CROWDSTRIKE

PROTECCIÓN DE ENDPOINTS
GUÍA DEL COMPRADOR

COMPAS SOLUTIONS

Los cinco elementos esenciales de la protección de endpoints basada en la nube

TABLA DE CONTENIDO

RESUMEN EJECUTIVO

La seguridad de los endpoints es uno de los componentes más críticos de una estrategia de ciberseguridad. Por desgracia, para los responsables de proteger los endpoints de sus organizaciones, nunca ha sido tan difícil seleccionar la mejor solución para el trabajo. Con tantas opciones en el mercado y características que parecen idénticas, la elección de una solución de protección de los endpoints es cualquier cosa menos sencilla.

CrowdStrike cree que una protección de endpoints realmente eficaz debe proporcionar el máximo nivel de seguridad y simplicidad, porque la complejidad sobrecarga a los equipos y los procesos, lo que en última instancia introduce brechas de seguridad y aumenta el riesgo. Para lograr tanto la seguridad como la simplicidad, la protección de endpoints debe incluir cinco elementos clave y ser suministrada a través de una arquitectura nativa de la nube. Estos objetivos pueden servir de guía a la hora de evaluar y elegir una plataforma de protección de endpoints:

- **Prevención** para mantener fuera el mayor número posible de elementos maliciosos
- **Detección** para encontrar y eliminar a los atacantes
- **La Cacería Gestionada de Amenazas** para elevar la detección más allá de la automatización
- **Integración de la información sobre amenazas** para comprender y adelantarse a los atacantes
- **Gestión de la vulnerabilidad e higiene de TI** para preparar y reforzar el ambiente contra las amenazas y los ataques

Estos cinco elementos deben ser habilitados, integrados y entregados a través de una arquitectura nativa en la nube para simplificar las operaciones y cumplir con la velocidad, la flexibilidad y la capacidad necesarias para defenderse de los atacantes modernos.

Entonces, ¿cómo evaluar estos elementos y encontrar la solución adecuada para su organización?

Hemos elaborado esta guía para ayudarle a formular esas preguntas y obtener la información que necesita para medir y comparar las distintas soluciones.

A medida que se sumerja y adquiera mayor insight, descubrirá que CrowdStrike pone el referente muy en alto. CrowdStrike ofrece todo lo necesario para detener brechas, de forma sencilla e inteligente. La plataforma de protección de endpoint nativa en la nube CrowdStrike Falcon® unifica la tecnología, la inteligencia y la experiencia en una solución probada y demostrada para detener brechas. Combina todos los elementos esenciales en un único agente que se puede implantar en minutos, prácticamente sin impacto alguno sobre los endpoints o los usuarios. La plataforma Falcon, nativa de la nube, ofrece una protección de endpoints realmente eficaz, con el máximo nivel de seguridad y simplicidad.

Con tantas opciones en el mercado y características que parecen idénticas, la elección de una solución de protección de los endpoints es cualquier cosa menos sencilla.

INTRODUCCIÓN

La protección de los endpoints ha sido durante mucho tiempo un componente crítico de todas las estrategias de seguridad, ya que se encuentran entre los principales objetivos para los atacantes. Los adversarios suelen tratar de aprovechar las crisis y los cambios, y la pandemia no ha sido una excepción. Con nuevos puntos de acceso, a menudo no seguros, a las redes y a los datos, junto con la instalación acelerada de nuevas infraestructuras, los agentes de amenazas han aprovechado esta superficie de ataque ampliada y han aumentado tanto el volumen como el alcance de sus actividades.

La creciente velocidad de las amenazas, junto con la necesidad de un cambio rápido a medida que más aplicaciones, infraestructuras y datos se trasladan a la nube, ha cambiado el enfoque de muchos equipos de seguridad y TI. Se han dado cuenta de que deben ser ágiles, eficientes y mantener la seguridad como prioridad. Esta transición ha puesto un énfasis aún mayor en la protección de los endpoints, el nuevo perímetro para muchos.

Esta guía fue creada para ayudar a los profesionales de la seguridad definiendo los elementos críticos de la protección de los endpoints necesarios para proteger eficazmente a una organización contra las amenazas modernas.

ELEMENTOS CRÍTICOS PARA CONSIDERAR: LO QUE VERDADERAMENTE NECESITA EN UNA PLATAFORMA DE PROTECCIÓN DE ENDPOINTS

Se necesita algo más que un conjunto de capacidades reunidas bajo un mismo paraguas para ser una solución de protección de endpoints capaz. Para ser realmente eficaz, una solución para endpoints debe estar diseñada para detener continuamente las brechas en todo el espectro de ataques.

Las técnicas de ayer para detectar y bloquear las amenazas en el endpoint son ineficaces contra las amenazas modernas de hoy en día. Las fallas no pueden evitarse de forma fiable mediante el monitoreo y el escaneo de archivos y la búsqueda de los malos conocidos.

La eficacia de la seguridad está directamente relacionada con la cantidad y la calidad de los datos que se puedan recopilar y con la capacidad de analizarlos, independientemente de su procedencia. La prevención de fallas requiere tomar estos datos y aplicar las mejores herramientas, incluyendo la inteligencia artificial (IA), el análisis de comportamiento, las informaciones sobre amenazas y el equipo de threat hunters. Las soluciones eficaces deben apalancar estos datos masivos para anticipar continuamente dónde aparecerá la próxima amenaza grave, a tiempo para actuar.

Aprovechar los datos y las herramientas para detener brechas requiere una plataforma escalable y nativa de la nube: una nube de seguridad.

Un enfoque nativo en la nube permite agregar, compartir y hacer operativa esta información sin dificultades para ofrecer el tipo de capacidades de anticipación, prevención, detección, visibilidad y respuesta que pueden vencer a un atacante decidido una y otra vez.

Para obtener esas capacidades, los responsables de la toma de decisiones deben buscar cinco elementos críticos en una solución de seguridad para endpoints nativa de la nube:

LOS CINCO ELEMENTOS CRÍTICOS DE LA PROTECCIÓN DE ENDPOINTS

ELEMENTO CRÍTICO 1: PREVENCIÓN

PROTECCIÓN CONTRA EL MALWARE Y MÁS ALLÁ CON ANTIVIRUS DE ÚLTIMA GENERACIÓN (NGAV)

Hay razones de peso por las que los productos tradicionales de protección de endpoints centrados en el malware simplemente no proporcionan un nivel adecuado de protección contra las amenazas y adversarios actuales.

La protección centrada en el malware no aborda las tácticas cada vez más sofisticadas sin archivos y libres de malware que utilizan los adversarios modernos. De hecho, el **Informe Global de Amenazas de CrowdStrike 2020** señaló que la tendencia hacia los ataques libres de malware se está acelerando, y que este tipo de ataques superará el volumen de los ataques con malware en 2020.

