The Forrester Wave™: Endpoint Security As A Service, segundo trimestre de 2021

Los 12 proveedores más importantes y su posición en el sector

por Chris Sherman
13 de mayo de 2021

Por qué debería leer este informe

En nuestra evaluación de 24 criterios de los proveedores de seguridad *endpoint* mediante SaaS, destacamos a los 12 más importantes: Bitdefender, BlackBerry, Cisco, CrowdStrike, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Symantec, Trend Micro y VMware. También los hemos investigado, analizado y puntuado. Este informe muestra las características de cada proveedor y ayuda a los profesionales del ámbito de la seguridad y el riesgo a escoger el que más se ajuste a sus necesidades.

The Forrester Wave™: Endpoint Security As A Service, segundo trimestre de 2021

Los 12 proveedores más importantes y su posición en el sector

por Chris Sherman
con Merritt Maxim, Allie Mellen, Shannon Fish y Peggy Dostie
13 de mayo de 2021

Los compradores de servicios de seguridad y riesgo exigen una solución de seguridad *endpoint* completa mediante SaaS

A medida que la pandemia de COVID-19 presionaba a los equipos de seguridad para migrar los productos de seguridad de los dispositivos locales a los gestionados en la nube, Forrester observó un aumento significativo en el interés de los clientes por los productos de seguridad *endpoint* mediante SaaS. A esto favoreció el hecho de que muchos proveedores de *endpoint* tuvieran casi la misma paridad de funciones en su paquete de seguridad *endpoint* en dispositivos locales y en la versión de *software* como servicio (SaaS, acrónimo de *Software-as-a-Service*), lo que facilitó la decisión de migrar a la versión SaaS. En la actualidad, la mayoría de los proveedores de paquetes de seguridad *endpoint* ofrecen las principales funciones de seguridad gestionadas a través de consolas en la nube. Se han desarrollado meticulosamente y se han incorporado nuevas funciones de productos principalmente para las versiones de SaaS.

Se ha aumentado la seguridad *endpoint* ahora que los riesgos cibernéticos ocurren con más frecuencia en *endpoint* y no en la red. Esto se debe a que cada vez más empleados trabajan desde casa y también a que los datos se están trasladando en masa hacia dispositivos perimetrales, en lugar de permanecer en centros de datos conectados a redes empresariales. Por este motivo, los clientes que exigen seguridad *endpoint* mediante SaaS deben buscar proveedores que:

- **Estén al tanto de las novedades:** Los proveedores deben innovar y adaptarse a las exigencias de los *endpoints* modernos a medida que surgen nuevos riesgos y tendencias empresariales. Al escoger una solución, los compradores exigen pruebas que corroboren el liderazgo corporativo, el desarrollo continuo con la incorporación de nuevas funciones relevantes y actualizadas y un dilatado historial en materia de innovación.

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140, EE. UU.
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

- **Sean eficaces:** Las herramientas de seguridad *endpoint* deben combinar de forma armónica la prevención eficaz de amenazas y la detección automática y oportuna de las mismas. Estas herramientas deben validarse regularmente mediante pruebas de laboratorio como MITRE ATT&CK y AV-Comparatives Endpoint Prevention and Response Test, que combinan evaluaciones del rendimiento de la prevención y detección de amenazas. Los compradores también deben buscar plataformas SaaS que estén consolidadas y cuenten con cobertura global, además de estar basadas en arquitecturas de agentes que permitan comunicaciones de red rápidas y eficaces para reducir al mínimo el impacto en la experiencia del usuario final cuando las medidas de protección estén activas.
- **Diseñado para integrarse:** La seguridad *endpoint* no puede funcionar en un entorno vacío, teniendo en cuenta la gran diversidad de la mayoría de los ataques. Los proveedores actuales de seguridad *endpoint* lo saben y ofrecen sistemas integrados con otras capas (ya estén relacionadas o no con la seguridad) más allá de los *endpoints* (por ejemplo, gestión de servicios de TI, seguridad en la nube, seguridad de la red y gestión de acceso e identificación). Los compradores deben buscar proveedores de seguridad *endpoint* que admitan funciones e integraciones de detección y respuesta ampliadas (XDR, por sus siglas en inglés), junto con políticas y reglas compatibles con el enfoque Zero Trust.

Resumen de la evaluación

La evaluación Forrester Wave™ distingue líderes, proveedores fuertes, aspirantes y desafiadores. Se trata de una evaluación de los principales proveedores y no representa el panorama completo del mercado.

Pretendemos que esta evaluación sea solo un punto de partida. Animamos a los clientes a consultar las evaluaciones de los productos y a adaptar las ponderaciones de los criterios mediante la herramienta de comparación de proveedores basada en Excel (consulte la figura 1 y la figura 2). Haga clic en el enlace al comienzo de este informe en Forrester.com para descargar la herramienta.

