

# Bitdefender®

## GravityZone

## Guía del comprador para medianas empresas

Cómo elegir la plataforma de seguridad adecuada

GUÍA DEL COMPRADOR



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.

Se prohíbe publicar o redistribuir este documento sin el permiso previo de Bitdefender.

## ¿Le conviene tener una plataforma de seguridad?

Las medianas empresas con equipos de informática y seguridad reducidos sufren desafíos de ciberseguridad similares a los de sus equivalentes de mayor tamaño y competidores con amplios presupuestos y un ejército de profesionales de seguridad y gestión de riesgos. Puede que su superficie de ataque no sea tan extensa como la de ellos, pero probablemente se ha ido ampliando notablemente durante los últimos años, lo que le expone más al ransomware y a otros responsables de amenazas.

No obstante, puede que los desafíos de su negocio sean más complejos. El Informe sobre investigaciones de vulneraciones de datos de Verizon 2025 puso de relieve que el 30 % de las filtraciones que se comunicaron involucraban a terceros<sup>1</sup>. Este nivel de ataques a la cadena de suministro ha conducido a que las organizaciones examinen rigurosamente a sus socios comerciales, que deben demostrar que cuentan con las medidas de seguridad adecuadas. Si usted no lo hace, podría perder negocios frente a la competencia o, en el mejor de los casos, retrasar la obtención de ingresos debido a un proceso de incorporación prolongado mientras se audita su posición de seguridad.

## ¿Cómo seguir siendo competitivo y no perder negocios frente a competidores con mayores recursos y financiación?

Una plataforma de seguridad podría ser la respuesta no solo para proteger su negocio, sino también para demostrar que lo hace. Esto le permitirá generar ingresos más rápidamente y, si se encuentra en un sector regulado, reducirá el esfuerzo requerido para las auditorías de cumplimiento normativo.

Esta guía del comprador describe seis pasos clave para ayudarle a saber si una plataforma de seguridad es adecuada para usted.

**1** ¿En qué estado se halla mi programa de seguridad?

**2** ¿Me conviene tener una plataforma de seguridad?

**3** ¿Cómo elijo la plataforma adecuada?

**4** ¿Cómo elijo el proveedor adecuado?

**5** ¿Cómo puedo sacar el mayor provecho a la plataforma que elija?

**6** Validar mi elección

Cuando haya dado estos seis pasos y confirme que lo mejor para usted y para su negocio es disponer de una plataforma, en la última sección de esta guía encontrará las preguntas que debe hacer a su lista de proveedores seleccionados para asegurarse de tomar la decisión adecuada en cuanto a cuál satisface mejor sus requisitos.

1 ¿En qué estado se halla mi programa de seguridad?

2 ¿Me conviene tener una plataforma de seguridad?

3 ¿Cómo elijo la plataforma adecuada?

4 ¿Cómo elijo el proveedor adecuado?

5 ¿Cómo puedo sacar el mayor provecho a la plataforma que elija?

6 Validar mi elección

## Comprender su posición de seguridad

Antes de embarcarse en este viaje y realizar cambios en su programa de seguridad, primero debe comprender si necesita hacerlo y por qué.

Disponer de visibilidad de su superficie de ataque es clave para comprender su posición de seguridad. Hay muchas soluciones técnicas que pueden contribuir a ello. Es probable que tenga una solución de administración de parches y una base de datos de gestión de configuraciones. Sin embargo, las herramientas de nivel empresarial, como las plataformas de administración de la exposición a las amenazas digitales (CTEM), probablemente no estén a su alcance debido a las limitaciones presupuestarias. De hecho, aunque lo estuvieran, aumentarían la complejidad de su programa de seguridad y conllevarían una carga notable sobre su reducido equipo de informática y seguridad.

### Definiciones de términos importantes

**Posición de seguridad** es su situación general de preparación en materia de seguridad de la información, incluida la visibilidad del estado de todo el hardware, software y servicios e información.

**Superficie de ataque** es la suma de todo lo que un atacante podría aprovechar para lograr sus objetivos.

## Simplificar los marcos de seguridad puede ayudar

Hay muchas organizaciones que publican marcos de seguridad y directrices para ayudarle a conocer su estado actual y sus principales brechas. Entre ellas se cuenta la Organización Internacional de Normalización (ISO), la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos. Algunas de ellas crean marcos simplificados para organizaciones pequeñas y medianas.

## Acción prioritaria: Comprender sus tecnologías de seguridad actuales

Independientemente de si se ajusta a un marco o no, su primera tarea, antes de plantearse cambiar o añadir tecnologías de seguridad, es comprender lo que ya tiene implementado para proteger sus principales recursos y puntos de acceso iniciales que un atacante podría explotar.

