

Bitdefender®

GravityZone

GUÍA DE SOLUCIONES

Cómo crear un programa de seguridad sólido con un equipo reducido



Todos los derechos reservados. © 2025 Bitdefender. Todas las marcas comerciales, nombres comerciales y productos a los que se hace referencia en este documento son propiedad de sus respectivos dueños. La información contenida en este documento es confidencial y solo para el uso de su destinatario previsto.

No puede publicar ni redistribuir este documento sin el permiso previo de Bitdefender.

La mayoría de los informes sobre seguridad informática comienzan con advertencias a cerca de nuevas amenazas, pero para los equipos reducidos, el verdadero reto reside en otro aspecto. Destacan estadísticas alarmantes, como los [55 000 millones de dólares](#) perdidos por vulneraciones de BEC (business email compromise) acaecidas durante la última década¹, el aumento del 66 % en los incidentes de BEC o la presencia de ransomware en el 44 % de las violaciones de la seguridad, con un aumento interanual del 37 %².

Aunque estas cifras ayudan a concienciar a los consejos de administración y a los ejecutivos, no son una novedad para los líderes de TI y seguridad, quienes saben que estas amenazas han ido en aumento desde hace años. Sin embargo, lo que sí es nuevo es la creciente huella digital de las organizaciones y la ampliación de la superficie de ataque que ello conlleva.

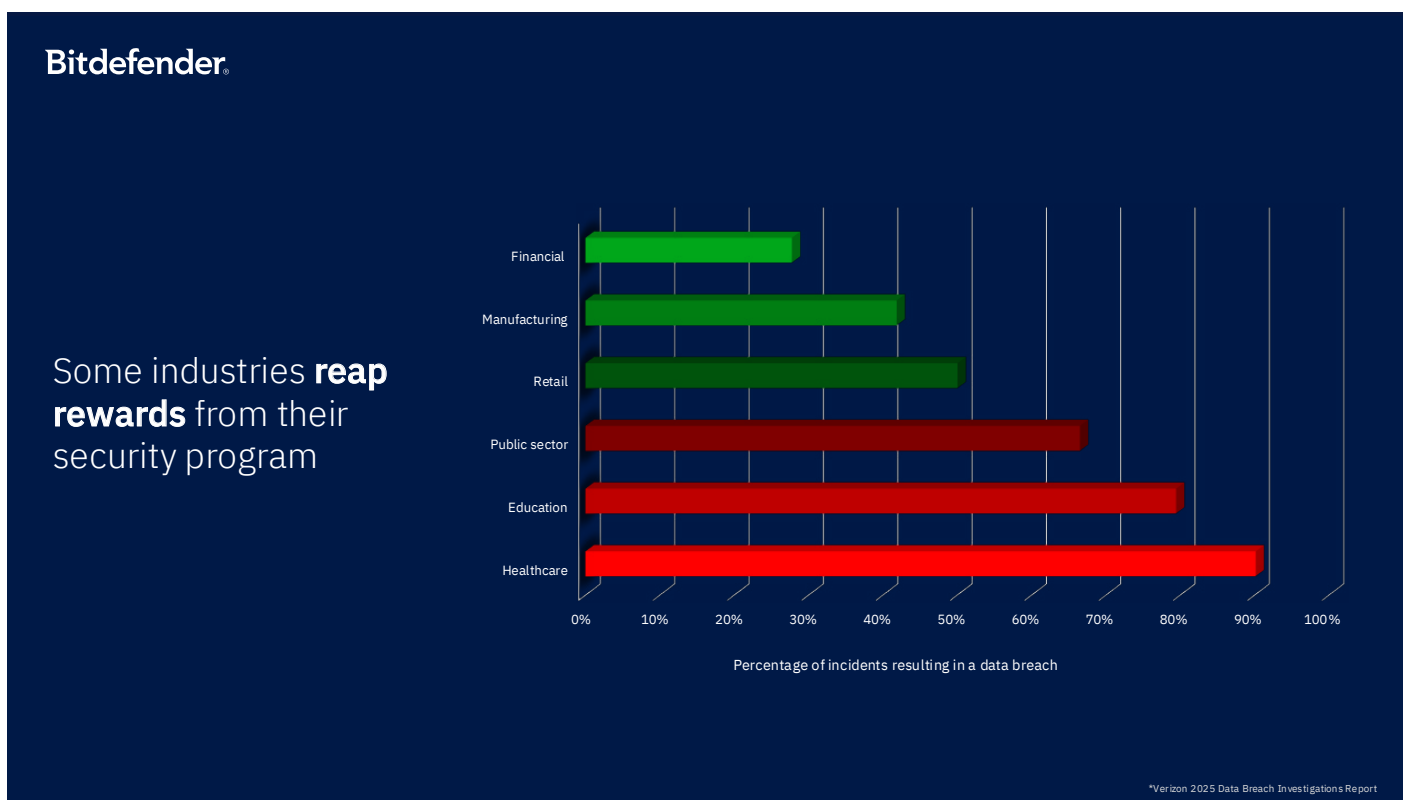
Si carece de visibilidad de todos sus recursos internos y externos, incluida su shadow IT, sus aplicaciones en la nube y los datos que fluyen hacia las herramientas de IA, puede estar seguro de que los atacantes encontrarán debilidades de las que aprovecharse. Su gente y su cadena de suministro también forman parte de su superficie de ataque y pasarlos por alto puede crear importantes puntos ciegos.