Una solución eficaz de protección de endpoints debe resolver este reto ampliando su alcance más allá de la simple identificación y tratamiento del malware conocido. En primer lugar, debe proteger contra el malware conocido y desconocido utilizando tecnologías tales como el machine learning (ML) que no requieren actualizaciones diarias. Debe mirar más allá del malware y aprovechar al máximo el análisis del comportamiento para buscar automáticamente señales de ataque y bloquearlas en el momento en que se produzcan. Además, la solución de protección de endpoints ideal debe proteger los endpoints contra todo tipo de amenazas, desde el malware conocido y desconocido hasta los ataques sin archivos y libres de malware, combinando todas las tecnologías necesarias para una protección definitiva.

La Tabla 1 resume los casos de uso clave y las capacidades críticas que debe ofrecer el componente NGAV de una solución eficaz de protección de endpoints.

NGAV: CASOS DE USO Y CAPACIDADES ESENCIALES

Evite el malware conocido y el de día cero	**Características Requeridas** ■ ML en el endpoint para evitar el malware conocido y desconocido, el adware y los programas potencialmente no deseados (PUP, por su sigla en inglés) ■ Análisis automatizado de malware (por ejemplo, sandboxing) ■ Inteligencia Integrada de Amenazas ■ Capacidades personalizadas de lista de permitidos y lista de bloqueados ■ Ingesta automática de indicadores de compromiso (IOC, por su sigla en inglés) de terceros
	Criterios de Evaluación ● Resultados de las pruebas de terceros independientes ● Tasas de falsos positivos
	Preguntas por Hacer ● ¿El producto es basado en la firma o utiliza ML? ● Si el producto utiliza ML, ¿el endpoint tiene que estar conectado a la nube para utilizarlo? ● ¿Cuál de las funciones de prevención requiere una conexión a la nube? ● En caso de que el malware no se bloquee, ¿qué otros mecanismos de prevención ofrece el producto?
Protección contra el ransomware	**Características Requeridas** ■ ML en el agente ■ Análisis de comportamiento/indicadores de ataque (IOA) específicos del ransomware ■ Inteligencia Integrada de Amenazas
	Criterios de Evaluación ● Rendimiento anterior contra ransomware de la vida real como WannaCry, NotPetya y Ryuk ● Resultados de las pruebas de terceros
	Preguntas por Hacer ● ¿Qué métodos utiliza para evitar el ransomware? ● ¿Qué métodos utiliza para evitar el ransomware de día cero? ● ¿Cómo ha gestionado el producto los brotes de ransomware como Wannacry, NotPetya y Ryuk?
Prevenir ataques sin archivos y libres de malware: Proteja sus endpoints contra todo tipo de amenazas, no sólo el malware y los exploits	**Características Requeridas** ■ Protección contra exploits conocidos ■ Protección contra exploits de día cero ■ Protección de la memoria ■ Indicador de ataque (IOA), bloqueo de comportamiento ■ Bloqueo de comportamiento IOA personalizado
	Criterios de Evaluación ● Éxito en la prueba de emulación de adversarios en MITRE ● Resultados en comparación con los ejercicios red team
	Preguntas por Hacer ● ¿Qué tipo de actividades maliciosas no relacionadas con el malware puede bloquear? ● ¿Puede bloquear a un atacante que se conecta utilizando credenciales robadas y herramientas legítimas para realizar sus acciones? ● ¿Contra qué áreas del marco MITRE ATT&CK® puede proteger? ● ¿Puede la solución impedir la utilización maliciosa de aplicaciones legítimas como PowerShell? ¿Cómo? ● ¿Cómo bloquea la solución los exploits? ● ¿Es capaz el producto de bloquear los exploits de día cero? ● En caso de que no se bloquee un ataque, ¿qué otros mecanismos de prevención emplea el producto? ● ¿Qué tipo de mecanismos de protección de la memoria ofrece el producto?

Ofrece la máxima protección en todo momento: Protege siempre al máximo nivel de sus capacidades	**Características Requeridas** ■ No requiere actualizaciones diarias para mantener la protección al máximo nivel ■ Se mantiene actualizada automáticamente ■ No se reinicia al instalar o actualizar ■ Protege fuera de línea cuando no hay conexión con la nube ■ Ofrece protección contra la manipulación de los sensores ■ Protección en todos los sistemas operativos y versiones del sistema operativo
	Criterios de Evaluación ● Frecuencia e impacto en el rendimiento de las actualizaciones (actualizaciones de la versión del producto/agente, firmas de malware o archivos DAT, etc.) ● Demostración de malware conocido y desconocido y de acciones maliciosas en un endpoint sin conexión
	Preguntas por Hacer ● ¿Con qué frecuencia hay que actualizar el producto para garantizar el máximo nivel de protección? ● ¿Qué puede evitar el producto cuando está fuera de línea, si el usuario abre un archivo o ejecutable, o realiza acciones maliciosas cuando no está conectado a Internet? ● ¿Con qué rapidez se admiten nuevas versiones del sistema operativo? ● ¿Las actualizaciones del sensor requieren reinicios? Si es así, ¿qué impacto tiene esto en los hosts críticos y servidores?
Proporcionar una respuesta y una remediación rápidas	**Características Requeridas** ■ La capacidad de poner en cuarentena un archivo malicioso ■ Conserva la información de detección durante al menos 90 días para su investigación ■ Proporciona visibilidad y contexto de los ataques ■ Envía los archivos en cuarentena al sandbox para su análisis automático ■ Proporciona una API para integrarse con los sistemas de orquestación/gestión de casos existentes del cliente
	Preguntas por Hacer ● Lista de acciones que puede realizar la solución ● Captura de pantalla o demostración del detalle de la alerta ● Resultado del análisis del sandbox ● Lista de los sistemas de orquestación de seguridad y de tickets existentes con los que se integra el producto
	Perguntas a Serem Feitas ● ¿Qué capacidad de respuesta ofrece el producto? ● ¿Cómo se integra el producto con las herramientas de seguridad existentes? ● ¿Las alertas del producto proporcionan un contexto para mejorar las defensas en general? ● ¿Puede el producto generar Indicadores de Compromiso (IOCs) a partir de una alerta para mejorar las defensas en general?

Tabla 1: Antivirus de Última Generación (NGAV): Casos de Uso y Capacidades Esenciales

EL ENFOQUE CROWDSTRIKE

La plataforma de protección de endpoints CrowdStrike Falcon proporciona una nueva generación de funciones de prevención, capaz de derrotar las sofisticadas herramientas y técnicas utilizadas por los atacantes actuales y de llenar el vacío dejado por las soluciones antivirus basadas en firmas. La plataforma Falcon combina una serie de potentes métodos para proporcionar prevención contra las tácticas, técnicas y procedimientos (TTP) que hacen que los ataques modernos tengan éxito. Esa combinación de métodos permite a Falcon no sólo proteger contra el malware básico, sino también prevenir el malware de día cero, los exploits y, lo que es más importante, los ataques sin archivos y libres de malware. Falcon utiliza la función de prevención adecuada en el momento adecuado para bloquear los agentes de amenaza en todo el espectro de ataques.

