Cuadrante mágico para plataformas de protección de endpoints

23 de septiembre de 2024 - ID G00808300 - 44 min de lectura

Por Evgeny Mirolyubov, Franz Hinner y 3 más

Todas las soluciones de este Cuadrante Mágico ofrecen protección eficaz contra los ataques más comunes.
Los compradores deben evaluar a los proveedores de EPP incluidos en el contexto de una estrategia integral de seguridad del espacio de trabajo y proyectos de modernización de operaciones de seguridad más amplios.

Supuestos de la planificación estratégica

Para 2028, el 30% de las empresas adoptarán seguridad preventiva de puntos finales, detección y respuesta de puntos finales y detección y respuesta a amenazas de identidad del mismo proveedor, frente a aproximadamente el 5% en 2024.

Para 2029, el 50 % de las organizaciones evaluarán las plataformas de protección de puntos finales como parte de una estrategia integral de seguridad del espacio de trabajo, frente a aproximadamente el 20 % en 2024.

Definición/Descripción del mercado

Nota: Debido a que Gartner ha interrumpido la cobertura de todos los proveedores rusos, es posible que haya proveedores que cumplieran con los criterios de inclusión descritos, pero que no hayan sido evaluados. Estos proveedores no están incluidos en esta investigación.

Gartner define una plataforma de protección de endpoints (EPP) como un software de seguridad diseñado para proteger endpoints administrados (incluidos equipos de escritorio, portátiles, dispositivos móviles y, en algunos casos, endpoints de servidores) contra ataques maliciosos conocidos y desconocidos. Las EPP brindan capacidades para que los equipos de seguridad investiguen y solucionen incidentes que evaden los controles de prevención. Los productos EPP se entregan como agentes de software, se implementan en endpoints y se conectan a consolas de administración y análisis de seguridad centralizadas.

Los EPP proporcionan un control de seguridad defensivo para proteger los puntos finales de los usuarios finales contra infecciones de malware conocidas y desconocidas mediante una combinación de técnicas de seguridad (como análisis estático y de comportamiento) y controles del sistema (como control de dispositivos y administración del firewall del host). Las capacidades de prevención y protección de EPP se implementan como parte de una estrategia de defensa en profundidad para ayudar a reducir la superficie de ataque y minimizar el riesgo de vulneración de los puntos finales. Las capacidades de detección y respuesta de EPP se utilizan para descubrir, investigar y responder a las amenazas de los puntos finales que evaden la prevención de seguridad, a menudo como parte de plataformas de operaciones de seguridad más amplias.

Capacidades imprescindibles

Las capacidades imprescindibles para este mercado incluyen:

- Prevención y protección contra amenazas de seguridad, incluido malware que utiliza técnicas de ataque basadas en archivos y sin archivos.
- La capacidad de detectar y prevenir amenazas mediante el análisis del comportamiento de los puntos finales, las aplicaciones y la actividad del usuario final.

Capacidades estándar

Las capacidades estándar para este mercado incluyen:

- Gestión y generación de informes sobre controles de seguridad del sistema operativo, como firewall de host, control de dispositivos y cifrado de puntos finales.
- Evaluación de puntos finales en busca de vulnerabilidades y generación de informes de riesgos basados en el inventario, la configuración, los parches y las políticas de los dispositivos de puntos finales.
- Funcionalidad integrada de detección y respuesta de puntos finales (EDR) que permite la recopilación de telemetría sin procesar, la personalización de la detección, la investigación posterior al incidente y la remediación.
- Envoltorios de servicios entregados por socios y proveedores, como detección y respuesta administradas (MDR) y monitoreo de seguridad coadministrado.

Capacidades opcionales

Las capacidades opcionales para este mercado incluyen:

- Capacidades de gestión de configuración de seguridad que permiten una evaluación continua frente a las mejores prácticas de configuración.
- Integraciones de seguridad del espacio de trabajo con seguridad de correo electrónico, servicio de seguridad perimetral, protección de identidad y controles de seguridad de datos.
- Detección y respuesta extendidas integradas (XDR) que permiten la recopilación, investigación y remediación de telemetría en múltiples controles de seguridad.
- Capacidades de gestión de parches o activación de controles de seguridad compensatorios para vulnerabilidades no parcheadas.
- Soporte extendido para sistemas operativos al final de su vida útil, poco comunes o cargas de trabajo de servidores heredados.

Cuadrante mágico

Figura 1: Cuadrante mágico para plataformas de protección de endpoints

Puntos fuertes y precauciones de los proveedores

Bitdefender

Bitdefender es un visionario en este Cuadrante Mágico. Bitdefender GravityZone es el producto EPP estrella. Además del EPP básico, Bitdefender ofrece seguridad de correo electrónico y análisis de riesgos humanos emergentes, seguridad en la nube y capacidades de detección y respuesta extendidas (XDR).

Bitdefender lanzó recientemente capacidades de gestión de incidentes unificadas para su detección y respuesta de endpoints (EDR) y alertas XDR, amplió el análisis de seguridad a los riesgos de la nube y de identidad humana, e integró su producto de defensa contra amenazas móviles en XDR. Bitdefender también ha ampliado su compatibilidad con la gestión de parches para macOS. Bitdefender también ha completado la adquisición de Horangi Cyber Security, ampliando su cartera de servicios y tecnología de seguridad, así como su alcance geográfico en el sudeste asiático.

El producto insignia de EPP de Bitdefender es ideal para pequeñas y medianas empresas que priorizan la facilidad de uso y la eficacia de la protección, así como para aquellas que buscan una ampliación de los servicios de detección y respuesta gestionados (MDR). Este proveedor también atiende a organizaciones que buscan una implementación de EPP entregada en la nube, híbrida o local (incluida la implementación con aislamiento).

Strengths

- Estrategia de producto: Bitdefender cuenta con una sólida hoja de ruta de productos que se alinea con los requisitos de sus clientes objetivo, pequeños y medianos.
- Experiencia del cliente: Los clientes generalmente califican como bueno el soporte que reciben de Bitdefender.
- Ejecución de ventas: Los precios de Bitdefender son generalmente más bajos que el promedio en comparación con otros proveedores en este Cuadrante Mágico.

Cautions

- Capacidad de respuesta del mercado y trayectoria: la participación de Bitdefender en el mercado EPP sigue siendo significativamente inferior a la de los líderes y retadores en este Cuadrante Mágico.
- Operaciones: Bitdefender es una empresa más pequeña y sus operaciones están menos diversificadas en comparación con los líderes del mercado EPP.
- Viabilidad general: Bitdefender está creciendo más lentamente en comparación con los líderes del mercado EPP en este Cuadrante Mágico.

Broadcom

Broadcom es un actor de nicho en este Cuadrante Mágico. Tras la adquisición de VMware, Broadcom ofrece dos productos EPP como parte de su Grupo de Seguridad Empresarial: Symantec Endpoint Security (SES) Complete y Carbon Black Cloud EPP. Además de las capacidades básicas de EPP, Broadcom ofrece una amplia gama de productos integrados de forma flexible en toda su cartera de seguridad. Gartner espera que se produzca una racionalización en la cartera de productos EPP de Broadcom debido a las superposiciones en las capacidades de los productos existentes.

Broadcom lanzó recientemente varias mejoras incrementales a sus productos EPP. Symantec Endpoint Security Complete mejoró la aplicación de políticas de integridad de red, controles de acceso basados en roles para acciones de respuesta, flujos de trabajo de administración de políticas y excepciones, integración de seguridad móvil con herramientas de administración de endpoints. Las mejoras de Carbon Black Cloud incluyeron mejoras de diseño en la página de clasificación de alertas, mejor seguimiento del estado de actualización de agentes, mayor personalización de políticas, una nueva versión de la aplicación Splunk y una mejor recopilación de telemetría de endpoints.

Los productos EPP de Broadcom son históricamente adecuados para grandes empresas globales que están familiarizadas con las ofertas del proveedor, tienen la experiencia para gestionar la solución internamente y prefieren los acuerdos empresariales para simplificar la adquisición. El proveedor ha declarado públicamente recientemente un cambio en la estrategia de comercialización, ampliando su enfoque a los segmentos del mercado medio y las PYMES a través de socios de canal y

Distribuidores. Este proveedor también atiende a organizaciones que buscan una implementación de EPP entregada en la nube (incluido GovCloud), híbrida o local (incluido el air gap).

Broadcom no respondió a las solicitudes de información complementaria, por lo que el análisis de Gartner se basa en otras fuentes creíbles.

Strengths

- Conocimiento del mercado: Broadcom tiene un buen conocimiento del mercado EPP y sus competidores, con su enfoque histórico en grandes empresas globales.
- Estrategia vertical: Broadcom continúa ofreciendo una combinación de implementaciones EPP locales, híbridas y entregadas en la nube que atraen a ciertos sectores verticales de la industria.
- Estrategia de ventas: Broadcom tiene una estrategia de ventas enfocada y alineada con los objetivos del proveedor de vender a grandes empresas globales.