Los resultados del Informe de investigaciones de vulneraciones de datos de Verizon 2025 muestran que el 60 % de las filtraciones involucran a usuarios y el 30 % a terceros². Las investigaciones llevadas a cabo por Bitdefender también muestran una preocupante tendencia reciente: en el 84 % de los incidentes, los atacantes secuestran herramientas legítimas ya instaladas en los dispositivos. No se trata de vulnerabilidades que requieran parches, sino que son herramientas diseñadas para un uso legítimo, lo que significa que detectar este abuso puede representar un gran problema.

Hallazgos adicionales de Verizon ponen de manifiesto que las organizaciones dedican aproximadamente 32 días a corregir problemas en los dispositivos perimetrales², lo que los deja expuestos durante demasiado tiempo. Esto pone de relieve las consecuencias de una visibilidad limitada, ya que las vulnerabilidades que no se detectan rápidamente no pueden repararse con rapidez. El verdadero reto reside en obtener la visibilidad necesaria para acortar la ventana de exposición, incluso con recursos limitados y un equipo reducido.

¿Quién está haciendo lo correcto en materia de seguridad?

El porcentaje de incidentes de seguridad que se convierten en vulneraciones de datos reales varía ampliamente según los sectores, lo que refleja diferencias en cuanto a la inversión en seguridad y a la madurez de los programas.



Las instituciones financieras, que están altamente reguladas y normalmente tienen importantes presupuestos de seguridad, comunican las tasas más bajas de violaciones de la seguridad, seguidas por el sector manufacturero. Esto sugiere que los programas de seguridad estructurados y los recursos dedicados pueden reducir notablemente las probabilidades de que los incidentes lleguen a convertirse en vulneraciones. En el otro extremo del espectro, los sectores que dependen en gran medida de la financiación pública, incluido el sector público, la educación y la atención sanitaria, afrontan dificultades mucho mayores.

Si analizamos los mismos datos desde la perspectiva del tamaño de las empresas, las organizaciones más grandes resultan claramente ganadoras. Casi un 20 % menos de organizaciones con más de mil empleados sufrieron una vulneración de seguridad como resultado de un incidente, en comparación con las organizaciones de menos de mil empleados².

La conclusión clara que se desprende de todo esto es que las organizaciones que priorizan e invierten en seguridad informática a través de políticas, tecnología y formación del personal obtienen mejores resultados cuando surgen incidentes. Por el contrario, aquellas con recursos limitados o programas menos maduros son mucho más vulnerables, y los incidentes de seguridad tienen muchas más probabilidades de convertirse en vulneraciones dañinas.

La pregunta es: ¿qué están haciendo bien estas empresas y cómo puede usted hacer lo mismo?

Cómo proteger su empresa durante todo el ciclo de vida de los ataques

Las organizaciones que implementan correctamente la seguridad cuentan con programas maduros basados en marcos de gestión de riesgos y cumplimiento normativo, e implementan la seguridad a lo largo de todo el ciclo de vida de los ataques.



A continuación, se presenta un breve resumen de cada etapa y su importancia:

1. Prevención

La primera etapa es la prevención, que implica obtener visibilidad completa de la superficie de ataque, identificar riesgos y evaluar vulnerabilidades. Con estos conocimientos, usted puede comprender claramente qué está defendiendo, lo cual le ayuda a reducir proactivamente su exposición ante amenazas potenciales.