FIGURA 1 Forrester Wave™: Endpoint Security Software As A Service, segundo trimestre de 2021

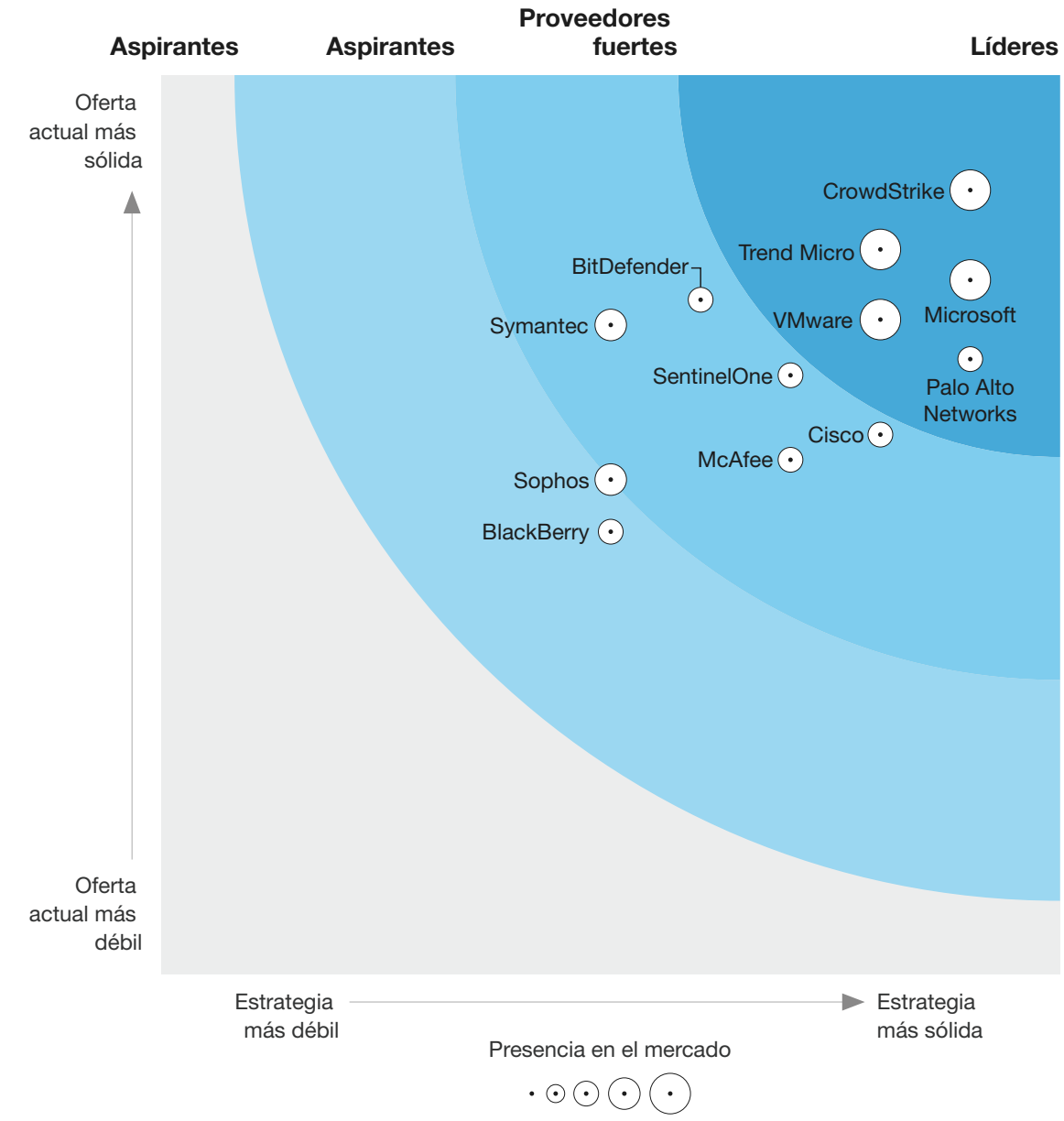

FIGURA 2 Forrester Wave™: Endpoint Security Software As A Service, segundo trimestre de 2021, tabla de puntuación

	Ponderación de Forrester	BitDefender	BlackBerry	Cisco	CrowdStrike	McAfee	Microsoft	Palo Alto Networks	SentinelOne
Oferta actual	50 %	3,75	2,46	3,00	4,36	2,86	3,86	3,42	3,33
Prevención de amenazas	20 %	4,20	3,00	3,40	4,60	3,40	3,80	4,20	3,00
Detección de amenazas	20 %	2,50	1,75	3,50	4,50	2,00	4,00	5,00	4,50
Control	20 %	3,67	1,67	2,33	4,33	3,67	5,00	3,00	3,00
Seguridad de datos	5 %	3,00	1,00	0,00	1,00	3,00	5,00	1,00	1,00
Seguridad móvil	5 %	3,00	5,00	3,00	5,00	5,00	5,00	1,00	1,00
Compatibilidad con el sistema operativo	5 %	5,00	5,00	5,00	5,00	3,00	1,00	5,00	5,00
Rendimiento del producto	25 %	4,50	2,50	3,00	4,50	2,00	3,00	2,50	3,50
Estrategia	50 %	3,00	2,50	4,00	4,50	3,50	4,50	4,50	3,50
Hoja de ruta del producto	25 %	3,00	5,00	3,00	5,00	3,00	3,00	3,00	5,00
Estrategia corporativa	25 %	5,00	1,00	3,00	5,00	3,00	5,00	5,00	5,00
Compatibilidad con el marco de trabajo Zero Trust	25 %	1,00	3,00	5,00	3,00	5,00	5,00	5,00	3,00
Participación de la comunidad en materia de seguridad	25 %	3,00	1,00	5,00	5,00	3,00	5,00	5,00	1,00
Presencia en el mercado	0 %	3,00	2,33	3,00	4,33	3,00	5,00	2,33	2,33
Ecosistema de socios	33 %	5,00	1,00	5,00	5,00	5,00	5,00	3,00	3,00
Base de clientes empresariales	33 %	1,00	3,00	1,00	3,00	1,00	5,00	3,00	1,00
Penetración empresarial	33 %	3,00	3,00	3,00	5,00	3,00	5,00	1,00	3,00