Cautions

- Experiencia del cliente: Los comentarios de los clientes indican que el soporte técnico y la gestión de cuentas que reciben de Broadcom son variables y que el producto puede afectar el rendimiento durante el escaneo.
- Estrategia de producto: Es poco probable que las recientes mejoras incrementales de Broadcom a sus productos EPP den forma al mercado EPP más amplio.
- Capacidad de respuesta y trayectoria del mercado: el crecimiento de la participación de mercado de EPP de Broadcom es menor que el de los líderes o retadores del mercado en este Cuadrante Mágico.

Tecnologías de software de Check Point

Check Point Software Technologies es un visionario en este Cuadrante Mágico. Check Point Harmony Endpoint es el producto insignia de EPP. Además del EPP básico, Check Point ofrece capacidades XDR emergentes y un conjunto de productos de seguridad para espacios de trabajo integrados.

Check Point lanzó recientemente una función de prevención de pérdida de datos (DLP) basada en navegador como parte de Harmony Endpoint para mejorar los controles de seguridad de datos, además de las funciones antiphishing y de filtrado de URL existentes habilitadas por la extensión del navegador. Check Point también agregó soporte de inspección del Sistema de nombres de dominio (DNS) como parte de Harmony Endpoint y mejoró su oferta con funciones de detección y respuesta ante amenazas de identidad (ITDR). El proveedor continuó su trabajo para reducir la huella del agente Harmony Endpoint. Check Point también completó la adquisición de Perimeter 81, lo que amplió su alcance en el mercado de servicios de seguridad en el borde (SSE).

El producto insignia de Check Point, EPP, está dirigido a organizaciones que priorizan la facilidad de uso, las capacidades de prevención y la consolidación de la suite de seguridad del espacio de trabajo más amplia. Este proveedor también atiende a

organizaciones que buscan una implementación de EPP entregada en la nube, híbrida o en las instalaciones (incluso con espacio de aire).

Strengths

- Conocimiento del mercado: Check Point tiene un buen conocimiento de la dirección del mercado de EPP, con un enfoque en la consolidación de la seguridad del espacio de trabajo.
- Estrategia geográfica: Check Point admite un número de puntos de presencia geográficos e idiomas superior al promedio en comparación con otros proveedores en esta investigación.
- Ejecución de ventas: Los precios de Check Point son generalmente más bajos que el promedio en comparación con otros proveedores en esta investigación.

Cautions

- Capacidad de respuesta del mercado y trayectoria: la participación de Check Point en el mercado de EPP sigue siendo significativamente inferior a la de los líderes y retadores en este Cuadrante Mágico.
- Experiencia del cliente: Harmony Endpoint consume más recursos en comparación con otros proveedores en esta investigación, lo que puede afectar negativamente el rendimiento del sistema.
- Viabilidad general: Check Point está creciendo más lentamente en comparación con los líderes del mercado EPP en este Cuadrante Mágico.

Cisco

Cisco es un visionario en este Cuadrante Mágico. Cisco Secure Endpoint es el producto insignia de EPP. Además del EPP principal, Cisco ofrece una amplia gama de productos de seguridad en sus suites User Protection, Cloud Protection y Breach Protection.

Cisco lanzó recientemente una versión de Cisco XDR disponible para el público en general, introdujo una nueva capacidad de scripts remotos, agregó funciones de administración de firewall de host y lanzó un marco de diseño de experiencia de usuario (UX) común para sus productos de seguridad. Cisco está en proceso de integrar Identity Intelligence (adquisición de Oort) en toda su cartera. Cisco también completó la adquisición de Splunk, lo que fortalece su posición competitiva en los mercados de operaciones de seguridad y observabilidad.

El producto insignia de EPP de Cisco es ideal para organizaciones que invierten en el conjunto de herramientas de seguridad de Cisco, aquellas que buscan simplificar la adquisición y aquellas que buscan la consolidación de las capacidades de seguridad del espacio de trabajo. Este proveedor también atiende a organizaciones que buscan una implementación de EPP entregada en la nube, híbrida o en las instalaciones (incluidas las que están aisladas).

Strengths

- Conocimiento del mercado: Cisco tiene un buen conocimiento del mercado de EPP, con un enfoque en la consolidación de la seguridad del espacio de trabajo y la modernización de las operaciones de seguridad.

- Estrategia de ventas: La estrategia de ventas de Cisco se beneficia de la recientemente introducida suite User Protection, que combina EPP con otros productos de seguridad del espacio de trabajo, y de la Breach Protection Suite, que combina EPP con XDR y otras tecnologías de detección y respuesta a amenazas.

- Ejecución de ventas: Los precios de Cisco son generalmente más bajos que el promedio en comparación con otros proveedores en esta investigación, especialmente a través de programas de compra, como los Acuerdos Empresariales.

Cautions

- Capacidad de respuesta del mercado y trayectoria: la participación de Cisco en el mercado de EPP sigue siendo significativamente inferior a la de los líderes y retadores en este Cuadrante Mágico.

- Producto: Cisco todavía tiene consolas de administración distintas para los productos Secure Endpoint, Orbital y XDR, lo que puede dificultar la eficacia operativa del uso del producto.

- Viabilidad general: Cisco Secure Endpoint está creciendo más lentamente en comparación con los líderes del mercado EPP en este Cuadrante Mágico.

Golpe de masas

CrowdStrike es líder en este Cuadrante Mágico. CrowdStrike Falcon es el producto insignia de EPP. Además del EPP principal, CrowdStrike ofrece un conjunto cada vez mayor de productos de seguridad integrados, que incluyen protección de identidad, seguridad en la nube, detección y respuesta extendidas, entre otros.

CrowdStrike lanzó recientemente su oferta inicial de protección de datos de endpoints. Además, el proveedor lanzó la solución Falcon for IT para la gestión de endpoints, el cumplimiento normativo y la supervisión del rendimiento.
CrowdStrike también ha lanzado Falcon NG-SIEM, que mejora la presentación de detecciones en toda su cartera de productos nativos y controles de seguridad de terceros. Falcon Flex es el nuevo modelo de licencia del proveedor. CrowdStrike también ha completado sus adquisiciones de Bionic y Flow Security, lo que fortalece su posición en seguridad de aplicaciones y en la nube.

El producto insignia de CrowdStrike, EPP, es ideal para una amplia gama de organizaciones en todo el mundo, especialmente aquellas que buscan modernizar las operaciones de seguridad o ampliar los servicios de MDR. Este proveedor está dirigido a organizaciones que buscan una implementación de EPP en la nube (incluido GovCloud).

El 19 de julio de 2024, la actualización de contenido de CrowdStrike para el cliente Falcon provocó una interrupción que afectó a millones de sistemas Windows en varias empresas de todo el mundo. CrowdStrike respondió rápidamente retirando la actualización defectuosa, apoyando los esfuerzos de recuperación del cliente y anunciando mejoras en la resistencia y las pruebas del software. Gartner tuvo en cuenta este incidente en la evaluación de CrowdStrike. Gartner también ha proporcionado un análisis más detallado de este incidente y las implicaciones para los clientes y clientes potenciales de CrowdStrike en una investigación publicada fuera de esta evaluación comparativa.

Strengths

- Capacidad de respuesta al mercado y trayectoria: la participación de CrowdStrike en el mercado de EPP y su tasa de consideración por parte de los compradores de EPP son significativas.

- Experiencia del cliente: Los clientes generalmente califican como sólidos el soporte técnico, la administración de cuentas y los servicios de seguridad administrados de CrowdStrike.
- Estrategia de producto: La estrategia de producto y la hoja de ruta de seguridad de CrowdStrike están alineadas con los requisitos emergentes de los clientes.

Cautions

- Operaciones: El incidente del Channel File 291 de CrowdStrike del 19 de julio de 2024 reveló limitaciones en las prácticas de garantía de calidad y pruebas de contenido de seguridad del proveedor.
- Ejecución de ventas: los precios de CrowdStrike son más altos que el promedio en comparación con otros proveedores en esta investigación, y su creciente conjunto de SKU de productos se está volviendo cada vez más complejo.
- Estrategia geográfica: CrowdStrike admite un número de idiomas inferior al promedio y un número promedio de puntos geográficos de presencia en comparación con otros proveedores en esta investigación.

Ciberreacción

Cybereason es un actor de nicho en este Cuadrante Mágico. Cybereason Defense Platform es el producto insignia de EPP. Además del EPP principal, Cybereason ofrece capacidades XDR emergentes.