2. Protección

Aquí, los equipos implementan herramientas automatizadas para detener o bloquear los ataques antes de que puedan ejecutarse, lo que minimiza las posibilidades de sufrir un compromiso.

3. Detección

Las organizaciones reconocen que ningún sistema es completamente impenetrable y, por lo tanto, invierten en tecnologías capaces de identificar rápidamente ataques que eluden las medidas preventivas, con el fin de limitar los posibles daños.

4. Respuesta

Cuando se producen incidentes, las organizaciones de alto rendimiento tienen la capacidad de contener rápidamente la amenaza, investigar lo sucedido, recuperarse de cualquier impacto e implementar acciones correctivas para evitar que se repita.

La velocidad es fundamental en la detección y la respuesta. Los equipos de seguridad monitorizan métricas como el tiempo medio de detección (MTTD), el tiempo medio de contención (MTTC) y el tiempo medio de respuesta (MTTR) para mejorar continuamente las operaciones de seguridad.



Por qué es clave la prevención proactiva

La idea fundamental aquí es que destacar en la fase de prevención proactiva constituye un factor decisivo para reducir la probabilidad de que un incidente se convierta en una brecha de seguridad.

Al gestionar eficazmente todo el ciclo de vida de los ataques, desde la prevención y la protección hasta la detección y la respuesta, las organizaciones más eficaces aumentan drásticamente su resiliencia y reducen las tasas de vulneraciones incluso cuando se producen ataques.

Para los líderes de seguridad, esto plantea una importante pregunta: ¿están midiendo el rendimiento de SecOps con estas métricas y tienen visibilidad de cada etapa del ciclo de vida de su ataque? Comprender esto puede revelar brechas en su programa y resaltar oportunidades para reforzar sus defensas donde más importa.

La proliferación de herramientas crea complejidad

La proliferación de herramientas es uno de los retos más importantes que afrontan las modernas operaciones de seguridad informática, ya que incrementa los costes y la complejidad. De media, las organizaciones utilizan 83 soluciones de seguridad distintas, según un estudio de IBM³. Para ilustrar la magnitud de este problema, el 52 % de los profesionales de la seguridad afirman que la complejidad es el mayor impedimento para una operativa eficaz³.

Algunas de las categorías de herramientas de seguridad más comunes incluyen las siguientes:

- ▶ Herramientas de gestión de la superficie de ataque, que monitorizan diversos recursos.
- ▶ Herramientas de protección, como seguridad de endpoints, correo electrónico, web y red.
- ▶ Tecnologías de detección que se implementan en todos los puntos de incursión y recursos.
- ▶ Plataformas de gestión de incidentes y eventos, que intentan dar sentido a las alertas de las otras herramientas.
- ▶ Herramientas de respuesta y recuperación, que ayudan a contener, analizar y reparar los efectos de los ataques.

Las empresas adoptan esta compleja combinación de herramientas para cubrir cada etapa de un ataque, y cada herramienta cumple una función específica. Lamentablemente, la gran cantidad de herramientas también crea fricción operativa, aumenta los costes y requiere experiencia en SecOps altamente especializada que resulta cara y puede ser difícil de contratar y conservar. Lo más importante es que cada herramienta aumenta la superficie de ataque y sube las posibilidades de que surjan configuraciones erróneas de las que los atacantes puedan aprovecharse.

Estos hallazgos muestran la importancia de consolidar y optimizar sus herramientas siempre que se pueda. Simplificar un entorno de seguridad complejo reduce su riesgo operativo y hace que sus defensas sean más eficaces, al tiempo que reduce sus costes a lo largo del tiempo.

Cómo el enfoque de plataforma controla la proliferación de herramientas

La solución ideal para reducir la proliferación y la complejidad de las herramientas es una plataforma de seguridad informática unificada. En teoría, esta plataforma consolidaría múltiples funciones de seguridad en un único entorno integrado. Agilizaría la prevención, la protección, la detección y la respuesta a lo largo de todo el ciclo de vida de los ataques, reduciendo la complejidad operativa y reduciendo los costes.

Desgraciadamente, la posibilidad de integrarlo todo tiene sus límites. Ninguna organización puede (ni debe) embutir a la fuerza todas las herramientas y procesos en una única plataforma. Las grandes empresas, con cuantioso presupuesto y amplios equipos de SecOps, a menudo operan con docenas de herramientas especializadas y pueden absorber la complejidad que ello conlleva. Para ellos, la adopción rara vez ha sido una preocupación porque disponen del personal y la experiencia para gestionar múltiples soluciones, incluso aunque eso cree ineficiencias y superficies de ataque adicionales.