Falcon emplea ML en el endpoint para la prevención previa a la ejecución de malware conocido y desconocido. Su función de ML es tan potente que ha protegido a los clientes de Falcon del ransomware WannaCry, NotPetya y Ryuk, desde que se saca de la caja, sin requerir ninguna acción o actualización por parte del usuario.

Falcon también utiliza la mitigación de exploits para defenderse de los atacantes que aprovechan los exploits como parte de ataques basados en malware o libres de malware. La mitigación de exploits consiste en detener los intentos de explotación de vulnerabilidades, tanto de exploits conocidos como de día cero, para evitar que los hosts se vean comprometidos.

Contra atacantes sofisticados que no limitan sus tácticas al uso de malware y exploits, Falcon utiliza IOAs. Se trata de algoritmos basados en el comportamiento que se centran en detectar la intención de los atacantes, o lo que intentan conseguir, independientemente de las herramientas utilizadas en el ataque. Las capacidades de prevención basadas en IOA permiten a los clientes evitar las amenazas que eluden las tecnologías tradicionales, tales como las firmas o las listas de permisos.

La protección siempre activa significa que los endpoints están seguros, ya sea en línea o sin conexión. El agente ligero Falcon tiene poco impacto en los endpoints, desde la instalación inicial hasta el uso diario, y no es necesario reiniciar después de la instalación.

ELEMENTO CRITICO 2: DETECCIÓN

PROPORCIONAR LOS DATOS ADECUADOS EN EL MOMENTO OPORTUNO PARA ACTUAR CON RAPIDEZ Y SEGURIDAD

Como los atacantes esperan encontrar medidas de prevención en un objetivo, han perfeccionado su arte para incluir técnicas diseñadas para eludir la prevención. Estas técnicas incluyen el robo de credenciales, los ataques sin archivos o los ataques a la cadena de suministro de software. Cuando un atacante es capaz de afianzarse o lograr un foothold sin que salte ninguna alarma, se denomina "fallo silencioso", que permite a los atacantes habitar un ambiente durante días, semanas o incluso meses sin ser detectados. El remedio para el fallo silencioso es la Detección y Respuesta de Endpoints (EDR), que proporciona la visibilidad que los equipos de seguridad necesitan para descubrir a los atacantes lo antes posible.

Un sistema EDR en pleno funcionamiento debe integrarse estrechamente con la capacidad de prevención. Debe registrar todas las actividades de interés en un endpoint para una inspección más profunda, tanto en tiempo real como a posteriori. Debe enriquecer estos datos con informaciones sobre amenazas para proporcionar el contexto necesario, que es fundamental para la cacería e investigación. Una solución EDR eficaz también debe ser inteligente y capaz de detectar automáticamente la actividad maliciosa y presentar ataques reales (no la actividad benigna) sin necesidad de que los equipos de seguridad escriban y ajusten las reglas de detección.

Igualmente importante es que el sistema EDR ofrezca una forma sencilla de mitigar una brecha descubierta. Esto podría significar la contención de los endpoints expuestos para detener la brecha en su camino, lo que permite la remediación antes de que se produzcan daños.

Consulte los casos de uso de la Tabla 2 para guiarse en su evaluación de las capacidades de EDR para las soluciones de endpoint que está considerando.

DETECCIÓN Y RESPUESTA DE ENDPOINTS (EDR): CASOS DE USO Y CAPACIDADES ESENCIALES

Descubra automáticamente a los atacantes sigilosos	**Características Requeridas** ■ Detección automática de incidentes: EDR inteligente con detecciones integradas en tiempo real ■ Detección automática basada en el análisis del comportamiento, como los IOAs ■ Integración con informaciones sobre amenazas ■ Automatizar el triaje priorizando de forma inteligente la actividad maliciosa y de los atacantes ■ Proporciona el nivel de amenaza de la organización en tiempo real
	Criterios de Evaluación ● No es necesario hacer ajustes, escribir reglas ni realizar configuraciones complejas ● Demostración de la priorización de incidentes ● Rendimiento eficaz frente a las pruebas de penetración
	Preguntas por Hacer ● ¿Qué tipo de reglas de detección o correlación hay que escribir para que el producto pueda detectar incidentes? ● ¿Qué nivel de conocimientos se requiere para utilizar la solución?
Detectar lo desconocido y cazar las amenazas: Detectar ataques que han burlado la prevención y reducen drásticamente el tiempo de permanencia de los atacantes	**Características Requeridas** ■ Captura de eventos sin procesar, incluso cuando no están asociados a alertas y detecciones ■ Retención de datos de detección a largo plazo (12 meses) ■ Funciona en modo kernel para una visibilidad total y para eliminar los puntos ciegos ■ Capacidades de búsqueda histórica y en tiempo real totalmente personalizables ■ Búsquedas simultáneas en toda la empresa sin impacto en los endpoints ■ Ofrece respuestas a las consultas en cinco segundos o menos ■ Repositorio de datos centralizado para permitir la detección avanzada
	Criterios de Evaluación ● Los tipos de eventos que el producto es capaz de observar y recoger ● Periodo de retención disponible tanto para los eventos crudos como para las detecciones ● Detección de ataques y comportamientos específicos
	Preguntas por Hacer ● ¿Qué nivel de visibilidad ofrece la solución (por ejemplo, a nivel del kernel)? ● ¿Qué tipo de datos de telemetría del endpoint recoge el agente? ● ¿Cómo facilita el producto la cacería de amenazas proactiva? ● ¿Cómo se obtienen las búsquedas y los resultados de las consultas? (por ejemplo, interrogando a los endpoints, consultando una base de datos en la nube)? ● ¿Las búsquedas ofrecen resultados en tiempo real? ● ¿Hay límites en los resultados de las consultas? ● ¿Dónde se almacenan los datos de los eventos y durante cuánto tiempo? ¿Datos brutos de los eventos? ¿Datos de detección? ● ¿Cómo proporciona el producto la detección y visibilidad de los ataques?