Estudie la cobertura de seguridad en los siguientes aspectos:

- ↳ **Endpoints:** administrados y sin administrar
- ↳ **Identidades:** ya correspondan a personas o no
- ↳ **Nube:** infraestructura y SaaS
- ↳ **Correo electrónico:** puerta de enlace y plataforma
- ↳ **Red:** perímetro e interior

Buena cobertura	Brechas en la cobertura
Si está cubierto en todos los aspectos, se halla en una buena posición. Ahora, debe determinar hasta qué punto son eficaces estos controles y, en caso de que se trate de soluciones puntuales, si le convendría consolidarlas en una plataforma de seguridad.	Si tiene brechas, debe priorizar su protección en función del riesgo que representan. Plantéese la probabilidad de que resulten comprometidas y el impacto que ello tendría. Luego, debe decidir si implementar soluciones de seguridad puntuales o si una plataforma satisface sus necesidades.

1 ¿En qué estado se halla mi programa de seguridad?

2 ¿Me conviene tener una plataforma de seguridad?

3 ¿Cómo elijo la plataforma adecuada?

4 ¿Cómo elijo el proveedor adecuado?

5 ¿Cómo puedo sacar el mayor provecho a la plataforma que elija?

6 Validar mi elección

## Confirmar que una plataforma de seguridad es lo que más le conviene

Consolidar las herramientas de seguridad en una plataforma no es nuevo. En 2023, eSecurity Planet informó que una encuesta de Gartner revelaba que el 75 % de los compradores de seguridad buscaban la consolidación de proveedores, lo que impulsaba a estos a fusionar productos específicos en plataformas<sup>2</sup>. El motivo de esta consolidación era, principalmente, la reducción de la complejidad, más que de los costes directos.

Si disminuye el número de herramientas de seguridad puntuales, reduce su superficie de ataque y, a menudo, como las plataformas suelen ofrecer una estrecha integración y correlación de alertas, puede abreviar también el tiempo necesario para responder a un ataque y contenerlo.

Sin embargo, es objeto de debate si la adopción de plataformas se ha convertido en una realidad generalizada, especialmente en grandes organizaciones con amplios presupuestos y equipos de seguridad.

Para una mediana empresa con un equipo de informática y seguridad reducido, disminuir la complejidad es crucial, pero debe evitar hacerlo en detrimento de su posición de seguridad. Contando con la visibilidad de su estado actual y comprendiendo el estado que desea, debe sopesar los pros y los contras de las soluciones puntuales frente a la filosofía de una plataforma de seguridad.