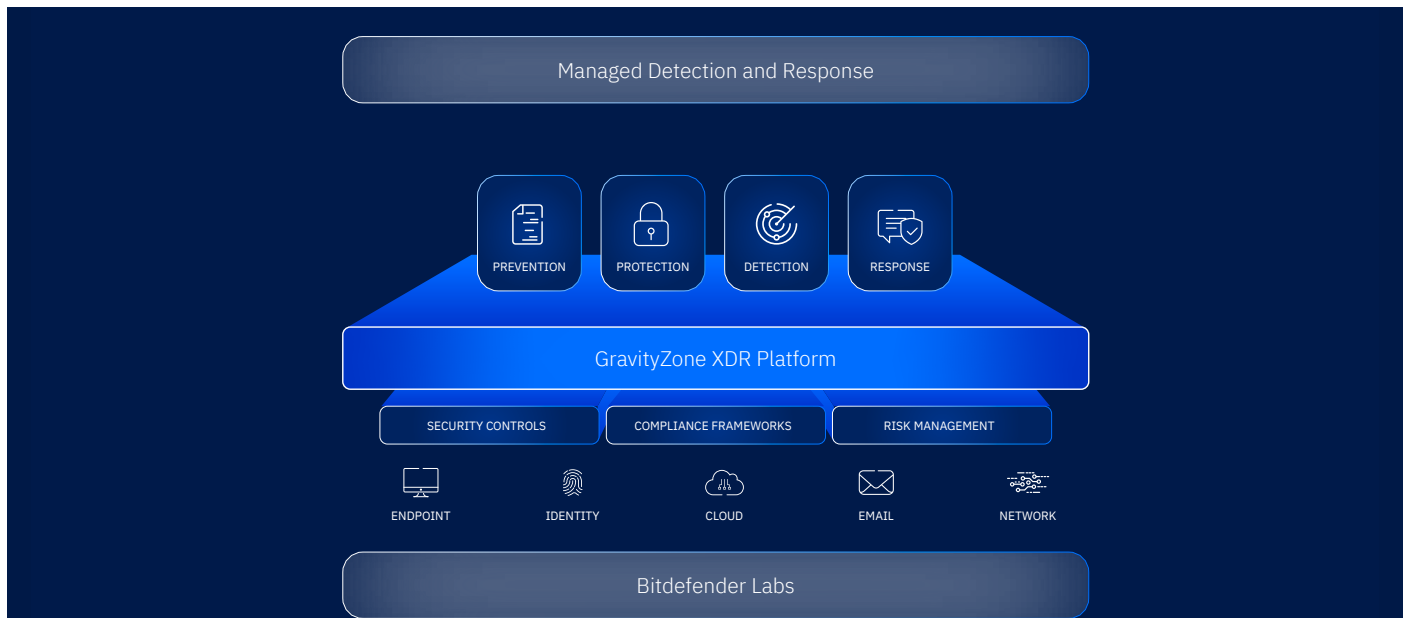
El enfoque de la plataforma se vuelve particularmente valioso para empresas de tamaño medio con equipos de TI y seguridad reducidos. En estas organizaciones, la proliferación de herramientas introduce un riesgo significativo, ya que las configuraciones erróneas, la demora en las respuestas y las brechas en la cobertura pueden escalar rápidamente a incidentes importantes. La plataforma adecuada consolida funciones esenciales, elimina herramientas redundantes y centraliza la administración. Esto permite que los equipos más pequeños operen con la escala y la eficiencia de departamentos de seguridad mucho más grandes.

Reducir la complejidad e integrar las capacidades esenciales son las principales fortalezas de una plataforma unificada. Permite a las medianas empresas proteger su negocio de forma integral sin depender de grandes equipos de expertos. Ofrece visibilidad a lo largo de todo el ciclo de los ataques, automatiza funciones críticas y simplifica tanto la detección como la respuesta.

Aunque no se trata de una solución universal, para las empresas que lidian con demasiadas herramientas y muy pocos recursos, una plataforma cuidadosamente seleccionada puede transformar un entorno de seguridad potencialmente caótico en un programa ágil, eficaz y fácil de gestionar. En resumen, ofrece una protección de nivel empresarial con mucha menos complejidad.