Recientemente, Cybereason mejoró sus capacidades antimanipulación en el agente de Windows para proteger el software del agente contra modificaciones no deseadas. El proveedor también mejoró la gestión de exclusiones de EPP al trasladar todos los elementos de configuración relacionados con las exclusiones a una sola página unificada.
Cybereason ha mejorado la compatibilidad de los agentes para las implementaciones de servidores, lo que permite a las organizaciones actualizar versiones menores de los agentes sin actualizar el sistema operativo del servidor. Cybereason continúa con su estrategia de detección y respuesta (SDR) de SIEM superponiendo las capacidades de detección y respuesta a los lagos de datos empresariales existentes.

El producto insignia de EPP de Cybereason es ideal para empresas con equipos de operaciones de seguridad bien dotados de personal que buscan capacidades EDR profundas, así como para organizaciones de tamaño mediano que buscan una ampliación del servicio MDR. Este proveedor también atiende a organizaciones que buscan una implementación de EPP entregada en la nube, híbrida o en las instalaciones (incluidas las que están aisladas).

Strengths

- Conocimiento del mercado: Cybereason tiene un buen conocimiento del mercado de EPP y sus competidores, con un enfoque en brindar servicios MDR a empresas medianas.
- Ejecución de ventas: Los precios de Cybereason son generalmente más bajos que el promedio en comparación con otros proveedores en este Cuadrante Mágico.
- Producto: La funcionalidad EDR de Cybereason es generalmente bien valorada por los clientes por su eficacia y facilidad de uso.

Cautions

- Estrategia de producto: Los desarrollos de productos recientes y planificados de Cybereason, como la gestión unificada de exclusiones y la gestión de vulnerabilidades, se implementan más lentamente en comparación con los líderes del mercado en este Cuadrante Mágico.

- Innovación: Es menos probable que las innovaciones recientes de Cybereason, como la nueva oferta de seguridad móvil y la compatibilidad mejorada de agentes para implementaciones de servidores, den forma al mercado EPP más amplio.

- Estrategia de ventas: según las consultas de los clientes finales de Gartner y los comentarios de los clientes de Peer Insights, Cybereason rara vez se incluye en las listas de proveedores de EPP competitivos en comparación con los líderes del mercado en este Cuadrante Mágico.

ESET

ESET es un competidor en este Cuadrante Mágico. ESET PROTECT es el producto insignia de EPP. Además del EPP principal, ESET ofrece seguridad de correo electrónico, autenticación multifactor, filtrado de contenido web y DNS, almacenamiento de archivos en red y otras capacidades de seguridad.

ESET lanzó recientemente ESET Connect, una puerta de enlace API REST para abrir su solución a integraciones de terceros. ESET también ha mejorado su Cloud Office Security con soporte adicional para Google Workspace, brindando protección para Gmail y Google Drive contra malware, phishing y ataques de compromiso de correo electrónico empresarial (BEC). El proveedor presentó un nuevo servicio MDR adaptado a las necesidades de sus pequeñas y medianas empresas. ESET también ha rediseñado y mejorado el soporte para sistemas operativos móviles, como Android e iOS, y ha mejorado sus capacidades de remediación automatizada y gestión de incidentes.

El producto insignia de ESET, EPP, es ideal para organizaciones pequeñas y medianas en las zonas geográficas donde opera, en particular aquellas que priorizan la facilidad de uso y la eficacia de la prevención. Este proveedor también atiende a organizaciones que buscan una implementación de EPP en la nube, híbrida o local (incluida la implementación con aislamiento).

Strengths

- Viabilidad general: ESET tiene una larga trayectoria y un crecimiento constante de los ingresos en el mercado de EPP.

- Experiencia del cliente: Los clientes generalmente califican como bueno el soporte que reciben de ESET.

- Estrategia vertical: ESET tiene una base de clientes bien diversificada en la mayoría de los sectores verticales de la industria y demuestra una buena comprensión de los requisitos verticales únicos.

Cautions

- Estrategia de producto: Es menos probable que las mejoras de productos planificadas y recientemente agregadas por ESET, como la compatibilidad con dispositivos móviles y ESET Connect, den forma al mercado EPP en general.

- Estrategia de ventas: según las consultas de los clientes finales de Gartner y los comentarios de los clientes de Peer Insights, ESET rara vez se incluye en las listas de proveedores de EPP competitivos en comparación con los líderes del mercado en este Cuadrante Mágico.

- Comprensión del mercado: la comprensión del mercado de ESET se centra en las necesidades de sus clientes pequeños y medianos en lugar del mercado EPP más amplio.

Fortinet

Fortinet es un actor de nicho en este Cuadrante Mágico. FortiEDR es el producto insignia de EPP. Además del EPP principal, Fortinet ofrece una amplia gama de productos integrados en toda su cartera de seguridad.

Fortinet lanzó recientemente mejoras incrementales en la interfaz de usuario (UI) de FortiEDR, integró FortiEDR con FortiClient en un agente de seguridad unificado para protección y acceso remoto, y mejoró la priorización de vulnerabilidades en su producto. Fortinet también lanzó funciones de administración de firewall de host y cifrado de disco completo, así como también introdujo soporte para sistemas operativos móviles, como Android e iOS.

Fortinet continúa buscando mejoras en la facilidad de uso y la paridad de funciones en sistemas operativos que no sean Windows.

El producto insignia de EPP de Fortinet es ideal para organizaciones que invierten en la gama más amplia de ofertas de seguridad de Fortinet, así como para aquellas que buscan una ampliación de los servicios de MDR. Este proveedor también atiende a organizaciones que buscan una implementación de EPP entregada en la nube, híbrida o en las instalaciones (excluidas las que están aisladas).

Strengths

- Estrategia geográfica: Fortinet admite un número de puntos de presencia geográficos superior al promedio en comparación con otros proveedores en esta investigación.

- Ejecución de ventas: Los precios de Fortinet son generalmente más bajos que el promedio en comparación con otros proveedores en este Cuadrante Mágico.

- Viabilidad general: el crecimiento de los ingresos de Fortinet en el mercado EPP es mayor que el de otros actores de nicho.

Cautions

- Capacidad de respuesta del mercado y trayectoria: la participación de Fortinet en el mercado de EPP sigue siendo significativamente inferior a la de los líderes y retadores del mercado en este Cuadrante Mágico.

- Estrategia de producto: Las mejoras recientes y planificadas de los productos de Fortinet, como la interfaz de usuario mejorada y la paridad de funciones en sistemas operativos que no son Windows, parecen centrarse en cerrar brechas técnicas en lugar de impulsar la innovación.

- Innovación: Es menos probable que las innovaciones recientes de Fortinet, como la integración de FortiRecon con FortiEDR para la priorización de vulnerabilidades y exposiciones comunes (CVE) y seguridad móvil, den forma al mercado EPP empresarial más amplio.

Microsoft

Microsoft es líder en este Cuadrante Mágico. Microsoft Defender for Endpoint es el producto insignia de EPP. Además del EPP principal, Microsoft ofrece una amplia gama de productos de seguridad en varios paquetes de productos.

Microsoft consolidó recientemente Defender XDR con Microsoft Sentinel, unificando la experiencia del usuario en estas herramientas de operaciones de seguridad. Microsoft también lanzó capacidades de administración de configuraciones directamente en su producto EPP, reduciendo la dependencia administrativa de Microsoft Intune. El proveedor lanzó una versión de Extended Berkeley Packet Filter (eBPF) de su agente Linux en un intento por mejorar la capacidad de administración, la utilización de recursos y la eficacia de la protección en el sistema operativo Linux. Microsoft también está en proceso de unificar sus agentes de endpoint para simplificar la experiencia de implementación y las operaciones.

El producto insignia de EPP de Microsoft es ideal para una amplia gama de organizaciones en todo el mundo, especialmente aquellas que invierten en el ecosistema tecnológico de Microsoft y que buscan la consolidación de proveedores de seguridad. Este proveedor está dirigido a organizaciones que buscan una implementación de EPP en la nube (incluido GovCloud).

El 12 de enero de 2024, el equipo de seguridad de Microsoft detectó un ataque a sus sistemas corporativos.
Microsoft respondió rápidamente activando sus procedimientos de respuesta internos y mitigando el impacto del incidente. El proveedor incorporó las lecciones del incidente en su Iniciativa de Futuro Seguro (SFI), que se lanzó en noviembre de 2023. Gartner ha proporcionado un análisis más detallado de este incidente y las implicaciones para los clientes y clientes potenciales de Microsoft en una investigación publicada fuera de esta evaluación comparativa.