Bitdefender®  
GravityZone

GUÍA DE SOLUCIONES

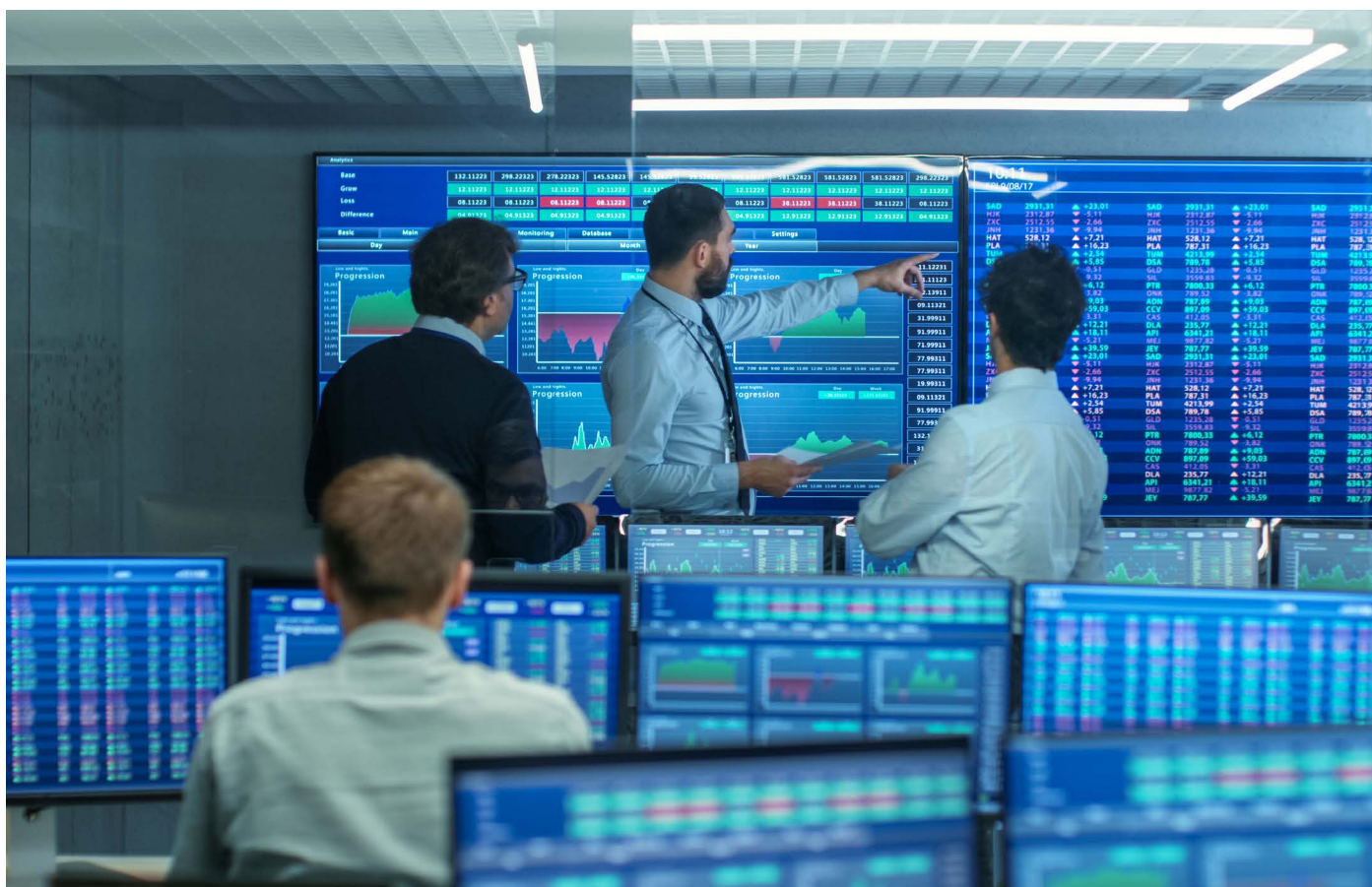
Cómo crear un programa de seguridad sólido con un equipo reducido

Descarga: [Guía de soluciones de Bitdefender: Cómo crear un programa de seguridad sólido con un equipo reducido.](#)

### Ventajas de la plataforma de seguridad

Reducción de la fragmentación.	Unificar la prevención, protección, detección y respuesta reduce el riesgo en todo el ciclo de vida de los ataques informáticos y en todos sus recursos, ya sean digitales o no.
Menor complejidad.	Tener menos herramientas reduce la superficie de ataque, la probabilidad de una configuración errónea y posibles vulnerabilidades.
Mayor eficiencia y productividad.	Una única interfaz de usuario simplifica la administración y las operaciones, reduce la fatiga de la consola y permite realizar tareas de forma fácil y rápida.
Respuesta mejorada ante los incidentes.	La estrecha integración entre las diversas herramientas aumenta la visibilidad de las amenazas y la correlación de alertas, lo que reduce los falsos positivos y el tiempo necesario para responder a un ataque y contenerlo.
Conformidad simplificada.	La coherencia de los informes procedentes de una única fuente reduce la carga que conllevan las auditorías.
Reduce el coste total de propiedad.	Reduce los costes de adquisición, mantenimiento periódico, soporte técnico y formación para lograr eficiencias operativas.

Inconvenientes de la plataforma de seguridad	
Único punto de error potencial.	Depender de un único proveedor concentra el riesgo. El proveedor podría sufrir problemas o un evento empresarial que conlleve un cambio en el nivel de su servicio.
Bloqueo del proveedor y dependencia.	Si la plataforma no satisface sus necesidades futuras, podría resultar difícil pasarse a otro proveedor.
Brechas de funcionalidad.	No hay ninguna plataforma capaz de satisfacer todas sus necesidades de seguridad y puede que una funcionalidad concreta no se ajuste tan bien a sus necesidades como un producto puntual equivalente.
Implementación inicial y migración.	La migración a una nueva plataforma puede implicar un alto coste de implementación y requerir tiempo antes de que obtenga valor.



1 ¿En qué estado se halla mi programa de seguridad?

2 ¿Me conviene tener una plataforma de seguridad?

3 ¿Cómo elijo la plataforma adecuada?

4 ¿Cómo elijo el proveedor adecuado?

5 ¿Cómo puedo sacar el mayor provecho a la plataforma que elija?