GravityZone ofrece protección sin complejidad

Bitdefender desarrolló GravityZone para resolver los desafíos descritos anteriormente, planteados por la proliferación de herramientas, la complejidad operativa y los crecientes costes de la seguridad informática. Combina las ventajas de las herramientas especializadas, sin los costes ni la necesidad de un gran equipo de profesionales de la seguridad.



GravityZone, diseñado partiendo de cero, tiene tres objetivos principales:

1. Protección integral durante todo el ciclo de vida de las amenazas o los ataques

GravityZone está pensado para brindarle toda la seguridad que necesita durante el ciclo completo de vida del ataque, cubriendo prevención, protección, detección y respuesta. Esta cobertura garantiza que las organizaciones puedan defenderse de los ataques en cada etapa, lo que reduce las probabilidades de sufrir vulneraciones aunque se produzcan incidentes.

2. Simplificación de las operaciones de seguridad

Al simplificar las operaciones de seguridad, GravityZone permite a los equipos lograr eficientemente sus objetivos y minimizar los riesgos. La consolidación de funciones clave en un único entorno integrado reduce la complejidad, el coste y la carga operativa que suelen asociarse a la administración de múltiples soluciones puntuales.

3. Con el respaldo de tecnologías de seguridad fiables de eficacia probada

La base de la plataforma reside en los laboratorios de Bitdefender. Con más de 16 años de innovación en inteligencia artificial, los laboratorios de Bitdefender analizan diariamente más de 500 000 nuevas variantes de amenazas para ofrecer un arsenal integral de prevención y protección que permite a las organizaciones con equipos reducidos implementar eficazmente ciberseguridad de extremo a extremo.

Las tecnologías de seguridad de Bitdefender están validadas por cientos de evaluaciones llevadas a cabo por instituciones independientes. Sus logros clave incluyen una tasa de respuesta ante las amenazas del 99,3 %, puntuaciones perfectas en pruebas de resistencia, una visibilidad del 100 % de la cadena de ataque y el mayor porcentaje (93 %) de informes útiles con la menor cantidad de notificaciones enviadas.

Cómo mejora GravityZone la seguridad durante todo el ciclo de vida de los ataques

GravityZone ayuda a los equipos de TI y seguridad a reducir los riesgos y actuar más eficientemente durante todo el ciclo de vida del ataque al combinar prevención, protección, detección y respuesta en una sola plataforma.

Prevención

GravityZone fortalece las estrategias de reducción de riesgos proporcionando visibilidad continua en toda la superficie de ataque. Identifica vulnerabilidades, configuraciones erróneas, comportamientos arriesgados y objetivos de alto valor, lo que permite a las organizaciones priorizar las acciones correctivas en función de la gravedad y su impacto potencial.

En las pruebas realizadas, el endurecimiento proactivo y la reducción de la superficie de ataque (PHASR) de Bitdefender demostraron su impacto al disminuir un 95 % ciertos tipos de ataques.

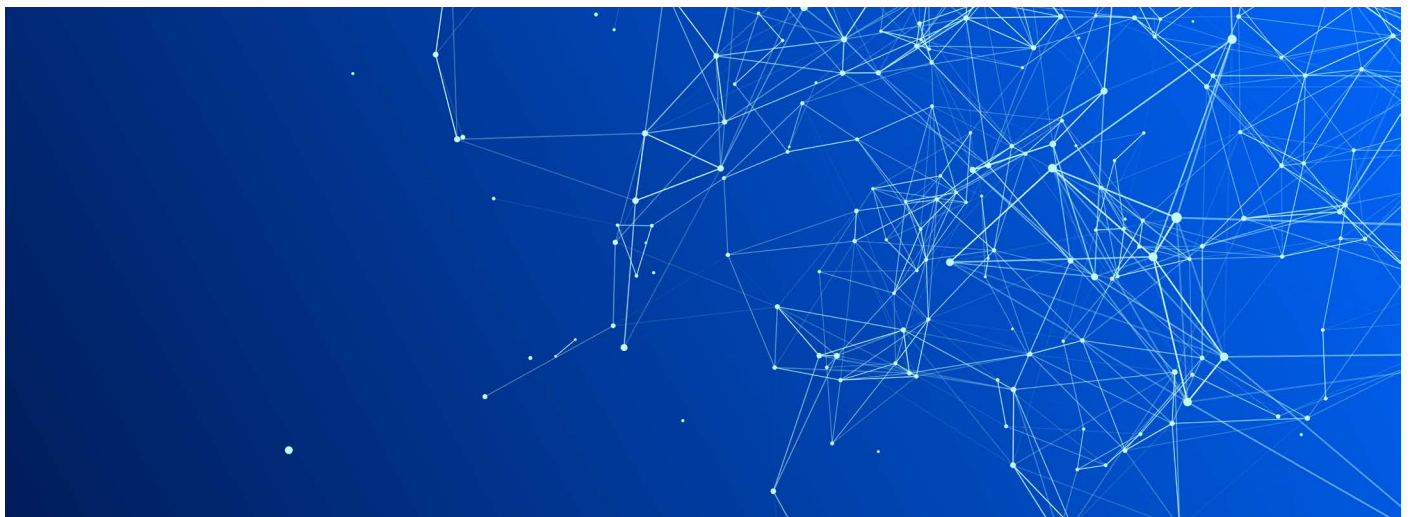
La plataforma está diseñada para fortalecer los esfuerzos de cumplimiento normativo contrastando los recursos respecto a los marcos regulatorios, generando puntuaciones de conformidad, identificando brechas y ofreciendo recomendaciones prácticas. Los informes automatizados demuestran el retorno de la inversión de los programas de gestión de riesgos y brindan evidencias para las auditorías, lo que ofrece al equipo de liderazgo una prueba tangible de las mejoras en cuanto a la posición de seguridad.