Strengths

- Capacidad de respuesta al mercado y trayectoria: la participación de Microsoft en el mercado de EPP y la tasa de consideración por parte de los compradores de EPP son significativas.
- Estrategia de producto: La estrategia de producto y la hoja de ruta de seguridad de Microsoft están alineadas con los requisitos emergentes de los clientes en torno a la consolidación de las operaciones de seguridad.
- Estrategia de ventas: Microsoft tiene una estrategia de ventas eficaz y una base de clientes grande y establecida que presenta oportunidades para seguir expandiendo el alcance de sus productos EPP.

Cautions

- Experiencia del cliente: Los clientes indican que el soporte técnico y el soporte de gestión de cuentas que reciben de Microsoft son variables.
- Ejecución de ventas: Los clientes informan que el modelo de licencias de Microsoft es complejo y difícil de entender.

- Estrategia vertical: Microsoft ofrece opciones limitadas de empaquetado, precios y descuentos de productos específicos de la industria y no admite implementaciones de EPP locales.

Redes de Palo Alto

Palo Alto Networks es líder en este Cuadrante Mágico. Cortex XDR es el producto insignia de EPP. Además del EPP principal, Palo Alto Networks ofrece una amplia gama de productos de seguridad integrados para seguridad de redes, seguridad en la nube y operaciones de seguridad.

Palo Alto Networks presentó recientemente un agente de punto final unificado que combina su solución de plataforma de protección de carga de trabajo en la nube (CWPP) y EDR, y mejoró las capacidades forenses en su plataforma XDR. El proveedor también agregó módulos de seguridad avanzados para mejorar sus capacidades de protección, que incluyen protección de interfaz de firmware extensible unificada (UEFI) contra ataques previos al arranque y protección en escritura para Windows. Palo Alto Networks también completó la adquisición de Talon, una empresa de navegadores empresariales, para fortalecer su oferta de borde de servicio de acceso seguro (SASE).

El producto insignia de EPP de Palo Alto Networks es ideal para equipos de operaciones de seguridad maduros y bien dotados de personal, organizaciones de seguridad menos maduras que buscan aumentar el servicio de MDR y aquellas que buscan la consolidación de proveedores de seguridad. Este proveedor está dirigido a organizaciones que buscan una implementación de EPP entregada en la nube, incluso en GovCloud.

Strengths

- Estrategia de ventas: Palo Alto Networks tiene una estrategia de ventas eficaz y una base de clientes grande y establecida, lo que presenta oportunidades para continuar expandiendo el alcance de sus productos EPP.
- Experiencia del cliente: Los clientes generalmente califican el soporte técnico, la administración de cuentas y los servicios de seguridad administrados de Palo Alto Networks como sólidos.
- Capacidad de respuesta del mercado y trayectoria: Palo Alto Networks ha ido adquiriendo rápidamente una mayor participación en el mercado de EPP durante el último año.

Cautions

- Ejecución de ventas: los precios de Palo Alto Networks son más altos que el promedio en comparación con otros proveedores en esta investigación.
- Producto: La personalización de productos de Palo Alto Networks requiere una curva de aprendizaje pronunciada y puede ser menos adecuada para equipos de seguridad reducidos y aquellos que buscan facilidad de uso.
- Estrategia vertical: Palo Alto Networks no ofrece públicamente paquetes de productos, precios ni opciones de descuento específicos de la industria.

Centinela Uno

SentinelOne es líder en este Cuadrante Mágico. SentinelOne Singularity es el producto insignia de EPP.
Además del EPP principal, SentinelOne ofrece protección de identidad integrada, seguridad en la nube, detección y respuesta extendidas y otros productos de seguridad.

SentinelOne lanzó recientemente Singularity Operations Center, que unifica la gestión de alertas de seguridad en todas las detecciones de controles de seguridad nativos y de terceros. El proveedor también ha mejorado sus capacidades de evaluación y priorización de vulnerabilidades, introduciendo inventario de activos, evaluación de vulnerabilidades de terceros y del sistema operativo, y vistas de gráficos de activos para identificar y abordar activos administrados y no administrados. SentinelOne también completó la adquisición de Krebs Stamos Group (KSG) y PingSafe, fortaleciendo sus servicios de asesoría y capacidades de seguridad en la nube, respectivamente.

El producto insignia de EPP de SentinelOne es ideal para una amplia gama de organizaciones en todo el mundo, especialmente aquellas que buscan facilidad de uso, amplia compatibilidad con sistemas operativos y ampliación del servicio MDR. Este proveedor atiende a organizaciones que buscan una implementación de EPP entregada en la nube (incluido GovCloud), híbrida o local (incluido el air-gapped).

Strengths

- Capacidad de respuesta al mercado y trayectoria: la participación de SentinelOne en el mercado de EPP y su tasa de consideración por parte de los compradores de EPP son significativas.
- Estrategia de producto: La estrategia de producto y la hoja de ruta de seguridad de SentinelOne están alineadas con los requisitos emergentes de los clientes.
- Experiencia del cliente: Los clientes generalmente califican el soporte técnico, la administración de cuentas y los servicios de seguridad administrados de SentinelOne como sólidos.

Cautions

- Ejecución de ventas: Los precios de SentinelOne son más altos que el promedio en comparación con otros proveedores en esta investigación.
- Estrategia geográfica: SentinelOne admite una cantidad de idiomas inferior al promedio y una cantidad promedio de puntos geográficos de presencia en comparación con otros proveedores en esta investigación.
- Estrategia de ventas: La estrategia de ventas de SentinelOne aún no ha dado como resultado una participación de mercado significativa ni visibilidad de mercado en categorías de productos adyacentes a la solución EPP principal del proveedor.

Sophos

Sophos es líder en este Cuadrante Mágico. Sophos Intercept X Endpoint es el producto insignia de EPP.
Además del EPP principal, Sophos ofrece capacidades XDR emergentes y un conjunto de productos integrados de seguridad del espacio de trabajo.

Sophos lanzó recientemente una nueva función de advertencia de ataque crítico que envía notificaciones urgentes a los clientes cuando se detecta una amenaza activa y persistente en su entorno. El proveedor también ha

Sophos ha mejorado su función de protección adaptativa contra ataques, lo que permite la exención de grupos de dispositivos específicos de los cambios de políticas dinámicas y agrega capacidades de respuesta adicionales. Sophos continúa fortaleciendo su suite de seguridad para espacios de trabajo mediante la integración de agentes en la protección de endpoints y el acceso seguro. El proveedor continuó su trabajo para reducir la huella de su agente de endpoints. Sophos también ha lanzado nuevas asociaciones con Tenable y Veeam centradas en la gestión de exposición y la copia de seguridad y recuperación, respectivamente.

El producto insignia de EPP de Sophos es ideal para pequeñas y medianas empresas que priorizan la facilidad de uso, organizaciones que buscan consolidar las capacidades de seguridad del espacio de trabajo y aquellas que buscan aumentar los servicios de MDR. Este proveedor está dirigido a organizaciones que buscan una implementación de EPP en la nube.

Strengths

- Estrategia de producto: Las recientes mejoras de productos de Sophos, como Adaptive Attack Protection, se centran en brindar servicios MDR y funciones centradas en la prevención a clientes con recursos limitados, y su hoja de ruta de productos está alineada con las necesidades de sus clientes objetivo.
- Estrategia de ventas: Sophos ha sido eficaz al vender su producto EPP junto con servicios MDR a organizaciones pequeñas y medianas con necesidades de ampliación de servicios administrados.
- Viabilidad general: Sophos tiene una larga trayectoria y un crecimiento constante de los ingresos en el mercado EPP.

Cautions

- Producto: Sophos Intercept X Endpoint ofrece menos opciones de personalización del producto en comparación con otros líderes en este Cuadrante Mágico.
- Estrategia vertical: la penetración de mercado de Sophos está sesgada hacia la industria de servicios y el proveedor no admite las implementaciones de EPP locales que requieren algunas verticales.
- Experiencia del cliente: Los clientes indican que el soporte técnico que reciben de Sophos es variable y que el producto puede afectar el rendimiento durante el escaneo.

Enrejado

Trellix es un Challenger en este Cuadrante Mágico. Trellix Endpoint Security Suite es el producto insignia de EPP. Además del EPP principal, Trellix ofrece una amplia gama de productos integrados en toda su cartera de seguridad.

Trellix continúa centrándose en los esfuerzos de unificación de productos y UX mediante la integración de EPP, EDR, XDR y ahora Forensics con Trellix XConsole. El proveedor también ha mejorado su experiencia de implementación de agente de punto final al ofrecer un instalador y un administrador de paquetes unificados en toda su cartera de aplicaciones de punto final. Trellix está buscando la incorporación de capacidades de gestión de exposición y gestión de configuración de seguridad para ayudar a los clientes a evaluar y optimizar la configuración de su EPP.

El proveedor ha lanzado Trellix Thrive para ampliar su oferta de servicios de éxito del cliente.