Acelerar las investigaciones y los análisis forenses	**Características Requeridas** ■ Visualización de alertas intuitiva y completa: muestra el historial completo de ataques en un árbol de procesos con capacidades de desglose y pivote ■ Pasos de ataque asignados a un marco de ataque estándar de la industria como MITRE ATT&CK ■ Proporciona datos forenses incluso si el endpoint no está disponible, es inaccesible o está destruido ■ Detecciones y alertas en todo el contexto, incluidos los datos de informaciones sobre amenazas ■ Periodo de conservación de datos flexible para los eventos ■ Lenguaje de consulta estándar para buscar datos de eventos ■ Flujos de trabajo intuitivos desde una única consola ■ Repositorio de datos centralizado para permitir la cacería e investigación de amenazas ■ Correlacionar eventos individuales en incidentes
	Criterios de Evaluación ● Captura de pantalla o demostración de la visualización de la alerta ● Prueba de concepto (POC) o prueba de valor (POV) ● Adopción de un marco de la industria para la representación de los ataques
	Preguntas por Hacer ● ¿Puede el producto decirme cómo está accediendo un atacante a mi ambiente? ● ¿Cómo permite la solución a los analistas de seguridad visualizar las alertas, hacer la conexión entre eventos y pivotar a otros eventos y endpoints? ● ¿Qué tipo de funciones permiten que el producto detecte comportamientos maliciosos en el momento en que se producen o después? ● ¿Cómo detecta y visualiza el producto el movimiento lateral? ● ¿El producto correlaciona las alertas de detección individuales en incidentes o ataques?
Aceleración de la remediación y la respuesta	**Características Requeridas** ■ Capacidad de contener en red los endpoints ■ Capacidad de poner en cuarentena los archivos ■ Capacidad para ejecutar comandos en endpoints sospechosos de forma remota y en tiempo real ■ API para integrarse con los sistemas de orquestación/gestión de casos existentes del cliente ■ Notificaciones de alerta personalizables
	Criterios de Evaluación ● Lista de capacidades de respuesta disponibles en el producto ● Compatibilidad con la API e integración con los sistemas de seguridad y flujos de trabajo existentes
	Preguntas por Hacer ● ¿Qué capacidades de respuesta ofrece la solución? ● ¿Cómo se integra la solución con las herramientas de seguridad y empresariales existentes, como las soluciones SOAR y otras?

Tabla 2. Detección y Respuesta de Endpoints (EDR): Casos de Uso y Capacidades Esenciales

EL ENFOQUE CROWDSTRIKE

CrowdStrike Falcon Insight™ EDR supervisa y registra las actividades que tienen lugar en el endpoint, proporcionando la visibilidad histórica y en tiempo real necesaria para detectar la actividad de los atacantes al tiempo que permite a los equipos de seguridad investigar y resolver los incidentes rápidamente. Este enfoque detiene a los atacantes antes de que hagan daño, eliminando esencialmente el riesgo de fallo silencioso.

Falcon también proporciona capacidades de análisis tanto automáticas como humanas que pueden realizarse mientras los eventos están teniendo lugar o después del hecho. El análisis automático puede detectar inmediatamente y priorizar de forma inteligente la actividad maliciosa y de los atacantes. La capacidad de análisis manual otorga a los equipos de seguridad la visibilidad profunda y el contexto que necesitan para la cacería de amenazas proactiva, la investigación rápida de incidentes y la remediación. Además, la arquitectura nativa en la nube de CrowdStrike proporciona la velocidad y la escalabilidad necesarias para recopilar y retener todos los eventos de endpoints necesarios, incluso si los endpoints no están disponibles, han sido destruidos o se han eliminado (como puede ser el caso de las cargas de trabajo virtuales).

La base de datos CrowdStrike Threat Graph®, el cerebro de la plataforma Falcon, ingiere y analiza más de 5 billones de eventos en tiempo real cada semana, lo que convierte a la plataforma de seguridad en la nube Falcon en una de las fuentes de verdad más avanzadas del sector para el insight sobre seguridad y la información de inteligencia sobre adversarios. La capacidad CrowdScore™, una innovadora función de detección de Falcon Insight, procesa constantemente los datos en Threat Graph, buscando actividad maliciosa mediante el análisis de todos los comportamientos, así sean o no alertados al usuario. No se trata simplemente de agrupar alertas atómicas, sino de buscar y ponderar las evidencias de actividad que conforman el comportamiento del atacante, haya sido o no alertado previamente al usuario. Cuando se detecta un ataque, se crea un incidente. CrowdScore aborda la fatiga de las alertas detectando ataques en lugar de detectar comportamientos específicos, lo que resulta en una reducción media del 98% de los elementos que requieren análisis (comparando el recuento de alertas con el de incidentes).

Desde una única consola, Falcon Insight proporciona visibilidad en tiempo real, eventos históricos y los medios para analizar los datos para garantizar que las organizaciones puedan identificar rápidamente cualquier posible fallo silencioso y responder adecuadamente con las herramientas necesarias.

ELEMENTO CRITICO 3: CACERÍA GESTIONADA DE AMENAZAS

ELEVAR LA DETECCIÓN MÁS ALLÁ DE LA AUTOMATIZACIÓN CON LA CACERÍA GESTIONADA DE AMENAZAS

Esperar pasivamente a que los productos de seguridad detecten automáticamente los ataques no permitirá descubrir y detener las sofisticadas amenazas ocultas. Así lo demuestran las continuas fallas que se producen incluso en ambientes en los que se ha desplegado tecnología de seguridad nueva y avanzada. Esto se debe a que las alertas automáticas pasivas se basan en parámetros preestablecidos que pueden ser probados y burlados por atacantes decididos. Por ello, la cacería de amenazas proactiva, dirigida por expertos en seguridad humana, es un elemento imprescindible para cualquier organización que desee lograr o mejorar la detección de amenazas y la respuesta a incidentes en tiempo real.

La cacería de amenazas desempeña un papel fundamental en la detección temprana de ataques y adversarios. Constituye un enfoque proactivo dirigido por el ser humano que busca actividades sospechosas de manera activa, en lugar de confiar pasivamente en la tecnología para detectar y alertar automáticamente sobre la actividad de un posible atacante. La detección e investigación tempranas de dicha actividad permiten a las organizaciones detener los ataques antes de que puedan causar daños.

Por desgracia, la falta de recursos y la escasez de conocimientos en materia de seguridad hacen que la cacería proactiva de amenazas sea inalcanzable para la mayoría de las organizaciones. Los equipos internos con poco personal no pueden vigilar las 24 horas del día la actividad de los adversarios y, en muchos casos, no están equipados para responder eficazmente a ataques extremadamente sofisticados. Esto puede dar lugar a tiempos de investigación más largos con menos alertas que se manejan de manera oportuna, lo que en última instancia resulta en tiempos de permanencia más largos y un mayor riesgo de que los atacantes logren sus objetivos.

La cacería gestionada de amenazas resuelve este reto proporcionando un equipo de cacería de élite que no sólo encuentra actividades maliciosas que pueden haber pasado desapercibidas por los sistemas de seguridad automatizados, sino que también las analiza a fondo y proporciona a los clientes directrices de respuesta.

La Tabla 3 le ayudará a identificar las capacidades esenciales que debe proporcionar una solución de cacería gestionada de amenazas y cómo evaluar y valorar las diferentes opciones.

