CROWDSTRIKE

Documento técnico

Guía para compradores de protección de endpoints

Capacidades esenciales de la protección moderna de endpoints

Índice

Proteger los endpoints es uno de los principales retos de seguridad en los entornos de trabajo modernos. Pese a ello, las organizaciones han tratado las soluciones para endpoints principalmente como herramientas básicas para la gestión de dispositivos, pasando por alto el hecho de que los endpoints son uno de los principales objetivos de los ciberdelincuentes. El auge del trabajo remoto e híbrido ha incrementado todavía más el riesgo, ya que los adversarios han multiplicado sus esfuerzos para explotar cualquier disparidad entre control y seguridad. La proliferación de nuevos puntos de acceso, a menudo inseguros, a las redes y a los datos, junto con el rápido despliegue de nueva infraestructura, ha proporcionado a los ciberdelincuentes una superficie de ataque mayor que les ha permitido ampliar tanto el volumen como el alcance de sus actividades.

Según IBM, "varios estudios determinan que el 90 % de los ciberataques realizados con éxito se originan en dispositivos de endpoint".[1]Los adversarios buscan mantener su presencia para lanzar ataques basados en la identidad, por eso se pasan a la infraestructura en la nube o explotan vulnerabilidades, entre otras cosas.

El aumento del ritmo y de la sofisticación de las amenazas ha obligado a los equipos de seguridad y de TI a evaluar sus capacidades actuales de seguridad de endpoints. Las soluciones de seguridad con métodos basados en firmas y agentes pesados, los elevados gastos de mantenimiento y la experiencia de usuario inconexa son ineficaces e ineficientes, ralentizan a los equipos de seguridad y dejan a las empresas expuestas a recibir ataques.

En respuesta a estos retos, CrowdStrike ha elaborado esta guía para ayudarte a proteger eficazmente tu organización de las amenazas modernas. Su objetivo es definir los componentes y los elementos necesarios para adoptar una estrategia de protección de endpoints moderna.

Necesidades actuales de protección de endpoints

Las técnicas que se utilizaban en el pasado para detectar y bloquear amenazas en los endpoints han demostrado ser ineficaces frente a las tácticas de ataque que se emplean hoy en día. Ya no es posible prevenir las brechas mediante la supervisión y el análisis de archivos para detectar entidades maliciosas conocidas, sobre todo si se hace sin contexto.

Los ciberdelincuentes más sofisticados buscan activamente brechas en los entornos aislados, por lo que se necesita algo más que una combinación de diferentes productos de seguridad. Para que una solución de protección de endpoints sea verdaderamente eficaz, debe estar cuidadosamente diseñada para mejorar los flujos de trabajo de los analistas, al tiempo que prioriza la resiliencia frente a las amenazas durante todo el ciclo de vida del ataque.

Protección de endpoints moderna con inteligencia artificial

Para adelantarte a los adversarios actuales, necesitas una protección de endpoints moderna. El tiempo medio de propagación de una intrusión ciberdelictiva ha pasado de 84 minutos en 2022 a 62 minutos en 2023, según el Informe Global sobre Amenazas 2024 de CrowdStrike. La inteligencia artificial (IA) se erige como un elemento fundamental para distinguir la protección de endpoints moderna de las alternativas tradicionales. Con la IA, las soluciones de protección de endpoints aprovechan modelos entrenados con miles de billones de puntos de datos diarios para predecir y detener las amenazas de forma eficaz. Esta capacidad es crucial para defenderse de los ataques sin archivos. El mismo informe de CrowdStrike indica que el 75 % de los ataques observados no contenía malware en 2023, un aumento considerable desde el 51 % en 2020.

[1]IBM, "¿Qué es la seguridad de puntos finales?": https://www.ibm.com/es-es/topics/endpoint-security

Adopción de un enfoque nativo de la nube

Para aprovechar todos los datos que necesita una solución de protección de endpoints basada en IA, es necesario contar con una plataforma escalable y nativa de la nube.

Con una estrategia nativa de la nube es posible acumular, compartir y operacionalizar fácilmente esta información para conseguir el nivel de anticipación, prevención, detección, visibilidad y capacidad de respuesta necesario para vencer una y otra vez a un ciberdelincuente tenaz.