Protección

Las organizaciones pueden bloquear automáticamente las amenazas en todos los recursos y puntos de incursión empleando las tecnologías de protección multicapa de GravityZone. Impedir que los atacantes lleguen a afianzarse reduce las probabilidades de que se produzca un incidente, así como la carga de responder ante él.

Pruebas llevadas a cabo por instituciones independientes confirman la alta eficacia y precisión de GravityZone con un mínimo de falsos positivos. Uno de los clientes de Bitdefender incluso informó de una caída del 80-90 % en el volumen de incidentes de seguridad relacionados con los endpoints.

La protección es la segunda línea de defensa proactiva, que minimiza las probabilidades de vulneraciones y permite que los equipos de seguridad se centren en tareas de mayor prioridad mientras mantienen una sólida cobertura en toda la organización.



Detección

Si un ataque logra eludir sus medidas proactivas, GravityZone le ayuda a detectarlo rápidamente correlacionando alertas en todos los recursos y vectores de amenaza. Identifica comportamientos anómalos, movimientos laterales y usos indebidos de credenciales en dispositivos administrados y sin administrar.

Está diseñado para permitir una rápida respuesta y contención mediante la priorización y correlación de señales y alertas, así como la presentación de incidentes en un formato fácilmente comprensible. La visibilidad contextual de recursos de alto valor y en riesgo mejora la toma de decisiones, mientras que el análisis automatizado de la ruta de ataque reduce el tiempo de investigación y resolución.

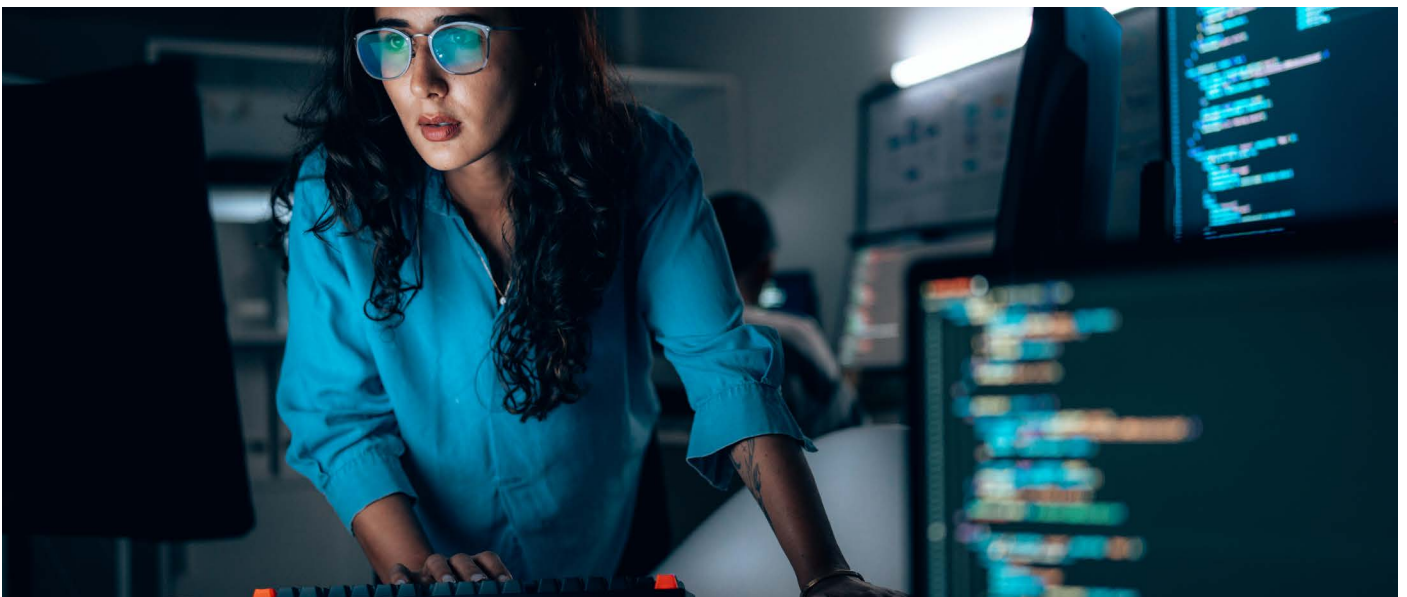
Un cliente de Bitdefender afirmó que la valiosa información proporcionada por GravityZone redujo a la mitad el tiempo que dedicaba a la investigación y resolución de problemas de seguridad.