6 Validar mi elección

## Determinar qué enfoque de plataforma se adapta mejor a sus necesidades

En el mercado hay muchas plataformas de seguridad para elegir. A continuación se indican algunas preguntas clave que debe plantearse.

¿Se ha creado la plataforma para los SOC de grandes empresas?	Es probable que se construyan alrededor de plataformas SIEM y/o SOAR y, a menudo, NDR. Ofrecen una excelente funcionalidad para organizaciones con entornos complejos. Sin embargo, necesitará un equipo de profesionales de seguridad y gestión de riesgos para aprovecharlas al máximo.
¿Añade la plataforma una complejidad innecesaria?	La funcionalidad que no necesita o no utiliza añade complejidad y aumenta su superficie de ataque. Podría estar aumentando, no reduciendo, el riesgo.
¿Es costosa la plataforma debido a sus muchas funcionalidades?	Comprenda sus necesidades prioritarias. Los proveedores añaden continuamente nuevas funcionalidades para demostrar que aportan valor. No pague por funcionalidades que no va a utilizar.
¿Tiene la plataforma un sistema de licencias flexible?	Probablemente no querrá hacerlo todo desde el primer día y obtener licencias para todo lo que le ofrece una plataforma, pero necesita garantías de que podrá añadir funcionalidades integradas a medida que vaya madurando su programa de seguridad.
¿Está la plataforma notablemente automatizada (basada en IA)?	Los equipos de informática y seguridad reducidos necesitan toda la orientación y ayuda que puedan obtener. La automatización es clave, no solo para una respuesta rápida, sino también para guiar a través de la investigación y recuperación de incidentes.
¿Le ofrece la plataforma cobertura para sus recursos prioritarios?	La plataforma debe proteger endpoints, redes, nube, identidades y correo electrónico.
¿Ofrece MDR el proveedor?	Los complementos de servicios de MDR son esenciales para garantizar que, cuando necesite ampliar su equipo, cuente con personal de SecOps experto en la plataforma.

## Elegir una plataforma basada en EDR

Para una mediana empresa, con un equipo de informática y seguridad reducido, una plataforma de seguridad XDR basada en EDR brinda el mejor equilibrio entre seguridad y complejidad. Otras plataformas que podría plantearse son las que han evolucionado a partir de NDR y herramientas de SOC generales, como SIEM y SOAR. A continuación, se describen las fortalezas y debilidades relativas de alto nivel de cada una.

	XDR basada en EDR	XDR basada en NDR	SIEM y SOAR
Implementación	<p>Se implementa fácilmente como parte de su seguridad de endpoints.</p> <p>La mayoría ofrece la opción de elegir entre consola en la nube u on-premise.</p>	<p>Se instala un hardware o appliance virtual en la red, conectado en línea o mediante un puerto SPAN.</p> <p>La mayoría ofrece la opción de elegir entre consola en la nube u on-premise.</p>	<p>La mayoría ofrece la opción de elegir entre consola en la nube u on-premise.</p>
Integración y cobertura	<p>Los agentes, conectores y API proporcionan señales adicionales a través de redes, identidades, nube y correo electrónico.</p> <p>Fuerte cobertura en todo el ecosistema del proveedor y señales de alta prioridad que aportan un gran valor. Por ejemplo, identidades.</p> <p>La ingesta de datos de herramientas de terceros depende del proveedor.</p>	<p>Como EDR, más sondas adicionales para segmentos de red.</p>	<p>Integración compleja para incorporar datos de registro en un SIEM desde todos los recursos y puntos de aplicación de la seguridad, incluidos endpoints, red, identidades, nube y correo electrónico.</p> <p>La cantidad de playbooks de SOAR que deben crearse depende de la complejidad de su entorno.</p>
Tiempo para rentabilizar	<p>Rápida implementación inicial de endpoints y un breve período de aprendizaje pasivo para establecer una referencia de comportamientos.</p>	<p>Depende de la arquitectura de la red y del número de sondas necesarias.</p> <p>Como EDR, requerirá un período de aprendizaje.</p>	<p>Dependiendo de la complejidad del entorno, la cantidad de registros que se ingieren de los recursos que se monitorizan, el ajuste requerido y la cantidad de playbooks.</p>
Visibilidad de los ataques	<p>Buena visibilidad de los ataques en el endpoint. La mayoría de los atacantes intentarán comprometer un endpoint para acceder a información confidencial.</p> <p>Se detecta movimiento lateral cuando un atacante intenta comprometer un endpoint.</p> <p>Los agentes de red detectan los intentos de comprometer dispositivos sin administrar y el movimiento lateral hacia o desde ellos.</p> <p>La visibilidad en otros recursos depende de los agentes, conectores y API en uso.</p>	<p>Buena visibilidad de los ataques a endpoints sin administrar, como el sabotaje a la tecnología operativa.</p> <p>Buena visibilidad de los intentos de movimiento lateral desde dispositivos sin administrar comprometidos, antes de que el ataque llegue a un dispositivo administrado.</p> <p>La visibilidad en otros recursos depende de los agentes, conectores y API en uso.</p>	<p>Depende de la profundidad de las fuentes de datos de las herramientas y los recursos de su entorno.</p> <p>Cuando se configuran bien, los SIEM proporcionan correlación de alertas y conocimientos profundos de todo el entorno que otorgan con prontitud una buena visibilidad del acceso inicial, el movimiento lateral y los recursos comprometidos.</p>
Protección	<p>Los mejores productos de EDR incluyen protección de endpoints para bloquear los ataques antes de su ejecución.</p> <p>Se basa en otras medidas de seguridad para bloquear los ataques por correo electrónico, web, etc.</p>	<p>La NDR puede interrumpir ataques, dependiendo de la implementación.</p> <p>Se basa en EPP de terceros y otras medidas de seguridad para bloquear ataques en los endpoints y a través del correo electrónico, la web, etc.</p>	<p>Se basa en EPP de terceros y otras medidas de seguridad para bloquear ataques en los endpoints y a través del correo electrónico, la web, etc.</p>

