COMPAS SOLUTIONS

CROWDSTRIKE
Ebook

CINCO CAPACIDADES ESENCIALES DE LA SEGURIDAD MODERNA PARA ENDPOINTS

Por qué la visibilidad total contribuye a una mejor protección

En los endpoints, lo que no se ve *sí* existe

Cada día más empresas trasladan más aplicaciones, infraestructura y datos a la nube. El número de endpoints que accede a ellos se dispara. Un endpoint es cualquier dispositivo que se pueda conectar a una red, incluidos computadoras, portátiles, teléfonos móviles, tablets y servidores, así como cualquier otro dispositivo que se pueda conectar a Internet (Internet de las cosas o IoT). Por eso, el endpoint se considera una de las mayores fuentes de riesgos para cualquier empresa.

La falta de visibilidad y escalabilidad en este entorno expansivo plantea un serio desafío para los equipos de seguridad y TI encargados de la protección de los endpoints, y ahí, los sistemas de seguridad antiguos no sirven realmente de ayuda. Estas soluciones, desarrolladas en un principio para identificar archivos de malware conocido, no se diseñaron en ningún momento para escalarse y ofrecer el nivel de visibilidad necesario para proteger el entorno expansivo actual, objetivo de agresores que emplean **malware sin archivos**, aprovechan las vulnerabilidades de las plataformas y las aplicaciones, roban y utilizan ilícitamente identidades, e inyectan **amenazas persistentes avanzadas**.

La complejidad se alía con el agresor. Tener visibilidad y control de lo que está pasando en los endpoints es difícil, cuando no imposible, por muchos motivos, debido principalmente al creciente número de endpoints que cambian de ubicación con frecuencia. Los ciberdelincuentes aprovechan las lagunas de seguridad derivadas de una visibilidad insuficiente y una falta de control para sacar partido de la situación.

¿Qué hace falta para que los equipos de seguridad y TI protejan los endpoints con agilidad, eficiencia y eficacia?

La protección de endpoints moderna requiere una visibilidad total

Una protección de endpoints verdaderamente eficaz debe proporcionar el máximo nivel posible de seguridad, pero también ser fácil de utilizar. La complejidad sobrecarga a los equipos y los procesos, e introduce lagunas de seguridad que incrementan el riesgo de que disminuya la productividad y se dañe la reputación de una empresa.

Para conseguir tanto seguridad como simplicidad, la protección de los endpoints debe incluir cinco elementos clave:

1. **Prevención** para impedir la entrada del mayor número posible de agentes maliciosos.
2. **Detección** para buscar y eliminar ciberdelincuentes.
3. **Threat hunting gestionado** para llevar la detección más allá de las defensas automatizadas.
4. **Inteligencia sobre amenazas** para conocer a los atacantes y anticiparse a sus movimientos.
5. **Gestión de vulnerabilidades e higiene de TI** para preparar y reforzar el entorno frente a amenazas y ataques.

Estas cinco capacidades solo se pueden implementar, integrar y ofrecer a través de una plataforma nativa de la nube que simplifique las operaciones de seguridad y cumpla los requisitos de velocidad, flexibilidad y escalabilidad necesarios para defenderse de las amenazas más sofisticadas de hoy en día.

Prevención: cierre la puerta a los ciberdelincuentes

La protección de endpoints tradicional centrada en el malware —como las soluciones antivirus— suele ser eficaz únicamente frente al malware conocido. Además, dado el aumento de las tácticas cada vez más sofisticadas sin archivos ni malware, resulta insuficiente ante el panorama de amenazas actual.

Los equipos de seguridad y TI necesitan la inteligencia de una solución **antivirus de nueva generación (NGAV)** capaz de reconocer y evitar malware conocido y de día cero, ransomware, y ataques sin archivos y sin malware. Las soluciones NGAV avanzadas pueden emplear análisis de comportamiento para buscar automáticamente indicios de ataque y bloquearlos mientras suceden.

A diferencia de las soluciones de seguridad antiguas, que requieren actualizaciones diarias que dejan desprotegidos temporalmente los endpoints, las soluciones NGAV pueden utilizar aprendizaje automático para mantener la seguridad actualizada, sin sobrecargar a los equipos de seguridad y TI. Las mejores soluciones NGAV combinan estas y otras técnicas avanzadas que proporcionan la visibilidad y el contexto necesarios para evitar que las tácticas, técnicas y procedimientos (TTP) de ataque modernos logren su objetivo.

No obstante, como bien sabe todo equipo de seguridad experimentado, hasta la mejor estrategia de prevención es insuficiente frente a los ciberdelincuentes sofisticados y con amplios recursos económicos de hoy día. La solución más segura para una empresa pasa por combinar la prevención con una estrategia de detección sólida para identificar y bloquear cualquier ataque furtivo que consiga acceder.