Este enfoque holístico permite a su organización detectar las amenazas con prontitud y responder rápidamente, lo que limita los daños y las interrupciones en su negocio.

Respuesta

Los equipos de seguridad deben poder contener, investigar y reparar los efectos de los ataques rápidamente. GravityZone permite llevar a cabo acciones con un solo clic para aislar endpoints, cerrar procesos maliciosos y restaurar sistemas. También proporciona análisis posterior al incidente con el fin de descubrir información sobre la causa raíz e identificar rutas de ataque, lo que ayuda a realizar esfuerzos correctivos para evitar que vuelva a producirse. Además, la elaboración de informes exhaustivos respalda los requisitos normativos de notificación y garantiza una comunicación transparente con las partes interesadas.

Al combinar una rápida contención con información forense detallada se minimiza el tiempo de inactividad, el impacto económico y el riesgo para la reputación, de modo que sus equipos puedan mantener la continuidad del negocio incluso durante los incidentes.



Managed Detection & Response

La detección y respuesta administradas (MDR) puede ayudarle a superar las limitaciones de recursos y conocimientos avanzados al brindarle soporte de SecOps a cualquier día y hora. Puede optar por ampliar su personal de seguridad actual o subcontratar a los expertos de Bitdefender para reducir sus necesidades de contratación y formación.

Bitdefender ha sido reconocido como proveedor representativo en la Guía de mercado de Gartner para MDR y cuenta con una valoración media de 4,8/5 en Gartner Peer Insights.

El servicio de MDR de Bitdefender va más allá de las alertas: su equipo responde activamente y contiene los ataques en su nombre, al tiempo que sus expertos le proporcionan orientación para mejorar las habilidades de sus equipos internos. Esto incluye recomendaciones personalizadas, apoyo para la búsqueda de amenazas y conocimientos estratégicos para ayudar a su organización a mantenerse en vanguardia de las amenazas en permanente evolución.

La MDR permite que su reducido equipo de TI y seguridad alcance niveles de seguridad similares a los de sus homólogos y competidores de la gran empresa, y le brinda mayor confianza al saber que su entorno está monitorizado de forma continua.

Un cliente de Bitdefender afirmó que le habría costado cinco veces más crear su propio SOC, mientras que otro dijo que el servicio de Bitdefender le ahorró un 40 % en costes operativos.

Laboratorios Bitdefender

Los productos y servicios de Bitdefender se sustentan en tecnologías de seguridad innovadoras, desarrolladas y respaldadas por el equipo de los laboratorios de Bitdefender. Impulsan la plataforma GravityZone y están licenciadas y las utilizan más de 200 proveedores de tecnología y de servicios en sus propios productos.

El rendimiento y la eficacia de estas tecnologías se demuestran de forma regular mediante evaluaciones independientes llevadas a cabo por terceros, y Bitdefender mantiene una valoración destacada tras haber participado en más de 450 pruebas publicadas.

Casi la mitad del personal de Bitdefender trabaja en I+D, y la innovación está impulsada por la colaboración con el mundo académico para investigar temas de vanguardia, como redes neuronales, computación cuántica y deepfakes. El equipo también mantiene estrechos vínculos con las fuerzas del orden, con 32 colaboraciones con cuerpos de todo el mundo, incluidas Europol, Eurojust e Interpol.