El potencial de una protección unificada

Con el objetivo de seguir el ritmo frenético de los adversarios, muchas organizaciones han optado por ampliar su conjunto de herramientas de seguridad para monitorizar y gestionar toda la superficie de ataque. Lamentablemente, la incorporación de más herramientas aumenta el número de problemas, ya que las empresas que desean reducir las brechas de seguridad podrían experimentar resultados de seguridad deficientes y necesitarían recurrir a más recursos para gestionar las herramientas. De media, estas cuentan con 50 herramientas de seguridad en sus entornos, aunque algunas superan las 140[2] y, de acuerdo con el Informe Estado de seguridad de las aplicaciones de CrowdStrike 2024, el 70 % tiene dificultades para hacer frente al volumen de alertas. Además, los adversarios aprovechan las deficiencias de las herramientas, explotan las vulnerabilidades y buscan formas de pasar desapercibidos en entornos fragmentados.

Al buscar una solución de seguridad de endpoints moderna, es fundamental que elijas una que reúna todas las funciones y elementos principales. Las funciones unificadas y estrechamente integradas proporcionan una visibilidad completa sobre los ataques, de forma que los equipos puedan comprender las amenazas rápidamente y actuar en consecuencia. Estos pueden intervenir en los problemas, investigarlos y solucionarlos más rápido al contar con una fuente información unificada y completa. El agente también debería estar unificado, para que las organizaciones puedan ampliar sus medidas de seguridad con el paso del tiempo sin tener que añadir más agentes. Así, los equipos de seguridad pueden poner en marcha nuevas protecciones en tan solo segundos a través del agente desplegado el primer día. A medida que las organizaciones intensifican sus esfuerzos por combatir ataques cada vez más sofisticados, la capacidad de sacar información a la luz es primordial. Con una solución de protección unificada podrás consultar enormes cantidades de datos en toda la posición de seguridad, para después extraer la información necesaria y tomar mejores decisiones más rápido.

Ten en cuenta todas estas necesidades a la hora de seleccionar una solución de seguridad. Sin perder de vista estas consideraciones, vamos a analizar los cinco elementos que constituyen la protección de endpoints moderna, y mencionaremos las capacidades clave que debería poseer la solución y las funciones necesarias para que estas capacidades sean efectivas:

- Prevención
- Detección y respuesta
- Detección y respuesta ante amenazas de identidad (ITDR)
- Inteligencia sobre amenazas
- Threat Hunting gestionado

[2] IDC, How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans? Número del documento: #US51973524, marzo de 2024: https://www.idc.com/getdoc.jsp?containerId=US51973524

Los cinco elementos de la protección de endpoints moderna

Elemento 1: prevención

Protección frente a malware y ataques sin archivos con antivirus de nueva generación (NGAV)

Hay razones de peso que explican por qué los productos tradicionales de protección de endpoints orientados al malware sencillamente no proporcionan un nivel de protección adecuado frente a las amenazas y los adversarios actuales.

La protección centrada en malware no aborda las tácticas cada vez más sofisticadas que emplean los adversarios modernos, especialmente en el ámbito de las técnicas de ataques sin archivos y sin malware. Según el Informe Global sobre Amenazas 2024 de CrowdStrike, el 75 % de los ataques de 2023 se produjo sin malware, lo que refleja una continua tendencia al alza.

Una solución eficaz de protección de endpoints debe solventar este problema y trascender la mera identificación y resolución del malware conocido. Debería:

- Proteger frente a malware conocido y desconocido mediante tecnologías como el aprendizaje automático, que no requieren actualizaciones diarias y son capaces de generar defensas frente a ataques nunca vistos.
- Mirar más allá del malware y sacarle el máximo partido a los análisis de comportamiento para buscar automáticamente indicios de un ataque y bloquearlos mientras suceden.
- Salvaguardar los endpoints frente a todo tipo de amenazas, desde malware conocido y desconocido hasta ataques sin archivos y sin malware, combinando todas las tecnologías necesarias para obtener una protección óptima.