Todas las puntuaciones se basan en una escala de 0 (débil) a 5 (fuerte).

FIGURA 2 Forrester Wave™: Endpoint Security Software As A Service, segundo trimestre de 2021, tabla de puntuación (continuación)

	Ponderación de Forrester	Sophos	Symantec	Trend Micro	VMware
Oferta actual	50 %	2,75	3,61	4,03	3,64
Prevención de amenazas	20 %	3,00	5,00	5,00	3,40
Detección de amenazas	20 %	2,00	3,00	4,00	4,00
Control	20 %	3,00	3,67	3,00	3,67
Seguridad de datos	5 %	5,00	3,00	5,00	1,00
Seguridad móvil	5 %	5,00	5,00	5,00	5,00
Compatibilidad con el sistema operativo	5 %	3,00	5,00	5,00	5,00
Rendimiento del producto	25 %	2,00	2,50	3,50	3,50
Estrategia	50 %	2,50	2,50	4,00	4,00
Hoja de ruta del producto	25 %	1,00	3,00	5,00	3,00
Estrategia corporativa	25 %	3,00	1,00	3,00	5,00
Compatibilidad con el marco de trabajo Zero Trust	25 %	3,00	3,00	3,00	5,00
Participación de la comunidad en materia de seguridad	25 %	3,00	3,00	5,00	3,00
Presencia en el mercado	0 %	3,67	3,67	4,33	4,33
Ecosistema de socios	33 %	1,00	5,00	3,00	5,00
Base de clientes empresariales	33 %	5,00	3,00	5,00	5,00
Penetración empresarial	33 %	5,00	3,00	5,00	3,00

Todas las puntuaciones se basan en una escala de 0 (débil) a 5 (fuerte).

Ofertas de proveedores

Forrester incluyó a 12 proveedores en esta evaluación: BitDefender, BlackBerry, Cisco, CrowdStrike, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Symantec, Trend Micro y VMware (consulte la figura 3).

FIGURA 3 Proveedores evaluados e información del producto

Proveedor	Producto evaluado	Versión del producto evaluada
BitDefender	Bitdefender GravityZone Ultra Security	2021
BlackBerry	BlackBerry Cyber Suite, BlackBerry Spark Suite	N/D
Cisco	Cisco Secure Endpoint (CSE)	Consola v5.4
CrowdStrike	Falcon	N/D
McAfee	McAfee Endpoint Security	v10.7
Microsoft	Microsoft Defender for Endpoint (MDE)	N/D
Palo Alto Networks	Cortex XDR	v2.7
SentinelOne	Singularity Complete	Plataforma: lanzamiento de Machu Picchu
Sophos	Intercept X Advanced	v3
Symantec	Endpoint Security Complete	N/D
Trend Micro	Apex One	N/D
VMware	Carbon Black Cloud	N/D

Perfiles de proveedores

Nuestro análisis reveló las siguientes fortalezas y debilidades de los proveedores.

Líderes

- **CrowdStrike ofrece una mayor seguridad *endpoint* con una arquitectura de nube nativa.** CrowdStrike ha experimentado un rápido crecimiento desde que lanzó por primera vez la plataforma SaaS de seguridad *endpoint* en 2011 en EE. UU. Su cartera incluye servicios como la seguridad *endpoint*, la seguridad de nube pública, la seguridad de identidades, la protección de cargas de trabajo y herramientas de operaciones de TI. Los clientes ensalzan las características de detección y respuesta automáticas de CrowdStrike, así como su eficacia a nivel general, especialmente a medida que la empresa progresa con respecto a la estrategia XDR, al tiempo que extrae los datos de un ecosistema de sensores cada vez mayor. Además, Falcon Store es uno de los ecosistemas de aplicaciones de terceros más activos en este estudio y ofrece funciones adicionales, relacionadas o no con *endpoints*, lo que mejora las capacidades de CrowdStrike en áreas como DLP y seguridad ICS/IoT.

