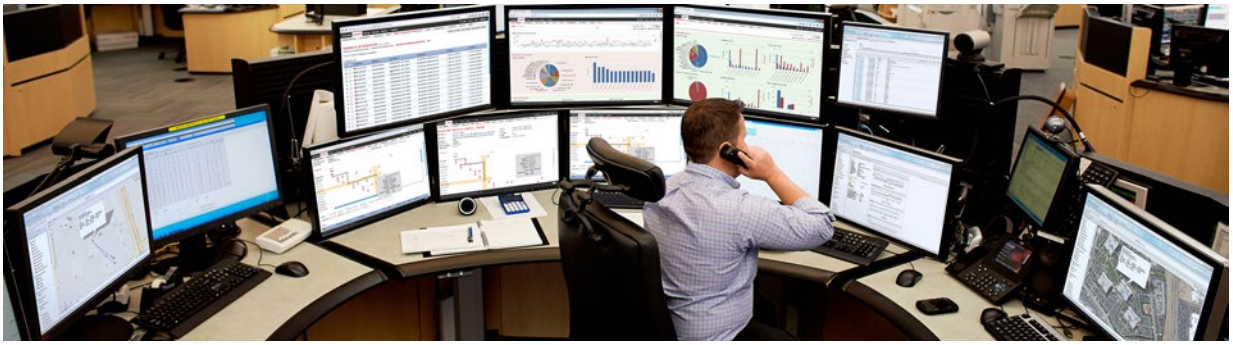

Cisco Advanced Malware Protection

Prevención y detección de violaciones, respuesta y corrección para el mundo real

BENEFICIOS

- Accede a una inteligencia inigualable sobre amenazas globales para fortalecer las defensas de primera línea
- Obtiene visibilidad profunda sobre el origen y el alcance de un riesgo
- Logra la detección, la respuesta y la corrección del malware con rapidez
- Evita las costosas situaciones de reinfección y su corrección
- Obtiene protección en cualquier lugar: en la red, en los terminales, en los dispositivos móviles, en el correo electrónico y en la Web; antes, durante y después

El malware avanzado de la actualidad es sigiloso, persistente y capaz de evadir las defensas tradicionales. Los equipos de seguridad afrontan el desafío de defenderse de estos ataques, ya que sus tecnologías de seguridad no proporcionan la visibilidad y el control necesarios para detectar y eliminar rápidamente las amenazas antes de sufrir los daños.

Las organizaciones sufren ataques y las violaciones a la seguridad son noticia constantemente. Hoy en día, la comunidad mundial de piratas cibernéticos crea malware avanzado y lo lanza a las organizaciones a través de diversos vectores de ataque. Estos ataques polifacéticos y dirigidos pueden evadir incluso las mejores herramientas de detección en un determinado momento. Estas herramientas realizan una inspección del tráfico y de los archivos al momento de ingreso en la red, pero proporcionan poca visibilidad de la actividad de las amenazas que logran evadir la detección inicial. Por ese motivo, los profesionales de seguridad no perciben el alcance de un posible riesgo para contener el malware y responder con rapidez, antes de que cause daños significativos.

La Protección contra malware avanzado (AMP) de Cisco es una solución de seguridad que aborda el ciclo de vida completo de los problemas relacionados con el malware avanzado. No solo evita violaciones, sino que también brinda visibilidad y control para detectar, contener y corregir las amenazas con rapidez cuando evaden las defensas de primera línea; todo de un modo rentable y sin afectar la eficacia operativa.

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Descripción general de Cisco Advanced Malware Protection

AMP es una solución empresarial inteligente, integrada de protección y análisis de malware avanzado. Usted obtiene una protección completa para su organización en todo el curso del ataque: antes, durante y después.

- **Antes** de un ataque, AMP utiliza la inteligencia sobre amenazas globales provista por Collective Security Intelligence de Cisco, Talos Security Intelligence and Research Group y la inteligencia sobre amenazas de AMP Threat Grid contribuye al refuerzo de las defensas y a la protección contra amenazas conocidas y emergentes.
- **Durante** un ataque, AMP utiliza esta inteligencia en conjunto con firmas de archivo conocidas y la tecnología de análisis de malware dinámico de Cisco AMP Threat Grid para identificar y bloquear los tipos de archivo que violan las políticas, los intentos de vulnerabilidad y los archivos maliciosos que intentan infiltrarse en la red.
- **Después** de un ataque o después de la inspección inicial de un archivo, la solución va más allá de las funcionalidades de detección en un momento determinado; analiza y controla constantemente toda la actividad y el tráfico de archivos, independientemente de su condición, y apunta a detectar cualquier indicador de conducta maliciosa. Si un archivo con una condición desconocida o que anteriormente se consideró “buena” comienza a comportarse mal, AMP lo detectará e inmediatamente generará una alerta para los equipos de seguridad con un indicador del riesgo. Luego proporciona visibilidad inigualable sobre el lugar de origen del malware, los sistemas que se vieron afectados y la actividad del malware. También ofrece controles para responder rápidamente a la intrusión y para corregirla en pocos pasos. Esto proporciona a los equipos de seguridad el nivel de visibilidad y control profundos que necesitan para detectar rápidamente los ataques, evaluar el alcance de un riesgo y contener el malware antes de que cause daño.