MÁS ALLÁ DEL MALWARE

En un estudio reciente, se concluyó que el 68 % de las detecciones realizadas desde abril hasta junio de 2021 no estaban basadas en malware. Cada vez es más frecuente que los atacantes intenten lograr sus objetivos sin copiar malware en el endpoint, usando credenciales legítimas y herramientas incorporadas (es decir, recursos que ya existen en el entorno de la víctima). Todo esto responde a un esfuerzo deliberado para evitar ser detectados por los antivirus convencionales. FUENTE: CROWDSTRIKE INFORME DE THREAT HUNTING 2021

Detección: halle y elimine a los ciberdelincuentes que consigan colarse

Cuando los ciberdelincuentes consiguen un primer acceso sin que se disparen las alarmas, pueden permanecer silenciosamente en un entorno y provocar daños durante días, semanas o incluso meses, sin ser advertidos.

Las soluciones de detección y respuesta para endpoints (EDR) con funciones de prevención bien integradas proporcionan la visibilidad que necesitan los equipos de seguridad para descubrirlos lo más rápido posible. Para ello, una solución EDR debe registrar todas las actividades de interés de un endpoint para someterlas a una inspección exhaustiva, tanto en tiempo real como a posteriori, y completar estos datos con inteligencia sobre amenazas, con el fin de suministrar el contexto necesario para el threat hunting y la investigación de las amenazas.

Los equipos de seguridad no deberían tener que dedicar tiempo a escribir y ajustar las reglas de detección. Una solución EDR eficaz cuenta con inteligencia para detectar automáticamente actividades maliciosas y presentar a los equipos ataques reales, sin distraerlos con falsos positivos y actividades lícitas. Mediante acciones de respuesta eficaces, los equipos pueden contener e investigar sistemas comprometidos, incluido el acceso remoto sobre la marcha, para tomar medidas inmediatas y detener la intrusión de raíz.

Aunque las soluciones EDR avanzadas pueden detectar ataques furtivos y descubrir amenazas que hayan conseguido eludir los sistemas de prevención, las empresas pueden dar un paso aún más proactivo para proteger los endpoints: incorporar threat hunters.

DEMASIADO INTELIGENTES PARA LAS SOLUCIONES ANTIVIRUS TRADICIONALES

A finales de 2021, se produjo un ataque contra la cadena de suministro de un conocido paquete de software —con más de 7 millones de descargas semanales de la biblioteca npm— que consiguió comprometerlo y utilizarlo para distribuir mineros de criptomonedas y ladrones de contraseñas. La mejor defensa frente a este tipo de ataque es la detección de los indicadores de ataque (IOA), basada en el comportamiento, para identificar y bloquear el malware distribuido a través de la biblioteca vulnerada. Esta detección se basa en la inteligencia obtenida gracias a la monitorización continua de las TTP empleados por grupos desconocidos y ciberdelincuentes. FUENTE: "COMPROMISED NPM PACKAGE USED IN SUPPLY CHAIN ATTACK", BLOG DE CROWDSTRIKE, 26 DE OCTUBRE DE 2021

Threat hunting gestionado: eleve la detección más allá de las defensas automáticas

El **threat hunting** permite a las empresas aplicar un enfoque humano y proactivo para buscar activamente actividades sospechosas, en lugar de confiar únicamente en la tecnología, para detectar y avisar de manera automática de la actividad de un posible ciberdelincuente.

El threat hunting gestionado sirve de ayuda a empresas que carecen de recursos y expertos en seguridad para descubrir a los ciberdelincuentes e impedir que las amenazas avanzadas acechen silenciosamente su entorno. Un equipo de threat hunting experimentado puede monitorizar su entorno de manera ininterrumpida para detectar actividades furtivas maliciosas.

Los equipos de threat hunting gestionado analizan las amenazas y trabajan codo con codo con el personal interno para guiarle desde la detección hasta la respuesta. Esta interacción con expertos eleva el nivel de sofisticación de los equipos de seguridad y TI internos, no solo en ese preciso momento, sino también a la larga.

Los threat hunters adoptan un enfoque proactivo en cuanto a la protección de endpoints, gracias a sus años de experiencia. Al tener visibilidad del estado de los endpoints y acceso a la inteligencia adecuada sobre amenazas, no solo son capaces de entender lo que observan, sino que pueden también anticiparse a las ciberamenazas contra la empresa.

Inteligencia sobre amenazas: conozca y anticípese a los ataques

Los agresores se mueven con tanta rapidez y sigilo que a las tecnologías y los profesionales de la seguridad les resulta difícil seguir el ritmo de las últimas amenazas y protegerse de ellas con antelación. Para responder con la misma celeridad, las soluciones de seguridad de endpoints deben incorporar siempre inteligencia sobre amenazas o tener la capacidad de integrar inteligencia de terceros.