Características principales	Características necesarias
Detección de amenazas avanzadas y desconocidas, incluidos los ataques sin archivos	• Protección basada en inteligencia artificial y aprendizaje automático para evitar el malware, el adware y los programas potencialmente no deseados (PUP), tanto conocidos como desconocidos • Análisis avanzado del comportamiento con indicadores de ataque (IOA). • Escaneo de memoria de alto rendimiento. • Mitigación de exploits. • Análisis de malware automático (p. ej., entornos aislados)
Velocidad para adelantarse a los adversarios	• Tecnología sin firmas que elimine la necesidad de actualizaciones que requieren mucho tiempo. • Un único agente ligero y unificado para un despliegue rápido y una protección instantánea.
Inteligencia sobre amenazas integrada	• Comprensión del alcance y el impacto de las amenazas encontradas en el entorno. • Visibilidad de las amenazas a nivel de adversario. • Evaluación de la gravedad de las amenazas para su priorización. • Análisis de amenazas con pasos de recuperación para resolver incidentes.

Elemento 2: detección y respuesta

Descubre amenazas más rápido con detección y respuesta para endpoints (EDR)

Si bien NGAV constituye una primera línea de defensa importante para una organización, no es infalible. Ninguna solución de este tipo, por muy avanzada que sea, es capaz de prevenir por completo todas las amenazas, especialmente si son ataques nunca vistos hasta ahora o que utilizan credenciales robadas o herramientas fiables.

El siguiente nivel de protección es EDR, con detección y respuesta extendidas (XDR) nativas. Las versiones anteriores de las soluciones de detección de amenazas se centran en funcionalidades básicas para monitorizar los endpoints. Con frecuencia, estas herramientas tradicionales aumentan la carga de trabajo de los analistas, ya que los sobrecargan con telemetría y alertas sin enriquecer que contienen muy poca información procesable. Cuanto más compleja es una herramienta de seguridad, mayores son las probabilidades de que se cree un vacío de seguridad y de que pase inadvertido hasta que se produzca una brecha.

La EDR moderna aborda estos problemas. Proporciona visibilidad a nivel de empresa al unificar y optimizar los análisis de seguridad, la investigación y la corrección en una sola consola fácil de utilizar. Además, la XDR nativa integrada amplía la correlación de datos de seguridad, análisis y flujos de trabajo más allá del endpoint para incluir el resto de capacidades nativas de la plataforma, como la prevención de amenazas de identidad. Esto mejora la visibilidad en torno a las amenazas de seguridad avanzadas y elusivas, y permite ofrecer una respuesta más precisa y fluida. La EDR con XDR nativa integrada mejora drásticamente la visibilidad de las amenazas, agiliza las operaciones de seguridad y alivia la carga constante del personal de seguridad.

Para superar a los ciberdelincuentes actuales, es necesario que las organizaciones empleen la EDR para optimizar la detección, la investigación y la búsqueda de amenazas en toda la empresa, así como su capacidad de respuesta ante estas, y la XDR nativa para ampliar la visibilidad y el control en las superficies de ataque clave. Al evaluar las diferentes opciones, busca una solución EDR que cuente con capacidades de XDR, para ofrecer la mayor cobertura en toda la infraestructura de endpoints y en el resto de ubicaciones.

Características principales	Características necesarias
Visibilidad completa del ataque	· Análisis de toda la empresa. · Correlación de datos entre dominios más allá del endpoint. · Visualización de alertas intuitiva y exhaustiva: muestra el historial de ataques completo en un árbol de procesos con funciones de desglose y tabla dinámica. · Correspondencia de las etapas del ataque con un marco de ataque estándar del sector, como MITRE ATT&CK®.
Detección de los ataques que eluden la prevención	· Captura de eventos sin procesar, incluso cuando no están asociados con alertas ni detecciones. · Funcionamiento en modo kernel para ofrecer una visibilidad completa y eliminar ángulos ciegos · Repositorio centralizado de datos para permitir una detección avanzada · Detección automática basada en análisis de comportamiento, como IOA
Clasificación de incidentes y análisis de investigación	· Clasificación automatizada con priorización inteligente de la actividad maliciosa y de los ciberdelincuentes. · Correlación de eventos independientes en incidentes. · Recomendaciones inteligentes de investigación basadas en IA. · Periodo flexible de retención de datos de eventos · Funciones de búsqueda en tiempo real e histórica totalmente personalizables · Contexto en distintos dominios. · Acceso remoto a endpoints e interacción con estos en tiempo real. · Posibilidad de que los analistas colaboren y trabajen juntos en incidentes en tiempo real desde cualquier ubicación. · Correlación del contexto para identificar comportamientos sospechosos y posibles endpoints en riesgo.
Acelerar la corrección y la respuesta	· Capacidad para contener endpoints en la red · Capacidad para poner archivos en cuarentena · Capacidad para ejecutar comandos en endpoints sospechosos de forma remota y en tiempo real · Capacidad para realizar acciones de respuesta para otras capacidades nativas en todos los dominios. · API para integrarse con los sistemas actuales de organización/gestión de casos del cliente. · Notificaciones de alerta personalizables