Aunque CrowdStrike ofrece una prevención y detección de amenazas total, los usuarios informan de que se necesitan conocimientos avanzados para utilizar el producto de forma eficaz. El agente Falcon tampoco cuenta con capacidades DLP y de seguridad de datos y, en su lugar, confía en socios de su ecosistema de aplicaciones para ofrecer funciones de seguridad de datos más completas. Además, las referencias de clientes y las evaluaciones realizadas por terceros de CrowdStrike para la prevención de *malware* fueron más mediocres que las de otros productos de este estudio, aunque, según las referencias, su grandísima capacidad de detección compensa este punto. CrowdStrike es la mejor opción para aquellos clientes que busquen una protección de gran eficacia con exhaustivas funciones de detección de amenazas.

- **Microsoft equilibra la seguridad** *endpoint* **y la experiencia del usuario.** Microsoft ofrece sus capacidades de seguridad *endpoint* en un producto independiente, Microsoft Defender for Endpoint (anteriormente Advanced Threat Protection), compatible con Android, iOS, Linux, macOS y Windows. Tanto las puntuaciones de los laboratorios externos como las referencias de clientes apuntan a una mejora continua con respecto a la prevención de *malware* y a su eficacia para evitar vulnerabilidades de seguridad, asignaturas en las que Microsoft suele obtener mejores puntuaciones que sus competidores. Asimismo, ejerce un impacto llamativamente bajo en el *endpoint* cuando se ejecuta de forma activa y el número de falsos positivos notificados por los clientes también es el más bajo de esta evaluación.

  El aspecto negativo es que sigue presentando ciertos problemas en cuanto a integración y flujo de trabajo. Los administradores se quejan de la cantidad de pantallas con las que tienen que trabajar y de la falta de integración entre las pantallas de prevención y detección de amenazas. Además, aunque Microsoft ofrece protección para *endpoints* que no pertenecen a Windows, la cobertura y la amplitud de las capacidades que se ofrecen son insuficientes en comparación con las ofertas de la competencia. Defender for Endpoint es una opción excelente para las organizaciones que dependen en gran medida de Windows, especialmente las que utilizan Office 365 o tienen una licencia E5.

- **Trend Micro ofrece una cartera bastante completa de productos de seguridad** *endpoint* **centrada en la detección.** Como uno de los proveedores de prevención de *malware* originales, Trend Micro, con sede en Japón, ofrece capacidades de prevención y detección de amenazas *endpoint*, configuración segura, respuesta a ataques y seguridad de datos dentro de una cartera más amplia de productos y servicios en materia de seguridad. Los compradores disfrutan de una paridad completa de características entre las versiones de los dispositivos locales y las gestionadas de Apex Central, lo que permite realizar transiciones más sencillas durante la fase "híbrida". Sus capacidades de detección, que se han ampliado, son sólidas y accesibles desde Trend Micro Vision One, una consola independiente diseñada para consumir datos telemétricos y de entorno, tanto de Trend Micro como de terceros, que abarcan fuentes de red, de carga de trabajo en la nube, de correo electrónico y *endpoint*.

  Los compradores se quejan de que, en ocasiones, la experiencia de administración puede resultar engorrosa. Es probable que la separación entre Trend Micro Vision One y Apex Central provoque ciertos problemas para los administradores hasta que se migren funciones adicionales a la nueva plataforma. Recientemente, algunos clientes también han informado de que tienen dificultades para eliminar versiones antiguas del agente. A pesar de todo, la satisfacción general del cliente sigue siendo alta. Forrester espera que Trend Micro siga ofreciendo un buen servicio a las grandes empresas, especialmente a aquellas con requisitos específicos de seguridad de puntos de conexión.

- **Palo Alto Networks (PAN) integra la prevención de amenazas *endpoint* con una detección mejorada.** Las ofertas de SaaS de Palo Alto Networks, con sede en EE. UU., dirigidas a la seguridad *endpoint* y la detección y respuesta mejoradas, pertenecen a la marca Cortex XDR. Durante los últimos dos años, PAN ha mejorado rápidamente sus capacidades de seguridad *endpoint* y su gama de productos de seguridad mediante la adquisición y el desarrollo de productos. La empresa sustituyó su antigua plataforma de seguridad de puntos de conexión en los dispositivos locales por Cortex XDR, que incluye mejoras en áreas como el análisis de la protección automática del comportamiento y las amenazas. Como primer proveedor en promover una estrategia XDR, PAN es el más completo de este estudio, ya que ofrece prevención de amenazas, detección y controles de acceso en aplicaciones *endpoint*, de IoT, de la red y de la nube. Las adquisiciones de herramientas de orquestación de seguridad, automatización y respuesta (Demisto) y agentes de seguridad de acceso a la nube ofrecen potentes secuencias de automatización y políticas de acceso entre productos nativos y de terceros a aquellos compradores que han invertido en varios productos de PAN.

  El aumento en la cartera de capacidades y consolas implica una mayor complejidad, ya que los compradores opinan que la implementación y el funcionamiento del producto conllevan un nivel de dificultad superior al de la media. Se han notificado problemas de rendimiento de los agentes cuando se implementan en *endpoints* con especificaciones de rendimiento inferiores a las que se consideran estándar. Cortex XDR tampoco ofrece todas las capacidades de un paquete convencional, como el control de las aplicaciones, la seguridad de los datos y la gestión completa de la seguridad nativa. Palo Alto Networks es una opción interesante para las empresas que desean adoptar una solución de seguridad de puntos de conexión renovada o una estrategia XDR con sólidas funciones de prevención de amenazas.

