. Plantéese aprovechar las soluciones de seguridad ofensiva, como las de penetration testing, el red teaming y los simulacros. Estas medidas ayudan a las organizaciones a identificar proactivamente las debilidades antes de que los atacantes las aprovechen.

Los servicios de asesoramiento pueden guiar a su equipo en la creación y maduración de programas de seguridad informática. También garantizan que las políticas, los procesos y los controles se ajusten a las necesidades del negocio y a los requisitos de cumplimiento normativo.

Facilitar una comunicación clara y demostrar valor

Finalmente, una plataforma unificada no solo simplifica el trabajo de los profesionales de la seguridad, sino que también transforma la manera de comunicar la información en toda la organización. Como toda la telemetría, las alertas y los resultados se concentran en una capa de inteligencia centralizada, la plataforma puede presentar la información en formatos adaptados a diferentes audiencias. Los analistas se benefician de alertas enriquecidas con contexto y datos forenses detallados, mientras que los directivos, los consejos y los responsables de cumplimiento normativo visualizan paneles claros que destacan tendencias, KPI y la posición general de riesgo.

Esta claridad permite que los especialistas desempeñen sus responsabilidades con mayor eficacia. Los directivos pueden comprender fácilmente la situación de la organización, los consejos pueden evaluar con confianza las inversiones en seguridad y los equipos de cumplimiento pueden generar evidencias listas para las auditorías sin necesidad de traducción técnica. La capacidad de presentar los resultados de seguridad en términos simples y accesibles garantiza que el valor de la función de seguridad no solo se perciba internamente, sino que también se demuestre externamente ante las partes interesadas y los reguladores.

El resultado es un programa de seguridad no solo más sólido, sino también más transparente, responsable y estratégicamente en sintonía con los objetivos empresariales. Al simplificar cómo se consume la información, las plataformas unificadas permiten que la seguridad evolucione desde una disciplina puramente técnica hacia un facilitador integrado del negocio.

Diseño pensado para los equipos de seguridad reducidos

A diferencia de los conjuntos de herramientas ensamblados a partir de productos de seguridad dispares, las plataformas unificadas hacen hincapié en la simplicidad, la integración y los resultados medibles. Esta filosofía de diseño implica menos interfaces que aprender, una implementación más rápida y un nivel de automatización que amplifica las capacidades de los equipos pequeños. Los equipos de seguridad acceden a funciones de nivel corporativo sin la carga de administrar la complejidad propia de ese entorno. La plataforma ofrece la visibilidad, prevención, protección, detección y respuesta necesarias para defenderse de las amenazas modernas, pero de una manera asumible y sostenible con equipos que disponen de personal limitado.

Los resultados incluyen una contención más rápida de las amenazas, una reducción más proactiva de las vulnerabilidades y la garantía de que los esfuerzos de seguridad están en consonancia con el riesgo empresarial. Al disminuir el tiempo dedicado a la priorización manual y al mantenimiento de herramientas, los equipos reducidos pueden invertir más energía en iniciativas estratégicas, como la planificación de la resiliencia, el cumplimiento normativo y la elaboración de informes ejecutivos.

Centrarse en lo que más importa

¿Listo para hacer más con menos? Cree una plataforma de seguridad unificada consolidando las herramientas tecnológicas y colaborando con proveedores de servicios expertos. En lugar de verse abrumado por datos y alertas fragmentadas, podrá centrarse en lo que realmente importa: mantener a salvo los datos y los sistemas de su organización.

¿Busca seguridad de nivel corporativo sin la complejidad que esta conlleva? Las soluciones de seguridad empresarial de Bitdefender pueden ayudarle a mitigar proactivamente los riesgos y defenderse de las amenazas.

LEARN MORE

Sede central en Rumanía
Orhideea Towers
Calle Orhideelor 15A,
Distrito 6,
Bucarest 060071

T: +40 21 4412452

Oficina en España
75-77 Calle Sants,
Principal 2ª, 08014
Barcelona, Spain

Fecha de lanzamiento: octubre de 2025