CACERÍA GESTIONADA DE AMENAZAS: CASOS DE USO Y CAPACIDADES ESENCIALES

Vea y detenga los ataques avanzados ocultos	**Características Requeridas** ■ Threat hunters internos, experimentados y dedicados ■ Servicios de cacería de amenazas 24/7 ■ Capacidad de encontrar amenazas que ningún otro sistema ha detectado ■ Acceso inmediato a los expertos en informaciones sobre amenazas para un análisis más rápido ■ Integración automática y nativa con las informaciones sobre amenazas para una mayor eficacia ■ Integración con la plataforma de seguridad de los endpoints
	Criterios de Evaluación ● Número de fallas únicas detectadas y evitadas al año ● Número de incidentes investigados por año ● Tipo de plataforma utilizada para la cacería de amenazas
	Preguntas por Hacer ● ¿Puede usted proporcionar servicios gestionados de cacería de amenazas, o tiene que depender de un tercero para proporcionar este servicio? ● ¿Qué tipo de plataforma utiliza para la cacería de amenazas?
Priorizar las amenazas más urgentes y garantizar que no se pierdan las alertas críticas	**Características Requeridas** ■ Capacidad para detectar las amenazas más urgentes en el ambiente ■ Proporcionar comunicaciones de bucle cerrado mejoradas para garantizar que las alertas importantes sean advertidas
	Criterios de Evaluación ● Acuerdos de nivel de servicio (SLA, por su sigla en inglés) ● Proceso documentado de retroalimentación en bucle cerrado
	Preguntas por Hacer ● ¿Cuál es su proceso para informar a la organización de que se ha detectado un incidente? ● ¿Tiene un proceso de escalado de alertas? Si es así, ¿qué tipos de alertas escalan y cuándo?
Guiarle en el proceso de respuesta	**Características Requeridas** ■ Proporciona alertas procesables ■ Proporciona asistencia durante los incidentes ■ Proporciona orientación sobre lo que hay que hacer a continuación y sugerencias de mitigación potencial en las detecciones
	Criterios de Evaluación ● Revisar ejemplos de alertas ● Ver ejemplos de recomendaciones
	Preguntas por Hacer ● ¿Cómo se comunica el equipo de cacería de amenazas con el cliente? ● ¿Qué tipo de información proporciona el equipo sobre la actividad maliciosa que ha detectado?
Aumentar el equipo de seguridad actual: Alcanzar un mayor nivel de madurez de seguridad de forma instantánea, minimizando los gastos administrativos, la complejidad y el costo	**Características Requeridas** ■ Capacidad para observar la actividad de los adversarios en directo y observar lo que están haciendo mientras lo hacen ■ Monitorizar después de un incidente para ver si los atacantes vuelven
	Criterios de Evaluación ● Tiempo transcurrido entre la detección inicial y el informe detallado sobre el incidente que incluye ● orientaciones para su remediación Referencias y testimonios de clientes
	Preguntas por Hacer ● ¿Qué experiencia tiene el equipo de cacería de amenazas de amenazas y cuál es la trayectoria de sus miembros? ● ¿Se dedican a la cacería de amenazas? Si no es así, ¿qué otras responsabilidades tienen, además de la cacería de amenazas? ● ¿Qué resultados están obteniendo otros clientes?

Tabla 3. Cacería Gestionada de Amenazas: Casos de Uso y Capacidades Esenciales

EL ENFOQUE CROWDSTRIKE

El incomparable equipo de CrowdStrike Falcon OverWatch™ del equipo de threat hunters dedicados, cuando se combina con la solidez de los datos recopilados por la plataforma Falcon, es capaz de frustrar ataques que nunca serían detectados por otro sistema o tecnología.

El equipo de OverWatch está formado por analistas altamente calificados y experimentados que llevan las operaciones de seguridad tradicionales al siguiente nivel ofreciendo una búsqueda proactiva de amenazas 24/7 los 365 días del año. Aumentan las capacidades de seguridad existentes y cubren las lagunas en la detección de amenazas avanzadas y la respuesta a incidentes. El resultado es una reducción drástica e incluso la eliminación de los tiempos de permanencia de los atacantes.

OverWatch aporta el mejor equipo de threat hunters del sector a las operaciones de seguridad de los clientes. Aprovechando al máximo la arquitectura nativa en la nube de CrowdStrike, impulsada por CrowdStrike Threat Graph, el equipo busca proactivamente actividades anómalas o nuevas de los atacantes que son invisibles para las tecnologías de seguridad. Una vez identificada una amenaza, OverWatch trabaja lado a lado con el cliente, ofreciéndole asesoramiento experto sobre cómo manejar el incidente. OverWatch aporta un elemento esencial de cacería humana que garantiza que no se pase nada por alto. Esta es la clave para detener las fallas.

ELEMENTO CRITICO 4: ANTICIPACIÓN

LOGRAR ESTAR Y QUEDARSE ADELANTE DE LOS ATACANTES CON INFORMACIONES SOBRE AMENAZAS

Los atacantes se mueven con tanta rapidez y sigilo que es un reto tanto para las tecnologías de protección como para los profesionales de la seguridad mantenerse al día con las últimas amenazas y protegerse proactivamente contra ellas. Las informaciones sobre amenazas permiten a los productos y equipos de seguridad comprender y predecir eficazmente las amenazas cibernéticas que podrían afectarles. Permite a las organizaciones anticipar el "quién" y el "cómo" del próximo ataque, y permite a los equipos de seguridad centrarse en priorizar y configurar los recursos para poder responder eficazmente a futuros ataques.

Además, las informaciones sobre amenazas proporcionan la información que permite a los equipos de seguridad comprender, responder y resolver los incidentes con mayor rapidez, acelerando las investigaciones y la remediación de incidentes. Por ello, los profesionales de la seguridad que se ocupan de la protección de los endpoints deben asegurarse de no centrarse únicamente en la infraestructura de seguridad.

Es importante que las informaciones sobre amenazas procesables se incluyan como parte de la solución total. Poner la información adecuada al alcance de los equipos de seguridad permite tomar decisiones y respuestas más rápidas y mejores. Al considerar dicha integración, los clientes deben asegurarse de que la inteligencia proporcionada se integre de manera transparente en la solución de endpoints y que su consumo pueda automatizarse.

Utilice la Tabla 4 para guiar su evaluación de la integración de las informaciones sobre amenazas proporcionadas en las soluciones de protección de endpoints que está considerando.