- **VMware tiene como objetivo reducir los problemas entre la seguridad de TI y las operaciones.** VMware, con sede en EE. UU., ofrece una cartera de servicios de seguridad, automatización del espacio de trabajo y tecnologías de virtualización que respaldan su objetivo de unificar la infraestructura, la seguridad y la gestión de TI de los entornos de sus clientes. Su principal oferta de seguridad *endpoint*, Carbon Black Cloud, ofrece prevención y detección de amenazas, refuerzo de dispositivos, configuración segura y búsqueda automática de ataques, todo ello como SaaS. Las integraciones de los controles de acceso, la gestión y la seguridad de dispositivos, la seguridad de la red y las aplicaciones facilitan la incorporación de políticas de seguridad detalladas basadas en riesgos para respaldar la estrategia Zero Trust.

  La capacidad de solucionar ataques por parte de VMware no está tan automatizada como la de otros participantes de este estudio. Los clientes de referencia se quejaron de la mediocridad de los flujos de trabajo de análisis al responder a los ataques (por ejemplo, la reversión de configuraciones y ciertas acciones de corrección requieren que los analistas pasen de una consola a otra). Aunque el ritmo de la innovación en seguridad *endpoint* ha mejorado tras la adquisición de VMware, el futuro de la estrategia sigue sin estar claro, dada la reciente salida del director ejecutivo y la inminente escisión de VMware de Dell. VMware es una opción excelente para aquellos compradores dispuestos a asumir este periodo de transición, especialmente los que ya son clientes de VMware o están interesados en sus servicios gestionados.

Proveedores fuertes

- **Cisco ha creado una cartera muy atractiva con capacidades de seguridad suministradas como SaaS.** Cisco Secure Endpoint se centra en la prevención de amenazas *endpoint*, la protección automática del comportamiento y la búsqueda de amenazas mediante la función de búsqueda avanzada orbital. La plataforma SecureX de Cisco incorpora y correlaciona telemetría de seguridad de dispositivos, cargas de trabajo y aplicaciones del cliente a través de productos de Cisco e integraciones de terceros (ya cuenta con 50 socios

y ha crecido significativamente en el último año). Si bien la empresa se ha centrado principalmente en las capacidades de seguridad de comportamiento y prevención de *malware*, su compromiso de crear controles de acceso a aplicaciones y redes detallados y basados en la posición de los dispositivos *endpoint*, así como en el riesgo de los usuarios, resulta atractivo para aquellos que desean adoptar una estrategia Zero Trust.

Cisco no ofrece capacidades habituales de paquetes auxiliares y su compatibilidad para funciones de gestión de parches, seguridad de datos y control de aplicaciones dispositivos son limitadas (aunque se prevé lanzar esta última en una versión futura). Además, las tareas más avanzadas de investigación de ataques y respuesta de Secure Endpoint pueden resultar engorrosas: los clientes se quejan de flujos de trabajo complicados con respecto a la gestión de políticas y la investigación de amenazas. Cisco Secure Endpoint es una muy buena opción para aquellas organizaciones que simplemente buscan un sistema de prevención de las amenazas principales y de protección del comportamiento que no presente muchos requisitos adicionales de seguridad *endpoint*.

- **SentinelOne se centra en ofrecer una protección amplia y automática con una carga administrativa baja.** SentinelOne se fundó en Tel Aviv en 2013, pero desde entonces ha trasladado su sede central a EE. UU., país en el que el interés de las empresas por sus productos ha aumentado rápidamente en los últimos tres años. Su principal plataforma de seguridad *endpoint*, SentinelOne Singularity, ofrece a los clientes capacidades para prevenir *malware*, evitar vulnerabilidades de seguridad y proteger el comportamiento en tiempo de ejecución, así como excelentes capacidades para solucionar problemas, incluido el restablecimiento completo de archivos y configuraciones. Su arquitectura SaaS es altamente escalable y fácil de gestionar y presenta una cobertura completa más allá del punto de conexión (por ejemplo, cargas de trabajo en la nube, red e IoT). Su función IoT Ranger es el único producto de esta evaluación que ofrece detección de dispositivos IoT y aplicación de políticas a través de su agente basado en puntos de conexión (utiliza una inspección exhaustiva de paquetes basada en *host*).

  SentinelOne carece de algunas de las características de un paquete auxiliar que siguen buscando las empresas más tradicionales, como la gestión de vulnerabilidades, el control de dispositivos/DLP, el cifrado y los cortafuegos de *host*. Los clientes de Forrester y los clientes de referencia se quejaron de la estabilidad de la dotación de personal durante las actualizaciones de los nuevos agentes. Sin embargo, la asistencia técnica fue, en general, más rápida y beneficiosa en comparación con otras que forman parte de este estudio. SentinelOne es una opción excelente para las grandes y pequeñas empresas que buscan simplificar sus flujos de trabajo de detección y la pila de seguridad *endpoint*, al tiempo que admite una estrategia de seguridad más amplia.