Esa validación nos ayuda a garantizar que GravityZone se mantenga a la vanguardia en prevención, protección, detección y respuesta frente a las amenazas para los clientes de Bitdefender.

Lograr una protección a nivel empresarial con equipos reducidos

GravityZone se ha diseñado específicamente para brindar seguridad integral de nivel empresarial y, al mismo tiempo, optimizar las operaciones para equipos de TI reducidos.

A modo de resumen, estos son los cinco resultados principales que las organizaciones logran al adoptar GravityZone:

1. Reducir de forma demostrable el riesgo a lo largo de todo el ciclo de vida de un ataque informático

GravityZone proporciona prevención, protección, detección y respuesta unificadas. El hecho de que los productos y servicios de Bitdefender cuenten con el reconocimiento de más de 20 informes de analistas actuales de Gartner, Forrester e IDC respalda su capacidad en materia de seguridad.

2. Reduzca el plazo de valor

La implementación rápida y sencilla ofrece visibilidad inmediata de los riesgos, lo que le permite priorizar adecuadamente los esfuerzos de reparación y mitigación. La plataforma tiene una alta calificación en cuanto a integración e implementación en Gartner Peer Insights (4,6/5).

3. Aumentar la eficiencia y la productividad en equipos reducidos de TI y seguridad

GravityZone cuenta con una interfaz única e intuitiva con amplias capacidades de automatización. Con esa configuración, el personal de TI puede realizar rápidamente las tareas de seguridad informática, mientras que las capacidades avanzadas permanecen a disposición de los especialistas. Un cliente informó en Peer Insights de una reducción del 70 % en el tiempo dedicado diariamente a la administración de seguridad desde que se pasó a Bitdefender.

4. Reducir el coste total de propiedad

La consolidación de herramientas y la optimización de las operaciones reducen la dependencia de grandes equipos de profesionales de la seguridad con altos salarios. Un cliente informó de que había logrado un retorno de la inversión del 120 %, mientras que otro dijo haber reducido a la mitad los costes operativos sin sacrificar la efectividad.

5. Invertir con confianza en una seguridad que crece con su negocio

El sistema de licencias modular y flexible y las actualizaciones continuas de I+D permiten que la plataforma evolucione al ritmo de las amenazas emergentes. Además, le ofrecen la posibilidad de seguir incorporando las funcionalidades que necesite a medida que su programa madura.

Estos resultados demuestran cómo GravityZone refuerza la posición de seguridad de su organización a lo largo de todo el ciclo de vida de los ataques. Además, permiten cuantificar un retorno de la inversión medible y reducciones significativas en los costes operativos.

[Visite nuestro sitio web](#) para descubrir cómo GravityZone puede ayudarle a suprimir la complejidad y reducir los riesgos con una seguridad optimizada para su negocio que lidera sistemáticamente las evaluaciones realizadas por instituciones independientes.

Notas finales

- 1 [Anuncio del FBI IC3 I-091124-PSA, 11 de septiembre de 2024](#)
- 2 Informe sobre investigaciones de vulneraciones de datos de Verizon 2025
- 3 [IBM Institute for Business Value: Cómo aprovechar el dividendo de la seguridad informática](#)

Bitdefender es líder mundial en seguridad informática y ofrece las mejores soluciones de prevención, detección y respuesta ante amenazas en todo el mundo. Bitdefender, que vela por millones de entornos domésticos, empresariales y gubernamentales, es uno de los expertos más confiables en el sector para eliminar amenazas, proteger la privacidad, la identidad digital y los datos, y facilitar la resiliencia informática. Gracias a sus grandes inversiones en investigación y desarrollo, los laboratorios de Bitdefender descubren más de 400 nuevas amenazas por minuto y procesan diariamente 40 000 millones de consultas sobre amenazas. La empresa ha sido pionera en innovaciones revolucionarias en el campo de la seguridad de IoT, antimalware, análisis del comportamiento e inteligencia artificial (AI), y más de 150 de las marcas tecnológicas más reconocidas del mundo licencian su tecnología. Fundada en 2001, Bitdefender tiene clientes en más de 170 países con oficinas por todo el mundo.

Fecha de lanzamiento: septiembre de 2025

Para obtener más información, visite <https://www.bitdefender.com/es-es/>.

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