	XDR basada en EDR	XDR basada en NDR	SIEM y SOAR
Detección	La detección primaria se realiza en el endpoint mediante profundas funciones de EDR listas para usar, incluido el análisis del comportamiento con IA. Esto se complementa con la correlación de señales de otros agentes, conectores y API.	La detección primaria se realiza en la red mediante inspección profunda de paquetes y análisis del comportamiento con IA. Esto se complementa con la correlación de señales de otros agentes, conectores y API.	Las reglas de correlación potentes y altamente personalizables requieren configuración manual, ajuste y mantenimiento continuo.
Fidelidad de la eficacia de detección	Excelente eficacia y pocos falsos positivos, especialmente cuando se utilizan señales adicionales para aportar más contexto.	A menudo, hay muchos falsos positivos y alertas.  Requiere un ajuste notable para garantizar la fidelidad de las alertas.	Depende de los datos ingeridos.  Requiere un ajuste notable para garantizar la fidelidad de las alertas.
Respuesta	Contención de ataques automatizada y guiada con mínimas molestias para los usuarios a través de acciones sencillas, que van desde el aislamiento del endpoint hasta el cierre de un proceso.	Las perturbaciones dependen de la implementación.  Opciones mínimas para la respuesta del endpoint; dependen del agente y de cualquier integración con EPP.	La SOAR proporciona una sólida orquestación/automatización, pero requiere la creación de un playbook y la integración con SIEM y otras herramientas externas.
Facilidad de uso	Varía notablemente dependiendo del proveedor.  Debe incluir paneles de control, flujos de trabajo y orientación, así como herramientas de consulta para una investigación más profunda de los incidentes cuando sea necesario.	Similar a EDR. Además, los productos NDR son notoriamente ruidosos y requerirán experiencia para el análisis y la respuesta a incidentes.	SIEM y SOAR requieren de experiencia para construir y mantener integraciones con los recursos y los puntos de aplicación de seguridad en todo su entorno.  SIEM requiere conocimientos de consultas.  SOAR requiere la elaboración de un playbook para automatizar la respuesta.
Coste total de propiedad	Los productos de protección de endpoints líderes del mercado incluyen EDR.  Algunos costes adicionales para conectores, agentes y conexión API.  La mayoría ofrece consolas basadas en la nube para eliminar la necesidad de una infraestructura costosa.  Requiere poco esfuerzo de administración y muchos incluyen informes fácilmente comprensibles y capacidad para una respuesta rápida ante los incidentes sin necesidad de un costoso personal de SecOps.	El hardware o los dispositivos virtuales deben instalarse y mantenerse on-premise.  La mayoría ofrece consolas basadas en la nube para eliminar la necesidad de una infraestructura e implementación costosas.  Los NDR requieren un costoso personal de SecOps para el análisis y la respuesta a incidentes.	Requiere infraestructura, almacenamiento, ajuste, personal especializado de SecOps y mantenimiento continuo.  La integración profunda con un entorno complejo existente le ayudará a obtener un retorno de la inversión en las herramientas de seguridad actuales.

1 ¿En qué estado se halla mi programa de seguridad?

2 ¿Me conviene tener una plataforma de seguridad?