- **BitDefender ofrece una gestión SaaS sencilla y un amplio ecosistema de socios.** BitDefender se centra en la seguridad de puntos de conexión y se ha ampliado para incluir protección de cargas de trabajo en la nube y servicios gestionados. Cuenta con funciones de prevención de *malware* y de vulnerabilidad de la seguridad líderes del mercado, validadas mediante pruebas de terceros y puntuaciones que valoran la eficacia proporcionada por el cliente. El amplio ecosistema de socios de BitDefender utiliza la telemetría recopilada de varias fuentes de consumidores y empresas. Esto se combina con el compromiso corporativo de automatizar la prevención y detección de amenazas en distintos tipos de ataques y entornos actuales, mientras se prepara a los clientes para amenazas futuras a través de su compromiso con la investigación y la participación en la comunidad (por ejemplo, la participación de Bitdefender en el intento de estandarización de la criptografía poscuántica).

  BitDefender ha pasado a una plataforma SaaS para gestionar la mayoría de sus capacidades de seguridad *endpoint*. Sin embargo, sus capacidades de control de aplicaciones en dispositivos locales no son compatibles con su plataforma SaaS. Es probable que sus capacidades de análisis de comportamiento no satisfagan a aquellos compradores avanzados que buscan un mayor nivel de

análisis y correlación de comportamiento de los usuarios. Con sede central en Rumanía y cobertura de ventas y asistencia en todo el mundo, Bitdefender es una opción atractiva para pequeñas y grandes empresas internacionales que buscan una solución fácil de gestionar con pocos requisitos de personal y necesidades limitadas de búsqueda manual de amenazas.

- **Tras su venta, McAfee ha iniciado la transición a soluciones nativas de la nube.** En los últimos años, la empresa estadounidense McAfee ha experimentado muchos cambios a medida que su estrategia dejaba de estar centrada en dispositivos locales y pasaba a focalizarse en soluciones nativas de la nube. En marzo de 2021 se anunció que el grupo empresarial se vendía a Symphony Technology Group y constituye el cambio más reciente. Aunque sigue teniendo una gran base de clientes para su producto de seguridad *endpoint* en dispositivos locales, McAfee ha estado trabajando para trasladar a los clientes a su nuevo servicio en la nube, MVISION, que combina la prevención de amenazas en puntos de conexión, la protección de datos (cifrado/DLP), la seguridad web y una puerta de entrada de seguridad en la nube. Su enfoque en las políticas de seguridad basadas en riesgos también se suele considerar una ventaja para los clientes, ya que cuenta con umbrales de riesgo definidos por el administrador y con información contextual sólida proporcionada por ePO, MVISION Insights y otros recursos de la cartera.

  Varias de las funciones de su cartera *endpoint* siguen en proceso de migración para gestionarse desde la nube, lo que incrementa la dependencia de los compradores. Además, su estrategia de detección ampliada no está desarrollada y todavía no extrae datos de la nube, de la web, de la red ni de fuentes de terceros. Si bien los clientes de referencia expresaron su preocupación por el rumbo de McAfee, seguirá siendo un candidato viable en las listas de opciones de muchas organizaciones si lleva a buen puerto su hoja de ruta durante el próximo año y desarrolla su plataforma de detección para incluir más fuentes que no sean de puntos de conexión.

- **Symantec ofrece amplitud técnica, pero ahora que pertenece a Broadcom necesita espacio para innovar.** Symantec ha dominado el mercado de la seguridad *endpoint* durante décadas. Después de que la empresa estadounidense Broadcom adquiriera Symantec en 2019, los clientes de Forrester expresaron su temor con respecto a la posibilidad de que los competidores de la empresa la dejaran atrás. Aunque al principio, justo después de la adquisición, surgieron problemas relacionados con las ventas y la asistencia, todos se han resuelto. Con una amplia cartera de tecnologías de seguridad *endpoint*, es importante que Symantec no pierda el rumbo bajo el mando de Broadcom y siga innovando. Actualmente, Symantec puede ofrecer una solución SaaS completa que integra en la nube la seguridad de los puntos de conexión con otras fuentes que no son de puntos de conexión. Cuenta con una ventaja competitiva gracias a su amplio abanico de servicios y productos de seguridad de red, correo electrónico, web, datos y nube.

  Los clientes se quejan de que se necesitan demasiadas medidas de correlación entre los diferentes productos de Symantec. Además, la satisfacción del cliente con respecto al detalle de las soluciones y el nivel de automatización fue baja en comparación con la media de este estudio. Si Symantec cumple su hoja de ruta, aquellas empresas que ya hayan invertido en sus productos encontrarán razones de peso para mantenerlos durante un largo tiempo.

- **Sophos ofrece una gama variada de capacidades, pero el rendimiento de sus agentes es inferior al esperado.** Thoma Bravo adquirió la empresa británica Sophos a principios de 2020, sumándose así a la creciente cartera de proveedores de seguridad y gestión de servicios de TI de la empresa de capital privado. Intercept X fue uno de los primeros productos de seguridad

endpoint del mercado en aprovechar el aprendizaje profundo (mediante la adquisición de Invincea) y hoy representa al principal agente *endpoint* principal de Sophos con prevención y detección integradas. Los clientes de Sophos aprecian la estrecha integración entre los servicios de seguridad que ofrece y el producto, así como las funciones integradas de filtrado web y corrección automática del *ransomware*. Sus ofertas de seguridad móvil marcan la diferencia, entre las que se incluyen la defensa contra amenazas móviles y el nivel de integración entre la gestión de la seguridad móvil y *endpoint*.