El producto insignia de EPP de Trellix es ideal para empresas con equipos de seguridad bien dotados de personal que requieren un conjunto integral de capacidades de protección de endpoints y opciones de personalización. Este proveedor está dirigido a organizaciones que buscan una implementación de EPP entregada en la nube (incluido GovCloud), híbrida o local (incluido el air-gapped).

Strengths

- Capacidad de respuesta al mercado y trayectoria: la participación de Trellix en el mercado de EPP es significativamente mayor que la de los actores de nicho y los visionarios.
- Operaciones: Trellix ha seguido aumentando su plantilla de empleados a pesar del desafiante entorno económico.
- Estrategia geográfica: Trellix tiene presencia global de recursos técnicos y de ventas y admite un número de idiomas superior al promedio en su consola de administración en comparación con otros proveedores en esta investigación.

Cautions

- Estrategia de producto: Es menos probable que las recientes mejoras de productos de Trellix, como la unificación de EDR con Forensics, la integración de XConsole y los elementos de la hoja de ruta de productos evaluados para este Cuadrante Mágico, den forma al mercado EPP más amplio.
- Estrategia de ventas: según las consultas de los clientes finales de Gartner y los comentarios de los clientes de Peer Insights, Trellix Endpoint Security Suite se incluye en las listas de proveedores de EPP competitivos con menos frecuencia en comparación con los líderes en este Cuadrante Mágico.
- Producto: Las consolas de administración de Trellix están integradas de forma flexible y solo ofrecen mejoras moderadas en la facilidad de uso del producto en comparación con las versiones anteriores del producto.

Microtendencia

Trend Micro es líder en este Cuadrante Mágico. Trend Vision One — Endpoint Security es el producto insignia de EPP. Además del EPP principal, Trend Micro ofrece una amplia gama de productos de seguridad para espacios de trabajo integrados, que incluyen correo electrónico, seguridad perimetral y otros.

Trend Micro continúa mejorando su experiencia y capacidades de consola única, que van desde la gestión de la superficie de ataque y la gestión de la configuración de seguridad hasta la detección y respuesta extendidas.
Trend Micro también mejoró la priorización de vulnerabilidades con la atribución de CVE explotados activamente. El proveedor continuó con sus esfuerzos de optimización de agentes, amplió el soporte del sistema operativo y agregó nuevas capacidades forenses.
Trend Micro lanzó mejoras en su conjunto de capacidades de detección y respuesta ante amenazas de identidad, lo que ayuda a evaluar la postura de seguridad de los sistemas de identidad y a implementar acciones de mitigación y respuesta automatizadas.

El producto insignia de Trend Micro, EPP, es ideal para una amplia gama de organizaciones en todo el mundo, especialmente aquellas que buscan consolidar una suite de seguridad para el espacio de trabajo más amplia y que buscan una amplia compatibilidad con sistemas operativos. Este proveedor está dirigido a organizaciones que buscan una implementación de EPP en la nube, híbrida o local (incluida la implementación con aislamiento).

Strengths

- conocimiento del mercado: Trend Micro demuestra un sólido conocimiento de los competidores del mercado de EPP y de la dirección del mercado, con un enfoque en la seguridad integral del espacio de trabajo.
- Estrategia de producto: Trend Micro tiene una hoja de ruta de productos que está alineada con los requisitos emergentes del mercado EPP.
- Viabilidad general: Trend Micro tiene una larga trayectoria y un crecimiento constante de los ingresos en el mercado EPP.

Cautions

- Estrategia de ventas: según las consultas de los clientes finales de Gartner y los comentarios de los clientes de Peer Insights, Trend Micro aparece en las listas de proveedores de EPP competitivos con menos frecuencia que otros líderes del mercado en este Cuadrante Mágico.
- Ejecución de ventas: la ejecución de ventas de Trend Micro está por detrás de otros líderes del mercado, con un crecimiento de ingresos comparativamente más lento en el espacio EPP.
- Estrategia geográfica: La penetración de mercado de Trend Micro fuera de Europa y Japón es limitada en comparación con otros líderes en este Cuadrante Mágico.

ConSecure

WithSecure es un actor de nicho en este Cuadrante Mágico. WithSecure Elements Endpoint Security es el producto EPP estrella. Además del EPP principal, WithSecure ofrece protección de correo electrónico y colaboración, seguridad en la nube y capacidades emergentes de XDR y gestión de exposición.

WithSecure lanzó recientemente la primera iteración de sus capacidades ITDR como parte de la solución Elements XDR. WithSecure también lanzó una funcionalidad de control de brotes que puede ajustar dinámicamente la configuración de la política de seguridad en función de la puntuación de riesgo cambiante del dispositivo de punto final y su ubicación. El proveedor también amplió sus detecciones de contexto amplio, mejorando la gestión de alertas en toda su cartera de seguridad, y mejoró la API de Elements, abriendo el producto a más integraciones de terceros predefinidas.

El producto insignia EPP de WithSecure es ideal para pequeñas y medianas empresas en las zonas geográficas donde se brinda soporte, que priorizan la facilidad de uso y buscan una ampliación de los servicios MDR. Este proveedor atiende a organizaciones que buscan una implementación de EPP entregada en la nube o en las instalaciones (incluso con espacio de almacenamiento).

Strengths

- Ejecución de ventas: Los precios de WithSecure son generalmente más bajos que el promedio en comparación con otros proveedores en este Cuadrante Mágico.
- Experiencia del cliente: Los clientes generalmente califican el soporte que reciben de WithSecure como bueno.
- Comprensión del mercado: WithSecure demuestra una buena comprensión del mercado EPP y sus compradores objetivo con la localización de servicios MDR específica de la UE.

Cautions

- Capacidad de respuesta del mercado y trayectoria: la participación de WithSecure en el mercado de EPP sigue siendo significativamente inferior a la de los líderes y retadores en este Cuadrante Mágico.
- Estrategia de ventas: según las consultas de los clientes finales de Gartner y los comentarios de los clientes de Peer Insights, WithSecure aparece en las listas de proveedores de EPP competitivos con menos frecuencia que los líderes del mercado en este Cuadrante Mágico.
- Estrategia geográfica: En nuestra evaluación, la estrategia geográfica de WithSecure está por detrás de la de sus competidores, y la mayoría de los clientes del proveedor están en Europa.

Proveedores agregados y eliminados

Revisamos y ajustamos nuestros criterios de inclusión para los Cuadrantes Mágicos a medida que cambian los mercados. Como resultado de estos ajustes, la combinación de proveedores en cualquier Cuadrante Mágico puede cambiar con el tiempo. La aparición de un proveedor en un Cuadrante Mágico un año y no al año siguiente no indica necesariamente que hayamos cambiado nuestra opinión sobre ese proveedor. Puede ser un reflejo de un cambio en el mercado y, por lo tanto, de un cambio en los criterios de evaluación, o de un cambio de enfoque por parte de ese proveedor.

Agregado

- No se agregaron proveedores a este Cuadrante Mágico.

Abandonó

- Broadcom (VMware) y su producto Carbon Black Cloud EPP ahora se analizan bajo el nombre de proveedor combinado Broadcom.

Criterios de inclusión y exclusión

El Cuadrante Mágico y la investigación de Capacidades Críticas identifican y analizan los proveedores más relevantes y sus productos en un mercado. De manera predeterminada, Gartner utiliza un límite superior de 20 proveedores para respaldar la identificación de los proveedores más relevantes en un mercado. Los criterios de inclusión representan los atributos específicos que los analistas consideran necesarios para la inclusión en esta investigación. Gartner no definió ningún criterio de exclusión para esta investigación.

Para ser elegibles para la inclusión, los proveedores debían cumplir con la definición del mercado de EPP y satisfacer todos los criterios de inclusión utilizando su producto EPP estrella al inicio del proceso de investigación y encuesta de Gartner (el 29 de abril de 2024). Los productos y las capacidades debían estar disponibles en general para ser considerados en la evaluación. Los requisitos incluían:

- La solución es compatible con los sistemas operativos Windows, macOS y Linux.
- La solución combina todas las funcionalidades de prevención, protección, detección y respuesta de seguridad en un solo agente.
- La solución aplica protección basada en agentes mediante una combinación de técnicas de seguridad, como análisis estático y de comportamiento, y controles del sistema, como control de dispositivos y gestión de firewall del host.
- La solución incluye una funcionalidad de detección y respuesta de puntos finales integrada, lo que permite la recopilación de telemetría de puntos finales sin procesar y en tiempo real, la personalización de la detección, la investigación posterior a incidentes y respuesta.
- La solución proporciona una clasificación de gravedad, un árbol de procesos y un mapeo de eventos y alertas a las tácticas, técnicas y procedimientos de MITRE ATT&CK para facilitar el análisis y la remediación de la causa raíz.
- La solución proporciona una infraestructura de gestión y análisis de seguridad multiinquilino, de estilo SaaS y basada en la nube, que mantiene el proveedor de EPP.
- La solución ofrece un acoplamiento estrecho con servicios suministrados por socios o proveedores, como detección y respuesta administradas o monitoreo de seguridad coadministrado.
- Un proveedor debe vender software EPP y sus licencias independientemente de otros productos o servicios.
- Un proveedor debe diseñar, poseer y mantener la mayor parte de su contenido de detección e inteligencia de amenazas internamente. La ampliación del OEM es aceptable si el OEM no es el método de protección principal.
- Un proveedor debe haber participado en al menos dos pruebas públicas reconocidas y centradas en la empresa (por ejemplo, MITRE Engenuity, AV-Comparatives, AV-TEST, SE Labs y MRG Effitas) para evaluar la eficacia de detección dentro de los 12 meses anteriores al 1 de abril de 2024.
- Un proveedor debe tener más de 7,5 millones de puntos finales con licencia protegidos y administrados activamente mediante su EPP al 29 de abril de 2024. Más de 500 000 deben ser instalaciones de producción activas con cuentas de más de 500 puestos. La proporción de clientes empresariales en una sola región fuera de América del Norte o Europa no debe superar el 60 % del número total.