3 ¿Cómo elijo la plataforma adecuada?

4 ¿Cómo elijo el proveedor adecuado?

5 ¿Cómo puedo sacar el mayor provecho a la plataforma que elija?

6 Validar mi elección

## Obtener el máximo valor mediante funcionalidades clave que marcan la diferencia

La información anterior confirma que, para una mediana empresa con un equipo de informática y seguridad reducido, la mejor opción es una plataforma de seguridad basada en EDR. Ahora, elabore su lista de proveedores seleccionados teniendo en cuenta no solo la mejor detección y respuesta, sino también el importante valor añadido que aportan las mejores plataformas de XDR que van más allá de un simple producto de XDR.

La fidelidad de la detección se demuestra en pruebas llevadas a cabo por instituciones independientes

**MITRE | ATT&CK®**

### Validar la eficacia y fidelidad de la detección de la plataforma

La tabla anterior sugiere que algunas plataformas de NDR son ruidosas. Esto también sucede con la EDR, por lo que una de sus consideraciones clave debe ser no solo lo eficaz que es a la hora de detectar una amenaza, sino también su eficacia para reconocer comportamientos anómalos que no constituyen una amenaza. Si su reducido equipo de informática y seguridad se ve sobrecargado con cientos de alertas que correlacionar y priorizar manualmente, es muy probable que un incidente se convierta en una violación de la seguridad antes de que puedan contenerlo.

Plantéese plataformas que hayan demostrado ofrecer una detección de alta fidelidad, es decir, que sean muy precisas y tengan una baja tasa de falsos positivos.

### Hay que proteger cada punto del ciclo de vida del ataque

Algunos proveedores de XDR se basan por completo en la premisa de que los incidentes son inevitables y usted debe centrarse principalmente en la detección y la respuesta. Sin embargo, esto es de poca ayuda para una organización con un equipo de informática y seguridad reducido y sin un SOC. Su objetivo consiste en evitar que la mayor cantidad posible de amenazas se conviertan en un incidente y trasladen la responsabilidad de la respuesta a su equipo.

La eficacia se demuestra en pruebas llevadas a cabo por instituciones independientes



### Bloquear tantas amenazas como sea posible antes de que lleguen a ejecutarse

Lo primero y más fácil es obtener la mejor protección posible: bloquear tantas amenazas como sea posible antes de que lleguen a ejecutarse. Plantéese un proveedor que tenga un rendimiento sistemáticamente bueno en evaluaciones llevadas a cabo por instituciones independientes.

## Hay que centrarse primero en la prevención

Las tecnologías de prevención que le ayudan a comprender y administrar su superficie de ataque, su posición de seguridad y sus vulnerabilidades estuvieron en su momento fuera del alcance de las medianas empresas. Hoy en día, ciertos proveedores de XDR se diferencian por integrar algunas de estas capacidades críticas en su plataforma. Los centrados en las empresas esperan que sus clientes ya tengan estas soluciones puntuales, por lo que debe plantearse plataformas de XDR que estén optimizadas para medianas empresas.

### Estos aportan a su programa de seguridad importantes beneficios tangibles y demostrables:

- ↳ Reducción proactiva del riesgo de que un ataque triunfe.
- ↳ Cuantificación de los resultados de sus actividades actuales de reducción de riesgos.
- ↳ Fácil demostración a los directivos de los cambios en la posición de seguridad.
- ↳ Reducción de las probabilidades de que se produzca un incidente y del esfuerzo de respuesta resultante por parte del personal de TI y seguridad.
- ↳ Reducción demostrable del coste y el esfuerzo necesarios para lograr y mantener el cumplimiento normativo.
- ↳ Reducción del coste y el esfuerzo que supone adquirir un seguro informático.

Considere una plataforma que no solo agrupe, sino que integre cumplimiento normativo, superficie de ataque, vulnerabilidad y administración de parches, junto con análisis de riesgos y reducción de la superficie de ataque, con herramientas como el endurecimiento de endpoints.

La integración es clave para maximizar el valor de estas herramientas. Tenga cuidado con los proveedores que han adquirido tecnologías y simplemente han rediseñado la interfaz de usuario.

## Asegúrese de que la funcionalidad diferenciadora no introduzca una complejidad innecesaria

Su objetivo durante todo este proceso es garantizar que la solución elegida simplifique sus operaciones de seguridad y reduzca el riesgo. Durante la evaluación de sus proveedores seleccionados, debe tener esto en cuenta y recordar que una funcionalidad adicional podría restarle valor al objetivo. No obstante, tenga en cuenta también que el valor añadido no significa necesariamente complejidad y que debe conseguir un equilibrio entre ambos aspectos. Para ello, plantéese plataformas que optimicen cualquier funcionalidad adicional para organizaciones como la suya.