Varios clientes de Sophos han expresado a Forrester su preocupación por la disminución del rendimiento en la prevención de amenazas y la dificultad del servicio de asistencia para solucionar problemas. Cabe destacar que Sophos cuenta con un largo historial con excelentes resultados en lo que a asistencia se refiere, según se deduce de las puntuaciones que otorgaron los clientes en evaluaciones anteriores de Forrester Wave. Por tanto, Forrester espera que este declive se solucione. Además, los administradores se han quejado por la complejidad para intentar pasar de la creación de políticas a la gestión y las operaciones relacionadas con los productos, incluida la búsqueda manual de amenazas. Aunque Sophos sigue siendo una opción excelente para las pequeñas y medianas empresas que buscan un proveedor con una cartera de tecnologías de seguridad *endpoint* completa, las grandes empresas deben probar el agente Sophos en su entorno para asegurar que es adecuado para el entorno y que es compatible con otras inversiones en seguridad.

Aspirantes

- **BlackBerry amplía la prevención de amenazas más allá de la seguridad convencional de los puntos de conexión.** BlackBerry Cyber Suite (anteriormente Cylance Protect) combina la protección de prevención de *malware* basada en el aprendizaje automático con capacidades de paquete como control de aplicaciones, capacidades de solución de ataques y gestión de seguridad nativa. Los clientes puntúan negativamente el impacto en el rendimiento pero dejan constancia de una gran satisfacción con respecto a las principales capacidades de prevención de *malware*. Las capacidades de autenticación constantes de BlackBerry a través de Persona siguen siendo únicas entre la competencia y prestan tanto servicios de autenticación como de gestión de riesgos, especialmente cuando se tienen en cuenta los planes del proveedor para ampliar su cobertura más allá de los *endpoints* del usuario (por ejemplo, IoT y automoción).

  La falta de análisis de comportamiento y de capacidades de prevención de vulnerabilidad de la seguridad impiden que alcance el podio en esta evaluación, y tampoco deja buen sabor de boca la limitación de sus funciones de seguridad *endpoint* gestionados por SaaS (algunas aún requieren gestión en los dispositivos locales). Los datos EDR de BlackBerry no se alojan en su nube, algo que sus competidores sí hacen de forma habitual, pero Forrester ha averiguado que este punto se resolverá en Optics 3 en el segundo trimestre de 2021. En general, BlackBerry ofrece varias oportunidades entre la gestión de *endpoints* y las inversiones en seguridad. Además, su metodología Zero Trust centrada en identidades probablemente resulte atractiva para las organizaciones que buscan enfoques exclusivos para supervisar y proteger los puntos de conexión.

Descripción general de la evaluación

Evaluamos a los proveedores en base a 24 criterios, que agrupamos en tres categorías principales:

- **Oferta actual.** La posición de cada proveedor en el eje vertical del gráfico de Forrester Wave indica la fuerza de su oferta actual. Entre los criterios fundamentales de estas soluciones se incluyen la prevención y la detección de amenazas, el control y el rendimiento del producto.
- **Estrategia.** La ubicación en el eje horizontal indica la fuerza de las estrategias de los proveedores. Evaluamos la hoja de ruta del producto, la percepción y el enfoque corporativos, la compatibilidad con el marco de trabajo Zero Trust y la participación de la comunidad en materia de seguridad.
- **Presencia en el mercado.** Representadas por el tamaño de los marcadores en el gráfico, nuestras puntuaciones de presencia en el mercado reflejan cada ecosistema de socios de los distribuidores y cada base de clientes empresariales.

Criterios de inclusión del proveedor

Forrester incluyó a 12 proveedores en la evaluación: Bitdefender, BlackBerry, Cisco, CrowdStrike, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Symantec, Trend Micro y VMware. Cada uno de estos proveedores dispone de:

- **Un paquete de seguridad basado en SaaS que puede prevenir, detectar y solucionar las amenazas de los puntos de conexión.** Consideramos que las soluciones que ofrecen solo una o dos de estas tres capacidades son productos específicos, no paquetes de seguridad. El producto debe haber estado en el mercado durante 12 meses previos a la fecha límite para enviar la encuesta Forrester Wave.
- **Un alto grado de interés por parte de los compradores de Forrester.** Solo incluimos a aquellos proveedores de los directivos en materia de seguridad empresarial que demuestran tener un gran interés, tal como determinan las menciones de consultas de clientes de Forrester. Por ejemplo, los clientes de Forrester realizan preguntas específicas sobre los proveedores durante las consultas y llevan a cabo otras interacciones.
- **Una fuerte presencia en el mercado empresarial.** Solo incluimos a aquellos proveedores que cuenten con, al menos, 600 clientes empresariales (cada uno con más de 1000 nodos implementados) en su plataforma SaaS en la fecha límite establecida por Forrester Wave.