Criterios de evaluación

Capacidad de ejecución

Los analistas de Gartner evalúan a los proveedores en función de la calidad y eficacia de los procesos, sistemas, métodos y procedimientos que utilizan para ser competitivos, eficientes y efectivos, y para mejorar sus ingresos, retención y reputación.

Producto o servicio: este criterio evalúa los bienes y servicios principales de un proveedor que compiten en el mercado definido o lo atienden. Incluye las capacidades actuales del producto y servicio, la calidad, los conjuntos de características, las habilidades, etc. Estos pueden ofrecerse de forma nativa o a través de acuerdos o asociaciones con fabricantes de equipos originales, tal como se define en la sección Definición/descripción del mercado y se detalla en los subcriterios. Los factores de evaluación incluyen las capacidades principales del producto y servicio, la profundidad y amplitud de la funcionalidad y la disponibilidad de complementos de seguridad.

Viabilidad general: este criterio evalúa la salud financiera general de un proveedor, así como el éxito financiero y práctico de la unidad de negocios. También analiza la probabilidad de que la organización continúe ofreciendo e invirtiendo en el producto, así como la posición del producto en la cartera actual. Los factores de evaluación incluyen la salud financiera general y la contribución del EPP al crecimiento de los ingresos.

Ejecución de ventas/fijación de precios: este criterio aborda las capacidades de un proveedor en todas las actividades de preventa y la estructura que las respalda. Incluye la gestión de acuerdos, la fijación de precios y la negociación, el apoyo de preventa y la eficacia general del canal de ventas. Los factores de evaluación incluyen la ejecución de las actividades de preventa, la competitividad de los precios de los productos y servicios y las revisiones de las propuestas de los clientes finales de Gartner.

Capacidad de respuesta/historial del mercado: este criterio evalúa la capacidad de un proveedor para responder, cambiar de dirección, ser flexible y lograr el éxito competitivo a medida que surgen oportunidades, actúan los competidores, evolucionan las necesidades de los clientes y cambia la dinámica del mercado. También se tiene en cuenta el historial de capacidad de respuesta del proveedor a las cambiantes demandas del mercado. Los factores de evaluación incluyen la capacidad de respuesta general a las tendencias del mercado de protección de puntos finales, la cuota de mercado y la tasa de crecimiento relativa de la cuota.

Experiencia del cliente: Este criterio evalúa los productos y servicios y/o programas de un proveedor que permiten a los clientes lograr los resultados previstos con los productos evaluados. En concreto, esto incluye interacciones de calidad entre proveedor y comprador, soporte técnico o soporte de cuentas. También puede incluir herramientas auxiliares, programas de soporte al cliente, disponibilidad de grupos de usuarios, acuerdos de nivel de servicio, etc.
Los factores de evaluación incluyen la gestión de las relaciones con los clientes, Gartner Peer Insights y las interacciones con los clientes de Gartner.

Operaciones: Este criterio aborda la capacidad de un proveedor para cumplir con sus objetivos y compromisos, incluida la calidad de la estructura organizativa, las habilidades, las experiencias, los programas, los sistemas y otros vehículos que permiten que la organización funcione de manera eficaz y eficiente. Los factores de evaluación incluyen los recursos dedicados al desarrollo de productos EPP, las certificaciones, la seguridad interna y la capacitación de los usuarios finales.
programas.

Tabla 1: Criterios de evaluación de la capacidad de ejecución

Criterios de evaluación	Ponderación
Producto o servicio	Alto
Viabilidad general	Medio
Ejecución de ventas/Precios	Medio
Capacidad de respuesta del mercado/historial	Alto
Ejecución de marketing	Sin calificación
Experiencia del cliente	Alto
Operaciones	Medio

Fuente: Gartner (septiembre de 2024)

Integridad de la visión

Los analistas de Gartner evalúan a los proveedores por su capacidad para articular declaraciones lógicas de manera convincente. relacionado con la dirección actual y futura del mercado, la innovación, las necesidades de los clientes y las fuerzas competitivas. También evaluamos qué tan bien estas afirmaciones corresponden a la visión de Gartner del mercado.

Comprensión del mercado: este criterio aborda la capacidad de un proveedor para comprender las necesidades del cliente y traducirlos en productos y servicios. Examina si un proveedor muestra una visión clara de sus Mercado: escucha y comprende las demandas de los clientes y puede dar forma o mejorar los cambios del mercado. con su visión añadida. Los factores de evaluación incluyen cómo los proveedores identifican el mercado de protección de endpoints tendencias y comprender a sus compradores y competidores.

Estrategia de ventas: Este criterio evalúa la capacidad de un proveedor para ofrecer una estrategia de venta sólida. utiliza las redes adecuadas, incluidas las ventas directas e indirectas, el marketing, el servicio y comunicación. También analiza socios que amplían el alcance y la profundidad del alcance del mercado, la experiencia,

Tecnologías, servicios y base de clientes. Los factores de evaluación incluyen el atractivo de las opciones de licencia y empaquetado de los productos, las estrategias de negociación, los logotipos para nuevos clientes proporcionados por el proveedor y las interacciones con los clientes finales y las tasas de consideración de Gartner.

Estrategia de oferta (producto): este criterio analiza la capacidad de un proveedor para ofrecer un enfoque de desarrollo y entrega de productos que enfatice la diferenciación en el mercado, la funcionalidad, la metodología y las características en función de los requisitos actuales y futuros. Los factores de evaluación incluyen la funcionalidad diferenciada del producto, la ejecución en relación con la hoja de ruta durante el año anterior y la hoja de ruta futura.

Estrategia vertical/industrial: este criterio evalúa la estrategia de un proveedor para destinar recursos (ventas, productos, desarrollo), habilidades y productos a satisfacer las necesidades específicas de segmentos de mercado individuales, incluidas las verticales. Los factores de evaluación incluyen el desempeño en industrias específicas y estrategias de expansión vertical.

Innovación: Este criterio se refiere a la capacidad de un proveedor para ofrecer recursos, experiencia o capital de manera directa, relacionada, complementaria y sinérgica, con fines de inversión, consolidación, defensivos o preventivos. Los factores de evaluación incluyen innovaciones técnicas y no técnicas diferenciadas realizadas en los últimos 12 meses e innovaciones anteriores de más de 12 meses.

Estrategia geográfica: Este criterio evalúa la estrategia de un proveedor para destinar recursos, habilidades y ofertas a satisfacer las necesidades específicas de geografías fuera de la geografía de origen, ya sea directamente o a través de socios, canales y subsidiarias, según corresponda a esa geografía y mercado. Los factores de evaluación incluyen el desempeño en los mercados internacionales, la localización de productos y las estrategias de expansión geográfica.

Tabla 2: Completitud de los criterios de evaluación de la visión

Criterios de evaluación	Ponderación
Comprensión del mercado	Alto
Estrategia de comercialización	Sin calificación
Estrategia de ventas	Medio
Estrategia de oferta (producto)	Alto

Criterios de evaluación	Ponderación
Modelo de negocio	Sin calificación
Estrategia vertical/industrial	Bajo
Innovación	Medio
Estrategia geográfica	Bajo

Fuente: Gartner (septiembre de 2024)

Descripciones de cuadrantes

Líderes

Los líderes demuestran un progreso equilibrado y consistente en relación con todos los criterios de Capacidad de ejecución e Integridad de la visión. Ofrecen capacidades de seguridad del espacio de trabajo amplias y estrechamente integradas, funcionalidad EDR profunda, paquetes de servicios entregados por el proveedor (como MDR) y capacidades de gestión comprobadas para clientes empresariales. Cada vez más, los líderes ofrecen plataformas XDR holísticas que permiten a los clientes consolidar o converger sus herramientas de seguridad y capacidades de gestión de incidentes.