INTEGRACIÓN DE INFORMACIONES SOBRE AMENAZAS: CASOS DE USO Y CAPACIDADES

Maximizar las defensas: Priorizar las actividades y los recursos, defenderse de forma proactiva contra futuros ataques	**Características Requeridas** ■ Generación automática de IOCs personalizados e inteligencia sobre amenazas relevantes y exclusivas a un ambiente, entregadas en cuestión de minutos ■ Ingesta automática de IOCs de terceros ■ Informes del perfil del adversario para priorizar la actividad y los recursos (qué parchear primero, etc.)
	Criterios de Evaluación ● El proveedor suministra su propia información sobre amenazas (no depende de fuentes de terceros) ● El proveedor es capaz de proporcionar múltiples niveles de inteligencia e información sobre amenazas: estratégica, operativa, táctica
	Preguntas por Hacer ● ¿Cómo se integran las informaciones sobre amenazas con la solución de protección de endpoints? ● ¿Cómo pueden los clientes utilizar la información sobre amenazas? ¿Cómo se presentan y formatean? ● ¿Con qué frecuencia se actualiza la información sobre amenazas? ● ¿Cuántas fuentes y qué tipo de fuentes utiliza el proveedor para generar su servicio de información de amenazas?
Acelerar las detecciones	**Características Requeridas** ■ Alertas automáticas sobre las actividades de los adversarios (estado-nación y crimen electrónico) detectadas en el ambiente ■ Detecciones automáticas basadas en la información sobre amenazas del propio proveedor (por ejemplo, IPs, dominio, archivo, malos conocidos etc.) ■ Capacidad de generar y consumir IOCs automáticamente ■ Capacidad de realizar barridos de IOCs personalizados
	Criterios de Evaluación ● Nivel de integración de la información sobre amenazas con el producto: cuánto está automatizado y cuánto requiere un procesamiento manual
	Preguntas por Hacer ● ¿Puede el producto decirme quién está atacando a mi organización? ● ¿Cuál es el motivo del atacante? ● ¿Qué tácticas y técnicas utiliza el atacante? ● ¿Qué herramientas podrían emplear?
Acelerar las investigaciones y la remediación	**Características Requeridas** ■ Proporciona un contexto adicional en las alertas y detecciones para una investigación más rápida ■ Proporciona la atribución de los ataques para saber quién le está atacando, por qué y cómo para ayudar a priorizar la respuesta y la acción ■ Capacidad para visualizar las relaciones entre los IOCs, los adversarios y los endpoints ■ Capacidad para analizar automáticamente el malware con la creación instantánea de IOC e informes de análisis detallados ■ Proporciona perfiles de actores y adversarios
	Criterios de Evaluación ● Información procesable: ¿Cómo se puede utilizar la información sobre amenazas?
	Preguntas por Hacer ● ¿Qué tipo de información sobre amenazas incluyen sus alertas y detecciones?

Tabla 4. Integración de la información sobre amenazas: Casos de Uso y Capacidades Esenciales

EL ENFOQUE CROWDSTRIKE

CrowdStrike Falcon es la primera plataforma que integra perfectamente la información sobre amenazas en la protección de los endpoints, automatizando las investigaciones de incidentes y acelerando la respuesta a las fallas. El análisis instantáneo de las amenazas que llegan a los endpoints, combinado con la experiencia del equipo global de CrowdStrike Intelligence, permite a cualquier equipo de seguridad, independientemente de su tamaño o sofisticación, hacer realidad la seguridad predictiva.

Falcon proporciona la inteligencia crítica que los equipos de seguridad necesitan para adelantarse a los atacantes y para priorizar y responder a los incidentes lo más rápido posible y de la forma más adecuada. Falcon aprovecha al máximo la información y el insight proporcionados por el equipo de CrowdStrike Intelligence para proporcionar un contexto adicional a las alertas e incidentes.

Esto reduce drásticamente la complejidad de las investigaciones de incidentes, que consume muchos recursos, y lleva las alertas de detección y respuesta de endpoints al siguiente nivel. No sólo muestra lo que ha sucedido en el endpoint, sino que también proporciona la atribución y revela "el quién, el por qué y el cómo" detrás del ataque. Por ejemplo, Falcon proporciona automáticamente la atribución de herramientas, dominios, IPs, tácticas y técnicas a adversarios conocidos. Por ejemplo, Falcon proporciona automáticamente la atribución de herramientas, dominios, IPs, tácticas y técnicas a adversarios conocidos. Proporciona perfiles detallados de los adversarios que ayudan a proteger de forma proactiva contra esos agentes de amenaza, si se encuentran en un ambiente.

Por último, Falcon puede automatizar el análisis de malware para ofrecer inteligencia procesable y IOCs personalizados que se ajusten específicamente a las amenazas encontradas en los endpoints de una organización. Con este nivel de automatización, los equipos de seguridad pueden priorizar muy rápidamente qué amenazas deben analizar primero y asignar sus recursos al análisis en lugar de la priorización.

Falcon combina las herramientas utilizadas por los investigadores de amenazas cibernéticas de clase mundial en una solución perfecta y realiza las investigaciones automáticamente. Esta estrecha y automática integración entre Falcon y la información sobre amenazas permite a todos los equipos, independientemente de su tamaño o sofisticación, comprender mejor, responder más rápido y adelantarse proactivamente a los atacantes.

ELEMENTO CRÍTICO 5: PREPARACIÓN

PREPARACIÓN PARA LA BATALLA CON LA GESTIÓN DE VULNERABILIDADES Y LA HIGIENE DE TI

La seguridad comienza con el cierre de brechas para reducir la superficie de ataque y estar mejor preparados para enfrentar las amenazas. Esto requiere comprender qué sistemas y aplicaciones son vulnerables y quiénes y qué están activos en su ambiente. Por ello, la gestión de la vulnerabilidad y la higiene de TI son los bloques fundamentales de una práctica de seguridad eficiente y deberían formar parte de cualquier solución sólida de protección de endpoints. Proporcionan la visibilidad y la información procesable que la seguridad y los equipos de TI necesitan para implementar medidas preventivas y asegurarse de que están preparados para hacer frente a las sofisticadas amenazas actuales.

Cuando se trata de la evaluación y gestión de la vulnerabilidad, el monitoreo regular y continuo es crítico para identificar y priorizar las debilidades dentro de los sistemas de su organización. Por ejemplo, si tiene aplicaciones desactualizadas, pero no supervisa continuamente las vulnerabilidades, su ambiente podría convertirse en un vector de ataque clave para los adversarios. Por lo tanto, la capacidad de descubrir, parchear y actualizar las aplicaciones vulnerables que se ejecutan en su ambiente proporciona una enorme ventaja contra los atacantes.

Lo mismo ocurre con la higiene de TI. Saber quién y qué hay en su red puede permitir al departamento de TI trabajar de forma proactiva para abordar las incógnitas o las lagunas de su arquitectura de seguridad. Las soluciones de higiene de TI ofrecen la posibilidad de identificar los sistemas no gestionados o los que podrían ser un riesgo en la red, como los sistemas BYOD o de terceros no protegidos. Esta solución también debe supervisar continuamente los cambios en sus activos, aplicaciones y usuarios.

El robo de credenciales sigue siendo otro vector popular y eficiente para los atacantes. Supervisar y obtener visibilidad de las tendencias de inicio de sesión (actividades/duración) en todo su ambiente, dondequiera que se utilicen credenciales y se creen credenciales de administrador, permite a los equipos de seguridad detectar y mitigar el abuso de credenciales y los ataques que emplean credenciales robadas.

La gestión de la vulnerabilidad y la higiene de TI proporcionan a los equipos de seguridad la información que necesitan para adoptar una postura proactiva eficaz para mejorar su postura de seguridad general y estar en la mejor posición para enfrentarse a los adversarios.

La tabla 5 le ayudará a evaluar las funciones de la gestión de la vulnerabilidad e higiene de TI que ofrece una solución de protección de endpoints.