Hable con un analista

Aumente la confianza en sus decisiones trabajando con los líderes de opinión de Forrester para aplicar nuestras investigaciones a sus iniciativas empresariales y tecnológicas específicas.

Consulta con un analista

Si necesita ayuda para poner en práctica las investigaciones, póngase en contacto con un analista y resuelva sus dudas en una sesión telefónica de 30 minutos, o plantee las preguntas por correo electrónico.

Más información

Asesoramiento de analistas

Ponga en práctica las investigaciones trabajando con un analista en un compromiso específico en forma de sesiones, talleres o charlas.

Más información.

Seminarios web

Únase a nuestras sesiones online sobre las últimas investigaciones que afectan a su negocio. Cada llamada incluye una sesión de preguntas y respuestas con un analista y diapositivas. También está disponible bajo demanda.

Más información

Aplicaciones de investigación de Forrester para iOS y Android.
Vaya un paso por delante de la competencia, independientemente de dónde se encuentre.

Material complementario

Recurso en línea

Publicamos todas nuestras puntuaciones y ponderaciones de Forrester Wave en un archivo Excel que ofrece evaluaciones detalladas de productos y clasificaciones personalizables. Se puede descargar esta herramienta haciendo clic en el enlace al comienzo de este informe en Forrester.com. Nuestra intención es que estas puntuaciones y ponderaciones predeterminadas solo sirvan como punto de partida y animen a los lectores a adaptar dichas ponderaciones a sus necesidades individuales.

La metodología de Forrester Wave

Un informe de Forrester Wave es una guía para compradores que estén analizando sus opciones de adquisición en el mercado tecnológico. Para ofrecer un proceso equitativo a todos los participantes, Forrester sigue la guía de la metodología de Forrester Wave™ a fin de evaluar a los proveedores participantes.

En nuestra revisión, llevamos a cabo una investigación inicial para elaborar una lista de proveedores candidatos de la evaluación. A partir de ese conjunto inicial de proveedores, restringimos nuestra lista final según los criterios de inclusión. Luego, recopilamos detalles del producto y la estrategia a través de un cuestionario detallado, demostraciones/informes, entrevistas y encuestas de referencia de clientes. Utilizamos estos datos, junto con los conocimientos y la experiencia de los analistas del mercado, para valorar a los proveedores mediante un sistema de puntuación relativa que compara a cada proveedor con los demás en la evaluación.

Incluimos la fecha de publicación de Forrester Wave (trimestre y año) claramente en el título de cada informe de Forrester Wave. Evaluamos a los proveedores que participan en este informe de Forrester Wave con los materiales que nos proporcionaron antes del 23 de febrero de 2021 y no permitimos recibir ninguna información adicional después de esta fecha. Animamos a los lectores a evaluar cómo cambian las ofertas del mercado y de los proveedores con el tiempo.

De acuerdo con la política de revisión de proveedores de Forrester Wave™ y New Wave™, Forrester solicita a los proveedores que revisen nuestros resultados antes de publicarlos para verificar su precisión. Los proveedores marcados como proveedores no participantes en el gráfico de Forrester Wave cumplían nuestros criterios de inclusión definidos, pero declinaron su participación o contribuyeron solo parcialmente en dicha evaluación. Puntuamos a estos proveedores de acuerdo con la política de proveedores de participación parcial o no participantes de Forrester Wave™ y de Forrester New Wave™ y publicamos su posición junto con aquellos proveedores que sí han participado.

Política de integridad

Llevamos a cabo toda nuestra investigación, incluidas las evaluaciones de Forrester Wave, de conformidad con la política de integridad publicada en nuestro sitio web.

Ayudamos a los líderes empresariales y tecnológicos a utilizar el foco en el cliente para acelerar el crecimiento.

PRODUCTOS Y SERVICIOS

- Investigación y herramientas
- Ayuda de analistas
- Datos y análisis
- Colaboración entre compañeros
- Consultoría
- Eventos
- Programas de certificación

Las investigaciones y los conocimientos de Forrester se adaptan a su función y a sus iniciativas empresariales esenciales.

FUNCIONES A LAS QUE PRESTAMOS SERVICIO

Profesionales de estrategia y marketing

Director de marketing
Marketing B2B
Marketing B2C
Experiencia del cliente
Conocimiento del cliente
eBusiness y estrategia de canal

Profesionales de gestión de la tecnología

Director de informática (CIO)
Desarrollo y entrega de aplicaciones
Arquitectura empresarial
Infraestructura y operaciones
- Seguridad y riesgos

Abastecimiento y gestión de proveedores

Profesionales del sector de la tecnología

Relaciones con analistas

ATENCIÓN AL CLIENTE

Para obtener información sobre las reimpresiones en papel o electrónicas, póngase en contacto con el servicio de atención al cliente en +1 866-367-7378, +1 617-613-5730, o a través del correo electrónico clientsupport@forrester.com. Ofrecemos descuentos por cantidad y precios especiales para instituciones académicas y sin ánimo de lucro.