1 ¿En qué estado se halla mi programa de seguridad?

2 ¿Me conviene tener una plataforma de seguridad?

3 ¿Cómo elijo la plataforma adecuada?

4 ¿Cómo elijo el proveedor adecuado?

5 ¿Cómo puedo sacar el mayor provecho a la plataforma que elija?

6 Validar mi elección

## Asegúrese de que el proveedor elegido pueda reforzar y apoyar su programa de seguridad y a su equipo

La MDR es un complemento importante para reforzar los equipos de informática y seguridad ajustados y reducir el riesgo mediante el fortalecimiento de todo su programa de seguridad. Su primera decisión consiste en determinar si necesita MDR o no. Considere las siguientes ventajas:

- ↳ Maximizar el retorno de su inversión en la plataforma de XDR aprovechando la experiencia disponible en el SOC del proveedor elegido.
- ↳ Superar las limitaciones de personal y eliminar los desafíos que conlleva la contratación y retención del personal.
- ↳ Proporcionar a su equipo de informática y seguridad el apoyo que necesita y centrar sus esfuerzos en actividades que brinden el mayor retorno de la inversión.
- ↳ Reducir de forma demostrable el coste y el esfuerzo necesarios para lograr y mantener el cumplimiento normativo, así como adquirir un seguro informático.

## Considere las ofertas de servicio que marquen la diferencia

Valore a los proveedores de plataformas de XDR que le ofrezcan la flexibilidad de añadir MDR posteriormente. Tenga cuidado: no todos los complementos de servicios son iguales, así que, aunque no vaya a usar la MDR de inmediato, debería evaluar la que le ofrece el proveedor de XDR que elija. Los servicios diferenciadores que debe buscar son los siguientes:

- ↳ Recomendaciones de expertos para ayudarle a mejorar sus controles de seguridad preventiva y reducir su superficie de ataque.
- ↳ Acceso directo a un equipo de expertos en inteligencia sobre amenazas digitales para realizar investigaciones especializadas y personalizadas.
- ↳ Búsqueda proactiva, con regularidad, de amenazas emergentes en su entorno y atacantes que hayan eludido sus defensas y estén profundizando silenciosamente en su ataque.
- ↳ No actúa solo como un agregador de alertas, sino que responde en su nombre con acciones previamente aprobadas para contener rápidamente un ataque con una mínima perturbación del negocio.
- ↳ Análisis de la causa raíz del incidente para permitir una rápida recuperación y el retorno a la normalidad.

1 ¿En qué estado se halla mi programa de seguridad?

2 ¿Me conviene tener una plataforma de seguridad?

3 ¿Cómo elijo la plataforma adecuada?

4 ¿Cómo elijo el proveedor adecuado?

5 ¿Cómo puedo sacar el mayor provecho a la plataforma que elija?

6 Validar mi elección

## Elija una plataforma de seguridad optimizada para equipos de informática y seguridad reducidos

Incluso las empresas con grandes equipos de profesionales de la seguridad exigen consolidación para deshacerse de la complejidad. El resultado es que los proveedores centrados en las empresas están comercializando lo que a menudo son un conjunto de productos puntuales poco integrados, repletos de funcionalidades que las medianas empresas no pueden aprovechar por falta de tiempo, personal y competencias.

### Hay plataformas disponibles que son más adecuadas para la mediana empresa, pero elija sabiamente y tenga en cuenta lo siguiente:

- ↳ ¿Proporciona seguridad durante todo el ciclo de vida de las amenazas: prevención, protección, detección y respuesta?
- ↳ ¿Simplifica las operaciones de seguridad para respaldar su estrategia de consolidación y reducir el riesgo operativo?
- ↳ ¿Ofrece la flexibilidad para ayudarlo a migrar hoy pero añadiendo funcionalidades a medida que su programa de seguridad madura para respaldar las necesidades de su negocio?
- ↳ ¿El proveedor de la plataforma proporciona los servicios de soporte necesarios para ayudar a su equipo reducido a madurar con su programa de seguridad?

### Valide su elección apoyándose en reseñas de terceros

Esta es su última tarea.

Céntrese en las referencias y reseñas de organizaciones como la suya. Los comentarios positivos de grandes empresas con entornos y programas de seguridad completamente diferentes no importan tanto como las de organizaciones similares a la suya. [Gartner Peer Insights](#) es una buena fuente de reseñas independientes y otorga [premios Customers' Choice](#) a los proveedores que destacan en las categorías que cubren.