Elemento 3: detección y respuesta ante amenazas de identidad

Detén los ataques modernos basados en la identidad en tiempo real

Si tu protección de endpoints no incluye seguridad de la identidad, estás dejando la puerta abierta para los adversarios oportunistas. Con el aumento de los ataques sin malware, los adversarios buscan deficiencias en la forma de proteger los endpoints y de gestionar las identidades. En muchos casos, los adversarios no están forzando la entrada, sino iniciando sesión. Una vez que aprenden a robar las identidades, y las credenciales de acceso privilegiado que las acompañan, pueden acceder rápidamente sin ser detectados.

Las organizaciones emplean soluciones de identidad para conocer el estado de la seguridad de la infraestructura de identidades, como Microsoft Active Directory y Entra ID. Esto les ayuda a detener las amenazas basadas en identidad antes de que se produzcan. Es fundamental identificar las contraseñas en riesgo, las cuentas con exceso de privilegios y cualquier otra brecha de seguridad que pueda dejar a la organización expuesta. Al unificar la protección de endpoints con la seguridad de la identidad, obtendrás también información sobre las posibles rutas de ataque que pueden seguir los adversarios en toda la red.

Las soluciones ITDR ayudan a las organizaciones a detectar y responder a amenazas basadas en identidad en tiempo real. Entre estas se incluyen ataques de ransomware, movimiento lateral, uso ilícito de cuentas de servicio, Pass-the-Hash (PtH) o Golden Ticket. A la hora de evaluar las soluciones ITDR, es fundamental que sean capaces de detener el movimiento lateral, incluido el movimiento lateral híbrido desde entornos locales a la nube, y desde dispositivos gestionados a dispositivos no gestionados. Puedes crear directivas que se correspondan con las rutas de ataque que ya has identificado, así como aprovechar las tácticas, las técnicas y los procedimientos (TTP) que ya conoces de los adversarios.

Si bien es fundamental detener a los ciberdelincuentes con protección de identidades en tiempo real, las organizaciones también deben garantizar la productividad empresarial. Por eso, es necesario que la solución ITDR incluya el acceso condicional basado en riesgos a través de la autenticación multifactor (MFA). Lo ideal es que con la solución puedas establecer bases de referencia del comportamiento normal de los usuarios para identificar rápidamente las anomalías cuando los adversarios más sofisticados se muevan por los endpoints y las identidades. Después, puedes implementar la autenticación MFA para aumentar la seguridad sin interrumpir a los usuarios legítimos.

Características principales	Características necesarias
Reducción de la superficie de ataque del almacén de identidades.	· Garantiza la visibilidad en la nube (Microsoft Entra ID u Okta), en el Microsoft Active Directory local y en los almacenes de identidades híbridos. · Clasifica automáticamente todas las identidades (es decir, cuentas humanas y de servicio). · Obtén información sobre el estado del almacén de identidades, incluidas las cuentas potencialmente comprometidas. · Identifica las posibles rutas de ataques basados en identidades que se puedan explotar.
Detección y prevención de amenazas basadas en identidad	· Detecta y responde a las amenazas basadas en identidad en toda la infraestructura. · Crea directivas que correspondan con las rutas de ataque y los TTP conocidos de los adversarios. · Aborda las vulnerabilidades inherentes de la nube y de los almacenes de identidades de Active Directory. · Garantiza la inclusión de ITDR en el Threat Hunting gestionado.
Habilita el acceso condicional	· Habilita la autenticación MFA basada en riesgo. · Amplía la protección MFA a las herramientas y aplicaciones tradicionales. · Resume las puntuaciones de riesgo para establecer una postura de riesgo de referencia.

Elemento 4: inteligencia sobre amenazas

Descubre cómo y por qué atacan los adversarios para adelantarte a ellos

Si la protección del endpoint no incluye inteligencia sobre amenazas, tanto la tecnología de protección como los profesionales de seguridad tendrán problemas para mantenerse al día con las últimas amenazas, así como para protegerse de ellas de forma proactiva.