La **inteligencia sobre amenazas** debe cumplir los siguiente requisitos:

- Proporcionar información práctica que permita a los equipos de seguridad y a las soluciones que ellos utilizan comprender, responder y solucionar incidentes de manera más rápida, para agilizar las investigaciones y la corrección de los incidentes.
- Generar y priorizar alertas que ayuden a los equipos de seguridad a comprender mejor las tácticas y las campañas asociadas a determinados ciberdelincuentes.
- Estar integrada a la perfección en la solución de protección de endpoints, de modo que esté al alcance de los equipos de seguridad y TI. Los equipos no deberían tener que cambiar manualmente entre las distintas soluciones de seguridad, sino que deben ser capaces de ver el contexto de una alerta y limitarse a hacer clic para desplazarse a otra pantalla con información más detallada.

La capacidad de entender y predecir ataques mediante la inteligencia sobre amenazas es un elemento clave de la preparación de una empresa a la hora de enfrentarse a ataques avanzados. Además, la gestión de las vulnerabilidades y la higiene de TI refuerzan las defensas aún más.

Gestión de vulnerabilidades e higiene de TI: refuerce su entorno frente a los ataques

La **gestión de vulnerabilidades** y la higiene de TI ofrecen la visibilidad y la información práctica que los equipos de seguridad y TI necesitan para comprender qué sistemas y aplicaciones están en riesgo, así como qué y quiénes están activos en el entorno.

Para que la gestión de las vulnerabilidades sea eficaz, se requiere una monitorización continua de todos los endpoints a fin de identificar los puntos débiles de seguridad dondequiera que se encuentren, ya sea en las instalaciones o fuera de ellas. Para garantizar que los sistemas de producción estén protegidos con parches actualizados, las empresas deben saber qué vulnerabilidades representan el nivel de riesgo más alto para la empresa y abordar las correcciones correspondientes.

A pesar de sus esfuerzos, inevitablemente, a las empresas les faltarán algunos parches y mitigaciones dado el constante aumento de las vulnerabilidades críticas. Dedicar a cada vulnerabilidad el tiempo necesario para mitigarla y responder para proteger el entorno es una tarea ingente, cuando no imposible. Las soluciones de higiene de TI monitorizan continuamente posibles cambios en los recursos, las aplicaciones y los usuarios, y ayudan a identificar los sistemas no gestionados o los que pueden comportar un riesgo para la red, como los dispositivos de terceros o los BYOD no protegidos.

Obtener visibilidad sobre las tendencias de inicio de sesión (por ejemplo, las actividades asociadas y la duración) en su entorno, dondequiera que se utilicen las credenciales y se creen las credenciales de administrador, permite a los equipos de seguridad detectar y mitigar el uso indebido de credenciales y los ataques basados en credenciales robadas.

La gestión de vulnerabilidades y la higiene de TI proporcionan a los equipos de seguridad la información que necesitan para adoptar una postura proactiva eficaz que mejore la estrategia de seguridad general y los coloque en una posición óptima para anticiparse a los adversarios y vencerles.

Dé el paso siguiente

En este ebook, se ha descrito lo que los equipos de seguridad y TI deben esperar de un enfoque exhaustivo de la protección de endpoints: prevención, detección, threat hunting gestionado, inteligencia sobre amenazas, y gestión de vulnerabilidades e higiene de TI.

Todos estos elementos juntos proporcionan una protección completa en toda la empresa, al tiempo que reducen la sobrecarga de administración y mejoran de forma significativa el rendimiento, la agilidad y la escalabilidad.

Estas cinco capacidades esenciales de la seguridad de endpoints moderna solo se pueden implementar, integrar y ofrecer a través de una plataforma nativa de la nube que simplifique las operaciones de seguridad y se ajuste a la velocidad, la flexibilidad y la competencia necesarias para defenderse frente a los ciberdelincuentes modernos.

¿Está preparado para encontrar una solución que proporcione una protección de endpoints robusta que cuente con estas cinco capacidades esenciales?

- **Consulte esta infografía** para entender rápidamente las diferencias entre la protección de endpoints tradicional y la moderna.
- **Descubra cómo** la protección de endpoints nativa de la nube de CrowdStrike proporciona la visibilidad necesaria para implementar las cinco capacidades esenciales que necesitan las empresas para adoptar una posición sólida en materia de seguridad.

ACERCA DE CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con una de las plataformas nativas de la nube más avanzadas 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, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa para facilitar detecciones hiperprecisas, protección y corrección 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 permite que los clientes se beneficien de un despliegue rápido y escalable, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: **We stop breaches.**

Más información: **https://www.crowdstrike.com/latam/**

Síganos: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Empiece una prueba gratuita hoy mismo: **https://go.crowdstrike.com/try-falcon-prevent-es**

COMPAS SOLUTIONS