Considere también los informes de analistas del sector, como las guías de mercado y los Magic Quadrant de Gartner. Actúe con cautela al evaluar las clasificaciones, ya que suelen basarse en funcionalidades de nivel corporativo y no en las orientadas a la mediana empresa. No obstante, su mera inclusión sí resalta que el proveedor elegido es relevante, puesto que los analistas lo tienen en cuenta.

# Preguntas que hacer a los proveedores de plataformas de seguridad

<p><b>General</b></p>	<ul style="list-style-type: none"> <li>↳ ¿Me ayuda a reducir el riesgo a lo largo de todo el ciclo de vida del ataque con herramientas críticas de prevención, protección, detección y respuesta?</li> <li>↳ ¿Protege todos mis recursos: endpoints, identidades, nube, red y correo electrónico?</li> <li>↳ ¿Podrá implementarla y administrarla mi equipo con facilidad?</li> <li>↳ ¿Cómo reduce mi coste total de propiedad?</li> <li>↳ ¿Hasta qué punto es flexible el modelo de licencias?</li> </ul>
<p><b>Prevención</b></p>	<ul style="list-style-type: none"> <li>↳ ¿Informa y demuestra cómo estoy reduciendo el riesgo y logrando el cumplimiento normativo que requerimos?</li> <li>↳ ¿Me ayuda a identificar incumplimientos normativos y me brinda información útil para cerrar las brechas?</li> <li>↳ ¿Incluye las capacidades de prevención críticas de las siguientes herramientas?:             <ul style="list-style-type: none"> <li>↳ Administración de la superficie de ataque de recursos informáticos (CAASM)</li> <li>↳ Administración continua de la exposición a las amenazas (CTEM)</li> <li>↳ Cloud Security Posture Management (CSPM)</li> <li>↳ Administración de la superficie de ataque externa (EASM)</li> </ul> </li> <li>↳ ¿Proporciona información práctica, recomendaciones y acciones correctivas guiadas que se priorizan según la gravedad y el impacto potencial?</li> <li>↳ ¿Qué capacidades de reducción de la superficie de ataque incluye? Por ejemplo, administración de parches y endurecimiento de endpoints.</li> </ul>
<p><b>Protección</b></p>	<ul style="list-style-type: none"> <li>↳ ¿Cómo se desenvuelve en pruebas técnicas realizadas por instituciones independientes para medir su eficacia y precisión?</li> <li>↳ ¿Qué credenciales poseen los investigadores de amenazas del proveedor?</li> <li>↳ ¿Qué recursos cubre la protección?</li> </ul>

<p><b>Detección y respuesta</b></p>	<ul style="list-style-type: none"> <li>↳ ¿Desde qué recursos de mi infraestructura se ingieren las alertas?</li> <li>↳ ¿Me proporciona visibilidad de los recursos de mi organización que podrían ser objetivo de un atacante?</li> <li>↳ ¿Qué automatización incluye para ayudar a correlacionar y clasificar las alertas?</li> <li>↳ ¿Cómo se desenvuelve en pruebas realizadas por instituciones independientes para medir la eficacia, precisión y volumen de las alertas?</li> <li>↳ ¿Qué medidas puedo adoptar para responder a un incidente y minimizar la perturbación del negocio?</li> <li>↳ ¿Qué herramientas de análisis de causa raíz proporciona?</li> <li>↳ ¿Incluye informes fácilmente comprensibles y capacidades de consulta avanzada?</li> </ul>
<p><b>MDR</b></p>	<ul style="list-style-type: none"> <li>↳ ¿Qué nivel de detalle tienen las recomendaciones del proveedor para ayudarle a mejorar su posición de seguridad?</li> <li>↳ ¿Cuento con acceso directo a los investigadores de amenazas del proveedor?</li> <li>↳ ¿Con qué frecuencia realiza el proveedor búsquedas de amenazas en mi entorno?</li> <li>↳ ¿Responde el proveedor en mi nombre y con qué nivel de detalle ejecuta las acciones para garantizar una mínima perturbación del negocio?</li> <li>↳ ¿Realiza el proveedor análisis de causa raíz?</li> <li>↳ ¿Ofrece el proveedor una garantía de seguridad informática?</li> </ul>

Notas finales

- 1 [Verizon 2025 Data Breach Investigations Report](#)
- 2 [Security Buyers Are Consolidating Vendors: Gartner Security Summit](#)

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 Orhideeor 15A,  
Distrito 6,  
Bucarest 060071

T: +40 21 4412452

**Oficina en España**

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