Gracias a la inteligencia sobre amenazas ha mejorado la capacidad de detección de NGAV y EDR/XDR, puesto que no solo se muestra lo que ha sucedido en el endpoint, sino que también expone "el quién, el por qué y el cómo" de un ataque. Conocer la amenaza a este nivel es fundamental para adelantarse a futuros ataques y aumentar el coste para el adversario. Además, la inteligencia sobre amenazas proporciona la información que necesitan los equipos de seguridad para comprender y resolver incidentes de forma más rápida, así como responder ante ellos, lo que acelera las investigaciones y la corrección.

A la hora de evaluar la protección del endpoint, es fundamental ir más allá de la infraestructura de seguridad. Es fundamental que la solución completa cuente con inteligencia sobre amenazas procesable. Los clientes deberían asegurarse de que la inteligencia se integra sin problemas en la solución de protección de endpoints y de que es posible automatizar su consumo.

Características principales	Características necesarias
Integración de endpoints ampliada	• Inteligencia sobre amenazas integrada en la solución EDR/XDR para evitar despliegues y gestiones adicionales. • Reenvío automático de todos los archivos en cuarentena, desde el endpoint hasta la inteligencia sobre amenazas, para realizar una investigación inmediata.
Automatización y simplificación de la investigación de incidentes	• Análisis del malware en entorno aislado y búsqueda de malware. • Priorización de la aplicación de parches en los sistemas críticos. • Capacidad de navegar por toda plataforma de seguridad para ver el contexto del ataque.
Uso compartido de IOC para la organización de seguridad	• Indicadores de compromiso e inteligencia personalizados generados automáticamente en cuestión de minutos sobre amenazas relevantes y exclusivas del entorno. • IOC de terceros absorbidos automáticamente
Identificación de adversarios	• Identificación de adversarios que se centran en atacar tu negocio, región o sector. • Datos de intención y de capacidad del adversario para predecir futuros ataques.

Elemento 5: Threat Hunting gestionado

Supera a tus adversarios con detección experta ininterrumpida

Los procesos de Threat Hunting proactivos, llevados a cabo por expertos humanos en seguridad con la ayuda de la IA, son imprescindibles para cualquier organización que desee lograr o mejorar la detección de amenazas y la respuesta a incidentes en tiempo real.

El Threat Hunting desempeña un papel crucial en la detección temprana de ataques y adversarios. En lugar de utilizar defensas predefinidas y reactivas, las investigaciones realizadas por humanos buscan activamente actividades sospechosas y evitan la dependencia pasiva de soluciones autónomas para detectar y enviar alertas automáticamente. Este enfoque permite a las organizaciones identificar antes las actividades maliciosas y poner fin a los ataques antes de que se produzcan daños irreparables.

Aunque el Threat Hunting es fundamental, sus resultados dependen de la inteligencia sobre amenazas en la que se basa. Este proceso emplea la inteligencia recopilada del entorno de una organización para identificar nuevos ataques, el uso inadecuado de herramientas de acceso remoto, las credenciales comprometidas o las amenazas internas, entre otros. A la hora de evaluar una solución de Threat Hunting, asegúrate de que se basa en inteligencia y de que puede aplicarse tanto en los endpoints como en la protección de identidades.

No obstante, debido a la falta de recursos y a la escasez de experiencia en seguridad, la mayoría de empresas no pueden poner en marcha un proceso de Threat Hunting proactivo. De acuerdo con el estudio ISC2 Cybersecurity Workforce Study de 2023, se necesitarían casi 4 millones más de expertos en ciberseguridad para proteger los recursos de forma eficaz.[3]

Faltos de personal suficiente, los equipos internos no pueden vigilar día y noche la actividad del adversario y, con frecuencia, no disponen de la capacidad necesaria para responder de forma eficiente a los ataques altamente sofisticados. Como resultado, las investigaciones se alargan y se gestionan menos alertas a su debido tiempo, lo que, en última instancia, incrementa el tiempo de permanencia de los ciberdelincuentes y el riesgo de que logren cumplir sus objetivos.