Los líderes tienen un fuerte impulso en el mercado en términos de ventas y reconocimiento de marca. Sin embargo, un líder no es la opción predeterminada para todos los compradores. Los clientes no deben asumir que deben comprarle solo a un líder. Los líderes pueden ser menos capaces de reaccionar rápidamente cuando los visionarios desafían el status quo en el mercado.

Retadores

Los competidores tienen productos de protección de endpoints maduros que pueden abordar las necesidades de seguridad del mercado. También tienen fuertes ventas y visibilidad en el mercado, lo que se suma a una mejor capacidad de ejecución que la que tienen los actores de nicho. Sin embargo, los competidores suelen llegar tarde a la hora de introducir capacidades nuevas y emergentes, carecen de funcionalidad y personalización avanzadas, carecen de facilidad de uso del producto y carecen de una estrategia de productos y servicios estrechamente integrada. Los competidores pueden carecer de alineación con la dirección del mercado. Esto afecta sus posiciones sobre la Integridad de la Visión en comparación con los Líderes.

Los Challengers son opciones sólidas, eficientes y prácticas, especialmente para los clientes que han establecido relaciones estratégicas con ellos.

Visionarios

Los visionarios ofrecen capacidades de vanguardia que serán importantes en la próxima generación de soluciones, lo que brinda a los compradores acceso temprano a una mejor seguridad y gestión. Por ejemplo, los visionarios suelen tener algunas de las siguientes capacidades: detección y respuesta extendidas, detección y respuesta ante amenazas de identidad, capacidades de seguridad del espacio de trabajo, gestión de configuración de seguridad, envoltorios de servicios entregados por el proveedor, funciones avanzadas de EDR, seguridad de datos y capacidades de inteligencia artificial generativa (GenAI).

Los visionarios pueden influir en el curso de los avances tecnológicos en el mercado, pero es posible que aún no demuestren un historial de ejecución consistente, que carezcan de visibilidad en el mercado y, a menudo, de participación en el mercado. Los clientes eligen a los visionarios para tener acceso temprano a funciones innovadoras.

Jugadores de nicho

Los actores de nicho ofrecen productos sólidos pero rara vez lideran el mercado en términos de características y capacidades.

Algunos proveedores son actores especializados porque se centran en una región geográfica específica o en un segmento de mercado específico. Otros son actores especializados porque se destacan en un caso de uso específico, una industria o un conjunto de capacidades técnicas específicas. Los actores especializados pueden ser una buena opción para los clientes existentes, los clientes en el segmento de mercado objetivo del proveedor, las organizaciones reacias al cambio en las regiones respaldadas o las organizaciones que buscan ampliar su EPP existente para un enfoque de defensa en profundidad.

Contexto

Los EPP se centran en proteger los puntos finales de los usuarios (computadoras portátiles, estaciones de trabajo, dispositivos móviles) mediante una combinación de capacidades de prevención, protección, detección y respuesta entregadas a través de un único agente. Cada vez más, los proveedores ofrecen EPP como parte de plataformas de operaciones de seguridad, como XDR y gestión de eventos e información de seguridad (SIEM), lo que habilita el camino para modernizar las operaciones de seguridad. Al mismo tiempo, los proveedores agrupan e integran cada vez más los EPP como parte de sus carteras más amplias de productos de seguridad del espacio de trabajo centrados en proteger el trabajo híbrido moderno.

Según las encuestas a proveedores y las consultas de clientes del Cuadrante Mágico de Gartner, el crecimiento en la adopción de soluciones EPP entregadas en la nube y capacidades EDR se ha estancado, con solo un aumento moderado en la adopción en comparación con la investigación del año anterior. Sin embargo, el interés en capacidades XDR e ITDR estrechamente integradas está aumentando, con una tasa de adopción estimada del 14% y el 9% (a mayo de 2024) entre los compradores de EPP, respectivamente. A pesar de la ola de anuncios y la disponibilidad general de asistentes GenAI y capacidades de resumen de incidentes, la mayoría de las organizaciones siguen siendo cautelosas, con un interés limitado por parte de los clientes de EPP de Gartner.

Los clientes de EPP contemplan cada vez más los beneficios y desventajas de adquirir múltiples productos y servicios de seguridad del mismo proveedor. La gestión de vulnerabilidades y exposición, la detección y respuesta ante amenazas de identidad, la seguridad del correo electrónico, la protección de cargas de trabajo en la nube, la detección y respuesta extendidas y la detección y respuesta administradas son cada vez más parte de la decisión de compra. Por lo tanto, este Cuadrante Mágico va más allá de evaluar la capacidad de un proveedor para ofrecer productos EPP básicos para ayudar a los compradores que buscan lograr un enfoque holístico para la seguridad del espacio de trabajo y la modernización de las operaciones de seguridad.

Descripción general del mercado

Evolución del producto

A pesar de la madurez del mercado de EPP, no existen soluciones perfectas. El año 2024 demuestra que incluso los proveedores de soluciones más sofisticados están sujetos a eventos impredecibles. Ningún proveedor es completamente inmune. Por lo tanto, las organizaciones deben prepararse para las posibilidades de una disrupción importante centrándose en la resiliencia como con cualquier otro riesgo de terceros.

Desde el último informe, la mayoría de los proveedores solo han realizado cambios incrementales en sus productos EPP. La mayoría de los proveedores han integrado completamente las capacidades de prevención, protección, detección y respuesta en una solución EPP unificada configurada y operada desde una única consola y habilitada con un único agente de punto final unificado. Sin embargo, los compradores deben tener cuidado con los proveedores que dependen de varias consolas para diversas funciones o que requieren múltiples aplicaciones de punto final, incluso si están vinculadas entre sí a través de un inicio de sesión único (SSO) o se implementan utilizando mecanismos de implementación de agente centralizados.

En 2024, los proveedores realizaron mejoras incrementales en la experiencia del usuario y las capacidades de administración, mejorando la facilidad general de uso del producto. La mayoría de los proveedores lanzaron capacidades GenAI integradas o asistentes de IA que tienen como objetivo mejorar la explicabilidad de los incidentes, brindar orientación sobre la incorporación y la configuración y respaldar a los equipos de seguridad con ingeniería de detección, consultas de búsqueda de amenazas y creación de scripts de respuesta. La mayoría de los proveedores se abstienen de afirmar que automatizan por completo la gestión de alertas, la configuración o las políticas de seguridad. A pesar del progreso de los proveedores con la IA generativa, la adopción de las capacidades GenAI entre los clientes de EPP sigue siendo baja.

Otras áreas de interés para los proveedores de EPP incluyeron capacidades mejoradas de gestión de activos, vulnerabilidades y exposición. Varios proveedores están buscando mejoras para la paridad de funciones y la calidad del producto de sistemas operativos que no son Windows, como macOS y Linux. Además, hemos visto un enfoque renovado de los proveedores de EPP en la investigación forense de endpoints, la prevención de pérdida de datos de endpoints y la gestión optimizada de la configuración de seguridad.

Integración empresarial

La integración empresarial continúa en áreas como XDR y seguridad del espacio de trabajo. Varios proveedores lanzaron capacidades de gestión de incidentes unificadas como parte de sus soluciones XDR para ayudar a correlacionar alertas de controles de seguridad nativos y de terceros en una única vista de incidentes. La mayoría de los proveedores también han fusionado por completo sus ofertas de EPP y XDR en una única consola UX. Sin embargo, los compradores deben tener cuidado con aquellos que aún ofrecen EPP y XDR como dos productos separados con consolas, configuraciones y vistas de alertas distintas, incluso si los productos están integrados a través de SSO y API. Las integraciones de seguridad de correo electrónico e ITDR en XDR son cada vez más críticas, ya que el uso de credenciales robadas y el phishing están involucrados en la mayoría de las infracciones.

El trabajo híbrido impulsa la necesidad de estrategias integrales de seguridad en el espacio de trabajo que integren la seguridad en el acceso a dispositivos, identidad, correo electrónico, datos y aplicaciones en soluciones modulares y cohesivas.

Los proveedores de seguridad de amplio portafolio continúan con sus esfuerzos de unificación para unir EPP con agentes SSE y DLP. Algunos ejemplos de integraciones entre herramientas EPP y SSE incluyen la evaluación de la postura de los puntos finales para el acceso condicional, paneles de administración comunes con elementos de políticas reutilizables, correlación de alertas de seguridad, creación de lógica de detección personalizada y aplicación dinámica de políticas de acceso seguro. La seguridad del correo electrónico se beneficia de la integración de datos de identidad de los usuarios que ayudan a medir el riesgo de los usuarios, identificar signos de apropiación de cuentas e iniciar acciones de mitigación. Además, varios proveedores ahora ofrecen un paquete de productos de seguridad bajo un único SKU diseñado para proteger el espacio de trabajo híbrido.