GESTIÓN DE VULNERABILIDADES E HIGIENE DE TI: CASOS DE USO Y CAPACIDADES ESENCIALES

Revelar las vulnerabilidades	**Características Requeridas** ■ Capacidad para generar una lista de hosts vulnerables y otras vulnerabilidades presentes en el ambiente ■ Prioriza las vulnerabilidades que son críticas para sus sistemas ■ Posibilidad de comprobar las vulnerabilidades de las aplicaciones ■ Distingue entre parches instalados y parches aplicados con éxito ■ No causa ningún impacto en los endpoints (no hay escaneo)
	Criterios de Evaluación ● Impacto en los endpoints ● Exactitud de la información (pertinente, actualizada, completa, etc.) ● Capacidades de priorización
	Preguntas por Hacer ● ¿Esta solución requiere un agente adicional? ● ¿Puede el producto diferenciar los parches instalados de los desplegados? ● ¿El producto ofrece la posibilidad de personalizar los tableros de mando o los filtros para agilizar el análisis de vulnerabilidad? ● ¿La información está actualizada o se requiere un escaneo para acceder al último estado?
Supervisar las cuentas y el uso de las cuentas privilegiadas	**Características Requeridas** ■ Identifica las tendencias de uso de las cuentas: en qué hosts se conectó el usuario, la duración media de las sesiones, la duración de las sesiones en cada host, las horas en que el usuario suele conectarse y el tipo de registro (por batch, remoto) ■ Proporciona información detallada sobre el uso de la cuenta de administrador local y de dominio ■ Muestra a los hosts cuando se ha utilizado una cuenta de usuario
	Criterios de Evaluación ● Evaluar el tablero de mando y los reportes de información sobre el uso de las cuentas que se proporcionan
	Preguntas por Hacer ● ¿Esta capacidad requiere un agente adicional? ● ¿Cómo se recoge esta información? ● ¿Cómo se integra esto con las demás capacidades del producto de endpoint?
Identificar los sistemas desprotegidos y encontrar los sistemas "rogue" no gestionados	**Características Requeridas** ■ Proporciona una visión en tiempo real de los activos en el ambiente ■ Distingue entre activos gestionados, no gestionados y no soportados, incluyendo impresoras, cámaras, etc. ■ No requiere un escaneo de la red ■ No requiere agentes adicionales
	Criterios de Evaluación ● Examinar el tablero de mando y los reportes de la información proporcionada
	Preguntas por Hacer ● ¿Esta capacidad requiere un agente adicional? ● ¿Cómo se recoge esta información? ● ¿Cómo se integra esto con las demás capacidades del producto de seguridad para endpoints?

Supervise qué programas se están ejecutando en su ambiente	**Características Requeridas** ■ Enumere todas las aplicaciones que se utilizan en un endpoint y en todos los endpoints del ambiente ■ Puede identificar y buscar aplicaciones utilizadas en un host concreto o por usuarios específicos
	Criterios de Evaluación ● Evaluar el tablero de mando y los reportes de información sobre la aplicación suministrados
	Preguntas por Hacer ● ¿Esta capacidad requiere un agente adicional? ● ¿Cómo se recoge esta información? ● ¿Cómo se integra esto con las demás capacidades del producto de endpoint?

Tabla 5. Gestión de Vulnerabilidades e Higiene de TI: Casos de Uso y Capacidades Esenciales

EL ENFOQUE CROWDSTRIKE

CrowdStrike Falcon Discover™ Higiene de TI y CrowdStrike Falcon Spotlight™ Gestión de Vulnerabilidades permiten a las organizaciones cerrar las brechas de seguridad y estar mejor preparadas para hacer frente a las amenazas proporcionando conciencia y visibilidad en áreas clave de una infraestructura. Estas soluciones proporcionan una sólida visibilidad sobre las vulnerabilidades existentes, los activos, las aplicaciones y las cuentas que se utilizan en un ambiente. Al utilizar el agente Falcon, Falcon Spotlight es único en su capacidad de informar sobre las vulnerabilidades en tiempo real sin necesidad de escanear los endpoints, identificando qué parches se han aplicado con éxito frente a los que se acaban de desplegar. Con Falcon Discover, el personal de TI obtiene visibilidad en tiempo real sobre quién y qué hay en la red y puede identificar sistemas rogue, desprotegidos y no gestionados, como los sistemas "traiga su propio dispositivo" (BYOD, por sus siglas en inglés) o de terceros.

El inventario de aplicaciones en tiempo real dentro de Falcon Discover proporciona una visión de todas las aplicaciones que se ejecutan en el ambiente a través de un sencillo tablero de mando con opciones de desglose. Los equipos de seguridad pueden ver al instante qué aplicaciones se están ejecutando actualmente en qué hosts sin afectar a los endpoints. También pueden determinar cuándo se lanzó la aplicación originalmente y pivotar a otros endpoints que ejecutan la misma aplicación para obtener más contexto encontrando el uso por aplicación o por host. Falcon Discover también supervisa y proporciona visibilidad de las tendencias de inicio de sesión (actividades/duración) en todo el ambiente, siempre que se utilicen credenciales existentes o se creen nuevas credenciales de administrador. Esto permite a los equipos de seguridad detectar y mitigar el abuso de credenciales y los ataques que emplean credenciales robadas.

En general, con Falcon Spotlight y Falcon Discover, recibirá una gestión integral de las vulnerabilidades con una supervisión continua, junto con el componente de higiene de TI necesario para mejorar la postura de seguridad general. Con estas soluciones, su organización estará mejor preparada para repeler los ataques y detener una falla.

ARQUITECTURA NATIVA EN LA NUBE PARA HABILITAR LOS ELEMENTOS CRÍTICOS DE LA SEGURIDAD DE LOS ENDPOINTS

A medida que las organizaciones crecen y añaden más endpoints distribuidos, las soluciones para endpoints locales pueden volverse rápidamente muy complejas y tardar meses en implantarse y ser plenamente operativas. Al poco tiempo, parece que toda la infraestructura debe actualizarse para garantizar que funciona con el máximo nivel de protección, o que hay que añadir un componente diferente para protegerse contra un nuevo tipo de amenaza. A menudo, esto obliga a empezar de nuevo todo el procedimiento de implantación, dejando entretanto lagunas en su protección.

Las implantaciones híbridas con componentes distribuidos entre las instalaciones y la nube pueden parecer una opción lógica, pero introducen desafíos. La sobrecarga de la infraestructura continúa si se requiere algún componente de gestión en las instalaciones. El control de versiones aumenta rápidamente la complejidad e introduce brechas de seguridad, ya que las capacidades, la protección y las rutinas de actualización varían en la propiedad. Los repositorios de datos descentralizados limitan las capacidades de detección y respuesta.

La nube nativa, por otro lado, ofrece un medio para proporcionar protección generalizada en toda la empresa de forma más rápida, a un costo menor y con una sobrecarga de gestión reducida, al tiempo que ofrece un rendimiento, agilidad y escalabilidad significativamente mayores. Sin hardware ni software adicional que adquirir, desplegar, gestionar y actualizar, el despliegue de la seguridad de los endpoints desde la nube resulta rápido y sencillo. Mientras que los sistemas locales pueden tardar hasta un año en desplegarse por completo, las soluciones basadas en la nube pueden implantarse con éxito en ambientes con decenas de miles de hosts en cuestión de horas.