Este problema se resuelve con un proceso de Threat Hunting gestionado y un equipo de profesionales de élite. Este equipo no solo identifica las actividades maliciosas que hayan pasado por alto los sistemas de seguridad automáticos, sino que también realiza análisis detallados y proporciona a los clientes pautas de respuesta. Al considerar una solución de seguridad de endpoints moderna, es crucial elegir una que sea compatible con el Threat Hunting gestionado.

Características principales	Características necesarias
Expertos humanos 24/7	· Equipo de expertos en Threat Hunting que ofrece servicios de detección de amenazas de forma ininterrumpida. · Asistencia durante incidentes y orientación sobre los siguientes pasos, como posibles sugerencias de mitigación. · Capacidad para encontrar nuevas amenazas que ningún otro sistema ha detectado. · Acceso inmediato a expertos en inteligencia sobre amenazas para agilizar el análisis · Integración automática y nativa con inteligencia sobre amenazas para actuar con la máxima eficacia · Integración con la seguridad de endpoints.
Visibilidad de las alertas perdidas	· Capacidad para identificar las amenazas más urgentes en el entorno, tanto en endpoints como en identidades. · Comunicación de bucle cerrado mejorada para garantizar que se tienen en cuenta las alertas importantes.

[3] ISC2 Cybersecurity Workforce Study 2023, "How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce", https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

La diferencia de CrowdStrike

Ahora que ya conoces las capacidades esenciales que necesita tu solución, veamos el enfoque de CrowdStrike sobre la seguridad moderna de endpoints.

Tecnologías avanzadas

Desde su fundación en 2011, CrowdStrike ha sido pionera en el uso de la IA y el aprendizaje automático en materia de ciberseguridad para resolver los retos más apremiantes de los clientes. La solución de protección de endpoints de CrowdStrike incorpora tecnologías innovadoras, como la IA y el aprendizaje automático, la protección basada en el comportamiento y la mitigación de exploits, para poner fin a las TTP en continua evolución que utilizan los adversarios para atacar a las organizaciones. Estos métodos incluyen malware básico, malware de día cero e incluso ataques sin malware avanzados.

Mediante el uso de la IA y el aprendizaje automático, CrowdStrike evita la dependencia de métodos basados en firma o IOC, que pueden ocasionar "errores silenciosos" y permitir las brechas de datos. En su lugar, CrowdStrike adopta enfoques de comportamiento que buscan indicadores de ataque de forma activa, por lo que la empresa recibirá alertas de cualquier actividad sospechosa antes de que se produzca una situación de riesgo. Los indicadores de ataque (IOA) basados en IA son la evolución más reciente de los IOA de CrowdStrike, pioneros en el sector, que amplían la protección al combinar la experiencia humana y el aprendizaje automático nativo de la nube.
Los IOA basados en IA aprovechan la velocidad, la capacidad de ampliación y la precisión de la nube para detectar rápidamente las clases emergentes de amenazas y predecir los patrones de los ciberdelincuentes, independientemente de las herramientas o del malware empleados.

Enfoque nativo de la nube de un solo agente

El agente único CrowdStrike Falcon® se basa en una plataforma escalable y nativa de la nube fácil de desplegar y gestionar. Todos los módulos de la plataforma Falcon se han diseñado para utilizar el mismo agente ligero, que es discreto y permite a las organizaciones implementar nuevas defensas fácilmente sin la necesidad de incorporar más agentes.

Además del agente único y ligero, la protección de endpoints de CrowdStrike ofrece tiempos de despliegue más rápidos, un rendimiento mejorado del endpoint y mayor facilidad operativa para el equipo de TI gracias a su enfoque nativo de la nube. La plataforma Falcon, que se despliega en minutos, funciona desde el primer día sin necesidad de actualizar constantemente la firma ni contar con una infraestructura de gestión local o integraciones complejas, y lo hace sin interrumpir al antivirus existente durante la migración.

Protección unificada

Uno de los principales factores que se deben tener en cuenta a la hora de elegir una solución para la protección de endpoints es cómo se integrará en la arquitectura de ciberseguridad existente sin aumentar la complejidad ni requerir una infraestructura de gestión local.

La plataforma Falcon está diseñada como un producto altamente modular y ampliable que ayuda a los clientes a abordar los nuevos retos de seguridad con un solo agente y sin necesidad de rediseñar o reestructurar la arquitectura. Esto evita los problemas asociados a los despliegues de seguridad.