Las organizaciones pequeñas y medianas a menudo prefieren este tipo de ofertas de seguridad para espacios de trabajo de un solo proveedor.

Diferenciación de proveedores

Los proveedores de este mercado muestran distintos niveles de madurez en cuanto a la amplitud y profundidad de sus funciones de prevención y protección, capacidades de detección y respuesta, funciones forenses, seguridad de datos, gestión de configuración de seguridad y compatibilidad con sistemas operativos. Si bien todos los proveedores intentan optimizar sus agentes de punto final para que tengan un impacto mínimo en el rendimiento del sistema, existe una diferencia significativa en el consumo de recursos de las distintas herramientas. Además, la calidad y la profundidad de la integración del ecosistema y la compatibilidad con varios escenarios de implementación local difieren.

Capacidades como el análisis del comportamiento, la gestión del firewall del host y el control de dispositivos son comunes entre la mayoría de los proveedores y, por lo tanto, la mayoría de los clientes de Gartner no las consideran diferenciadoras.
Cada vez hay más productos que incorporan funciones integradas de gestión de vulnerabilidades, exposición y parches. Algunos proveedores ofrecen sus productos a equipos de seguridad experimentados y con personal completo, mientras que otros ofrecen soluciones más fáciles de usar con menos opciones de personalización y una orientación más contextual.
La mayoría de los proveedores ofrecen paquetes de servicios entregados por socios y proveedores, como MDR, para ayudar a los usuarios finales en el monitoreo, la clasificación, la investigación y la respuesta las 24 horas del día, los 7 días de la semana.

Factores impulsores del mercado

Las tendencias generales del mercado que impulsan la adopción de ofertas de EPP incluyen:

- Consolidación: las organizaciones necesitan gestionar la complejidad y aumentar la eficacia de su limitado personal de seguridad. Las pilas de seguridad de infraestructura complejas generan complejidad en la gestión de la configuración de seguridad y brechas en el control de seguridad que pueden exponer a las organizaciones a amenazas.
  Las plataformas de seguridad, que ofrecen un conjunto modular de capacidades de productos de seguridad integrados, están cada vez más disponibles para satisfacer estas necesidades. Consulte Innovation Insight para plataformas de seguridad y simplificar la ciberseguridad con un marco de consolidación de plataformas.

- Trabajo híbrido: las herramientas de protección de endpoints solo abordan parte de los problemas relacionados con la seguridad de los trabajadores híbridos, y se centran en proteger los endpoints administrados de los ataques de malware. El robo de identidad, el phishing y la exfiltración de datos son riesgos de seguridad del espacio de trabajo que requieren mayor atención. Para abordar estos problemas, las organizaciones necesitan una estrategia de seguridad integral del espacio de trabajo que coloque al trabajador en el centro de la protección e integre la seguridad en el acceso a dispositivos, correo electrónico, identidad, datos y aplicaciones.

Controles. Consulte Cómo proteger el trabajo híbrido: adoptar la estrategia de seguridad adecuada para el espacio de trabajo y Hype Cycle para la seguridad de endpoints y espacios de trabajo, 2024.

- Operaciones de seguridad: la disponibilidad y la experiencia de los equipos de seguridad, junto con la necesidad de una cobertura las 24 horas del día, los 7 días de la semana, siguen siendo las barreras más importantes para el éxito de las operaciones de seguridad. Las tecnologías modernas de gestión proactiva de la exposición y gestión reactiva de incidentes, junto con la inversión en personal y capacitación, permiten que más organizaciones modernicen sus operaciones de seguridad. Para las organizaciones menos maduras, los servicios de MDR brindan a los clientes funciones de centro de operaciones de seguridad (SOC) modernas, listas para usar y dirigidas por humanos y entregadas de forma remota. Consulte la Guía de mercado para detección y respuesta administradas.

Evidencia

El equipo del Cuadrante Mágico de Gartner utilizó datos de las siguientes fuentes:

- Más de 2000 consultas de clientes de Gartner desde enero de 2024.
- Más de 4000 reseñas de Gartner Peer Insights en gartner.com.
- Respuestas de los proveedores a una encuesta del Cuadrante Mágico, con más de 230 preguntas sobre productos, servicios y mejoras hasta el segundo trimestre de 2024, así como demostraciones de productos en vivo de 60 minutos por parte de cada proveedor.

Definiciones de criterios de evaluación

Capacidad de ejecución

Producto/servicio: bienes y servicios básicos que ofrece el proveedor para el mercado definido. Esto incluye las capacidades actuales del producto/servicio, la calidad, los conjuntos de características, las habilidades, etc., ya sea que se ofrezcan de forma nativa o a través de acuerdos/asociaciones con OEM, tal como se define en la definición del mercado y se detalla en los subcriterios.

Viabilidad general: la viabilidad incluye una evaluación de la salud financiera general de la organización, el éxito financiero y práctico de la unidad de negocios y la probabilidad de que la unidad de negocios individual continúe invirtiendo en el producto, continúe ofreciendo el producto y avance en el estado del arte dentro de la cartera de productos de la organización.

Ejecución de ventas/fijación de precios: las capacidades del proveedor en todas las actividades de preventa y la estructura que las respalda. Esto incluye la gestión de acuerdos, la fijación de precios y la negociación, el apoyo de preventa y la eficacia general del canal de ventas.

Capacidad de respuesta al mercado/historial: capacidad de respuesta, cambio de dirección, flexibilidad y éxito competitivo a medida que surgen oportunidades, actúan los competidores, evolucionan las necesidades de los clientes y cambia la dinámica del mercado. Este criterio también tiene en cuenta el historial de capacidad de respuesta del proveedor.

Ejecución de marketing: La claridad, calidad, creatividad y eficacia de los programas diseñados para transmitir el mensaje de la organización para influir en el mercado, promover la marca y el negocio, aumentar

Conciencia de los productos y establecer una identificación positiva con el producto/marca y la organización en la mente de los compradores. Esta "participación mental" puede ser impulsada por una combinación de publicidad, iniciativas promocionales, liderazgo intelectual, boca a boca y actividades de ventas.

Experiencia del cliente: relaciones, productos y servicios/programas que permiten a los clientes tener éxito con los productos evaluados. En concreto, esto incluye las formas en que los clientes reciben asistencia técnica o asistencia de cuentas. También puede incluir herramientas auxiliares, programas de asistencia al cliente (y su calidad), disponibilidad de grupos de usuarios, acuerdos de nivel de servicio, etc.

Operaciones: La capacidad de la organización para cumplir sus objetivos y compromisos. Los factores incluyen la calidad de la estructura organizacional, incluidas las habilidades, experiencias, programas, sistemas y otros vehículos que permiten que la organización funcione de manera eficaz y eficiente de manera continua.

Integridad de la visión

Comprensión del mercado: Capacidad del proveedor para comprender los deseos y necesidades de los compradores y traducirlos en productos y servicios. Los proveedores que muestran el mayor grado de visión escuchan y comprenden los deseos y necesidades de los compradores, y pueden moldearlos o mejorarlos con su visión adicional.

Estrategia de marketing: Un conjunto claro y diferenciado de mensajes comunicados consistentemente en toda la organización y externalizados a través del sitio web, la publicidad, los programas de clientes y las declaraciones de posicionamiento.

Estrategia de ventas: La estrategia para vender productos que utiliza la red adecuada de afiliados de ventas directas e indirectas, marketing, servicios y comunicación que amplían el alcance y la profundidad del alcance del mercado, las habilidades, la experiencia, las tecnologías, los servicios y la base de clientes.

Estrategia de oferta (de producto): El enfoque del proveedor hacia el desarrollo y la entrega de productos que enfatiza la diferenciación, la funcionalidad, la metodología y los conjuntos de características a medida que se adaptan a los requisitos actuales y futuros.

Modelo de negocio: La solidez y lógica de la propuesta comercial subyacente del proveedor.

Estrategia vertical/industrial: La estrategia del proveedor para dirigir los recursos, las habilidades y las ofertas para satisfacer las necesidades específicas de segmentos de mercado individuales, incluidos los mercados verticales.

Innovación: Disposiciones directas, relacionadas, complementarias y sinérgicas de recursos, experiencia o capital con fines de inversión, consolidación, defensivos o preventivos.

Estrategia geográfica: La estrategia del proveedor para dirigir recursos, habilidades y ofertas para satisfacer las necesidades específicas de geografías fuera de la geografía "de origen" o nativa, ya sea directamente o a través de socios, canales y subsidiarias según sea apropiado para esa geografía y mercado.