Además, las actualizaciones de la infraestructura se realizan en la nube, de forma inmediata, bajo la supervisión del proveedor, y no requieren meses de planificación que pueden dejar lagunas en la eficacia de la protección y agotar los recursos de los equipos de TI.

Otras ventajas de un modelo nativo en la nube son la capacidad de recopilar conjuntos de datos abundantes en tiempo real y de escalar bajo demanda, lo que permite almacenar petabytes de datos durante meses y analizar esos datos en segundos sin afectar a los endpoints. Todas estas son tareas extremadamente arduas que no son adecuadas para los modelos locales. Por último, las implantaciones en la nube son cruciales para proteger los sistemas remotos cuando están fuera de la red o de la VPN.

Una arquitectura de nube bien diseñada debe proporcionar las siguientes capacidades:

1. Ser inmediatamente operativa sin necesidad de configurar la infraestructura antes de la implantación
2. Escalar sin problemas a medida que se añaden endpoints y eventos, sin requerir la intervención del cliente
3. Reducir al mínimo el impacto en los endpoints (por ejemplo, no se requiere una base de datos en el endpoint para mantener los datos de los eventos, no se consumen recursos del endpoint cuando se realizan búsquedas o análisis)
4. Analizar los datos a una velocidad y volumen que proporcionen resultados rápidos y precisos

Las siguientes preguntas le ayudarán a descubrir las verdaderas capacidades que ofrece la arquitectura en la nube de una solución de protección de endpoints:

- ¿Cuánto tiempo tarda el producto en ser plenamente operativo?
- ¿Qué hardware y software adicionales -servidores (físicos o virtuales), dispositivos, licencias de bases de datos, etc. se necesitan para implantar el producto?
- ¿Es una verdadera arquitectura diseñada en la nube o un dispositivo virtualizado alojado en la nube?
- ¿El cliente necesita hacer algo si el número de endpoints crece o si añade ubicaciones adicionales al ambiente?
- ¿Cómo afecta la solución a los endpoints al espacio en disco, al uso de la CPU y a la utilización de la RAM?
- ¿Cómo se ven afectados los endpoints cuando se realizan búsquedas y se recogen eventos?
- ¿Cuántos eventos por segundo puede manejar la infraestructura de la nube?
- ¿Cuántos endpoints puede soportar la arquitectura?

La arquitectura nativa en la nube de la plataforma CrowdStrike Falcon fue diseñada e implementada desde el principio para aprovechar la potencia y la escala de la nube. Permite a CrowdStrike ofrecer un tiempo de valor inmediato, lo que significa que los clientes pueden estar en funcionamiento y totalmente operativos en horas, en lugar de las semanas o meses que suelen requerir las arquitecturas locales.

Además de permitir una implementación rápida y sencilla, con unos costos de mantenimiento y expansión extremadamente bajos, la arquitectura en la nube creada específicamente por CrowdStrike ofrece una serie de ventajas únicas y potentes que refuerzan la protección y reducen la complejidad.

Esta arquitectura es fundamental para la capacidad de CrowdStrike de recopilar, analizar y almacenar billones de eventos a la semana, lo que sería casi imposible de conseguir con una arquitectura in situ. El modelo de nube de seguridad de CrowdStrike, una de las mayores arquitecturas de la nube en el mundo, está diseñado para almacenar y analizar un gran y creciente volumen de datos. Proporciona una visibilidad completa en tiempo real y una visión de todo lo que ocurre en sus endpoints, cargas de trabajo y contenedores en todo su ambiente. Utilizando un potente análisis de gráficos para explorar miles de millones de eventos en tiempo real, CrowdStrike Threat Graph establece vínculos entre los eventos de seguridad en toda la comunidad global de agentes Falcon para detectar y prevenir inmediatamente la actividad de los adversarios, a escala y con una velocidad sin precedentes. Cuando se descubre una nueva amenaza a nivel local en un ambiente, todos los clientes se benefician de la inteligencia impulsada por la comunidad de CrowdStrike de forma inmediata gracias a la capacidad de Threat Graph para analizar los datos a escala de la nube y tomar las medidas más eficaces para proteger a todos los clientes. De este modo, Threat Graph dota a los clientes de CrowdStrike de un nivel extraordinario de protección contra las fallas.

La plataforma Falcon está diseñada como una solución altamente modular y extensible que utiliza un único agente ligero. Esto garantiza que los clientes puedan resolver nuevos retos de seguridad con un solo clic, sin necesidad de volver a crear o rediseñar la solución, lo que elimina la fricción asociada a los despliegues de seguridad.

CONCLUSIÓN

Puede parecer difícil ver la diferencia entre los proveedores, pero cuando se mira más allá del revuelo publicitario, se puede ver que sólo CrowdStrike ofrece las capacidades esenciales de protección de endpoints:

1. **Prevención** para mantener fuera el mayor número posible de elementos maliciosos
2. **Detección** para encontrar y eliminar a los atacantes
3. **La Cacería Gestionada de Amenazas** para elevar la detección más allá de la automatización
4. **Integración de la información sobre amenazas** para comprender y adelantarse a los atacantes
5. **Gestión de la vulnerabilidad e higiene de TI** para preparar y reforzar el ambiente contra las amenazas y los ataques

CrowdStrike habilita y ofrece de forma única estos elementos a través de una arquitectura nativa en la nube para satisfacer la velocidad, la flexibilidad y la capacidad necesarias para defenderse de los atacantes modernos y detener brechas. Ofrece un único agente ligero para la prevención, la detección, la cacería de amenazas, la respuesta, la remediación, la gestión de vulnerabilidades y la Higiene de TI. La opción también está disponible para ser totalmente gestionada 24/7, por los expertos en seguridad de CrowdStrike, a través de la seguridad gestionada para endpoints CrowdStrike Falcon Complete™, que cuenta con una garantía de hasta 1 millón de dólares.

ACERCA DE CROWDSTRIKE

CrowdStrike, líder mundial en ciberseguridad, está redefiniendo la seguridad para la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las fallas. La arquitectura de agente único y ligero de la plataforma CrowdStrike Falcon® se apalanca en la inteligencia artificial (IA) a escala de la nube y ofrece protección y visibilidad en tiempo real en toda la empresa, impidiendo los ataques a los endpoints dentro y fuera de la red. Impulsado por el CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona más de 5 billones de eventos relacionados con endpoints por semana en tiempo real desde todo el mundo, impulsando una de las plataformas de datos más avanzadas del mundo para la seguridad.

Con CrowdStrike, los clientes se benefician de una mejor protección, un mejor rendimiento y un tiempo de valor inmediato, gracias a la plataforma Falcon nativa en la nube.

Sólo hay que recordar una cosa sobre CrowdStrike: **Detenemos las brechas.**

Inicie su Prueba Gratuita
del Antivirus de Última Generación

Conozca más en **www.crowdstrike.com**

COMPAS SOLUTIONS