Cada vez son más las empresas que se replantean sus estrategias de seguridad en busca de un enfoque más integrado. Un ejemplo es la unificación de la protección de endpoints con ITDR para acabar con las brechas en la cobertura y la complejidad asociadas a la implementación de estas soluciones por separado. Con una protección unificada de endpoints e identidades, conseguirás reducir el riesgo y mejorar la productividad. De esta forma, las organizaciones pueden responder ante las amenazas un 85 % más rápido, lo que reduce el tiempo de investigación en 5000 horas al año.[4]

[4] No se garantizan los resultados previstos y las consecuencias efectivas, que pueden variar según el cliente. El cálculo de beneficios esperados se basa en medias acumuladas de más de 100 casos de evaluaciones de valor comercial (Business Value Assessment, BVA) y valor comercial realizado (Business Value Realized, BVR) efectuadas con clientes de CrowdStrike Enterprise y el equipo Business Value de CrowdStrike entre 2018 y diciembre de 2022. Las BVA son análisis de la rentabilidad de la inversión prevista basados en el valor de CrowdStrike comparado con la solución que poseen los clientes. Los valores de BVR corresponden al análisis de la rentabilidad de la inversión de los clientes que llevan más de 6 meses utilizando nuestra solución, y se basa en las opiniones de los clientes y la telemetría registrada.

Además de unificar la protección de endpoints con ITDR, los resultados de las investigaciones demuestran que consolidar varios productos de seguridad tiene ventajas significativas. En un estudio reciente realizado por IDC en el que se analizó el impacto de la unificación de los módulos de Falcon, los equipos de seguridad descubrieron que sus operaciones mejoraron al ayudarles a identificar un 96 % más de amenazas potenciales en la mitad de tiempo. Además, también mejoró la capacidad de los equipos de seguridad para seguir el ritmo de los ciberdelincuentes, por lo que son el doble de efectivos y capaces de investigar y responder un 66 % más rápido.

Servicios de seguridad gestionados

En este documento técnico se detallan las capacidades fundamentales que son necesarias en una solución moderna de seguridad de endpoints. No obstante, en función de las necesidades específicas de cada empresa, es posible que una solución de detección y respuesta gestionadas (MDR) sea la mejor opción para aprovecharlas. Muchas organizaciones se enfrentan a retos para contratar, formar y retener al personal de seguridad, lo que les impide desplegar un programa de seguridad madura o centrarse en iniciativas clave de negocio. La solución MDR es útil para suplir estas lagunas, ya que reúne la experiencia, la tecnología avanzada y los procesos optimizados necesarios para que las empresas cuenten con una posición de seguridad consolidada de manera ininterrumpida.

La solución CrowdStrike Falcon® Complete Next-Gen MDR ofrece protección ininterrumpida y garantía experta al basarse en la plataforma Falcon de IA nativa. Funciona como una extensión perfecta de los equipos de los clientes, y permite gestionar y supervisar la plataforma con soltura. Además, incorpora funciones de detección, respuesta e investigación de amenazas en las principales superficies de ataque, como los endpoints, la nube y las identidades. También cuenta con inteligencia y Threat Hunting, o búsqueda de amenazas, que son funciones integradas de CrowdStrike Falcon®Adversary OverWatch, para garantizar la protección frente a los ataques más sofisticados y agilizar el tiempo de respuesta promedio (MTTR). Esto permite a las empresas mejorar la ciberseguridad.

Conclusión

El panorama de la protección de endpoints ha experimentado una evolución significativa impulsada por la sofisticación de las ciberamenazas, que cada vez lo son más, y la naturaleza dinámica de los entornos de trabajo modernos. Las tecnologías avanzadas de la plataforma Falcon, el enfoque de agente único nativo de la nube, la protección unificada y los servicios de seguridad gestionados, junto con las cinco capacidades esenciales descritas en esta guía para compradores, posicionan a CrowdStrike como líder en el ámbito de la seguridad moderna de endpoints. A medida que las organizaciones se abren camino por el cambiante panorama de amenazas, adoptar una solución completa que se adapte a las necesidades descritas es fundamental para conseguir una protección y resiliencia sólidas frente a las ciberamenazas actuales.

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa en la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, una protección y un rendimiento superiores, una menor complejidad y una rentabilidad inmediata.

CrowdStrike: We stop breaches.