Inteligencia sobre amenazas globales y análisis de malware dinámico

AMP se basa en una inteligencia de seguridad inigualable y en el análisis de malware dinámico. El ecosistema de Cisco Collective Security Intelligence, Talos Security Intelligence and Research Group y los aportes de la inteligencia sobre amenazas de AMP Threat Grid representan la recopilación líder del sector de análisis de datos masivos e inteligencia sobre amenazas en tiempo real. Posteriormente, estos datos se envían de la nube al cliente AMP a fin de ofrecerle la inteligencia sobre amenazas más actualizada para defenderse de ellas de manera proactiva. Los beneficios que obtienen las organizaciones son los siguientes:

- 1,1 millones de muestras entrantes de malware por día
- 1,6 millones de sensores globales
- 100 TB de datos recibidos por día
- 13 mil millones de solicitudes web
- 600 ingenieros, técnicos e investigadores
- Operaciones durante todo el día

AMP correlaciona los archivos, el comportamiento, los datos de telemetría y la actividad con esta base de conocimientos sólida y rica en contexto para detectar el malware con rapidez. Los equipos de seguridad se benefician del análisis automático de AMP gracias al ahorro de tiempo destinado a la búsqueda de actividades de violación y al constante acceso a la inteligencia sobre amenazas más actualizada, a fin de establecer un orden de prioridades, comprender y bloquear los ataques complejos.

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

La integración de nuestra tecnología Threat Grid con AMP también proporciona las siguientes ventajas:

- Aportes de inteligencia de gran precisión y contexto presentados en formatos estándar para que se integren sin inconvenientes con las tecnologías de seguridad existentes
- Análisis de millones de muestras por mes, en comparación con más de 350 indicadores de comportamiento, lo que deriva en miles de millones de medios
- Calificación simple de las amenazas para que los equipos de seguridad puedan establecer un orden de prioridad

AMP utiliza la totalidad de la inteligencia y el análisis para brindarle información útil en la toma de decisiones en materia de seguridad o bien para tomar medidas automáticamente en su nombre. Por ejemplo, gracias a una inteligencia que se actualiza constantemente, el sistema puede bloquear el malware conocido y los tipos de archivos que violan las políticas, crear de manera dinámica listas negras de conexiones que se consideran maliciosas y bloquear los intentos de descarga de archivos desde sitios web y dominios clasificados como maliciosos.

Análisis ininterrumpido y seguridad retrospectiva

La mayoría de los sistemas contra malware basados en terminales y en la red examinan los archivos solo cuando atraviesan un punto de control para ingresar a su red extendida. Allí acaba el análisis. Sin embargo, el malware es complejo y logra evadir muy bien la detección inicial. Las técnicas de suspensión, el polimorfismo, el cifrado y el uso de protocolos desconocidos son solo algunas de las formas en las que el malware puede ocultarse y evitar su detección. Usted no puede defenderse de algo que no ve y así ocurren la mayoría de las principales violaciones a la seguridad. Los equipos de seguridad no ven la amenaza al momento de ingreso y desconocen su presencia posteriormente. No tienen visibilidad para detectarla o contenerla rápidamente y en poco tiempo el malware logra sus objetivos y causa daño.

Cisco AMP es diferente. Ante el reconocimiento de que los métodos preventivos de detección y bloqueo en un momento determinado no son 100% eficaces, el sistema AMP analiza constantemente los archivos y el tráfico, incluso después de la inspección inicial. AMP controla, analiza y registra todas las comunicaciones y la actividad de los archivos en los terminales, en los dispositivos móviles y en la red con el objetivo de descubrir rápidamente las amenazas sigilosas que tienen un comportamiento sospechoso o malicioso. Ante el primer indicio de un problema, AMP generará una alerta retrospectiva destinada a los equipos de seguridad y proporcionará información detallada sobre el comportamiento de la amenaza. Entonces, usted puede responder preguntas cruciales en materia de seguridad, como las siguientes:

- ¿De dónde provino el malware?
- ¿Cuál fue el método y el punto de ingreso?
- ¿Dónde ha estado y qué sistemas se vieron afectados?
- ¿Qué actividad tuvo y tiene la amenaza?
- ¿Cómo detenemos la amenaza y eliminamos la causa?

Con esta información, los equipos de seguridad pueden comprender rápidamente lo que sucedió, además de utilizar la funcionalidad de contención y corrección de AMP para actuar. En pocos pasos, desde la consola de administración basada en el explorador fácil de usar de AMP, los administradores pueden contener el malware mediante el bloqueo del archivo para que nunca más pueda ejecutarse en otro terminal. Dado que AMP conoce todos los lugares en los que estuvo el archivo, puede extraer el archivo de la memoria y ponerlo en cuarentena para todos los demás usuarios. En caso de intrusión de malware, los equipos de seguridad ya no necesitan volver a crear una imagen del sistema completo para eliminar el malware. Esto lleva tiempo, cuesta dinero y supone recursos, además de interrumpir funciones empresariales importantes. Con AMP, la corrección del malware es quirúrgica, ni los sistemas de TI ni la empresa sufren daños colaterales asociados.

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Esta es la potencia del análisis ininterrumpido, de la detección continua y de la seguridad retrospectiva: la capacidad de registrar la actividad de cada archivo en el sistema y, si un archivo supuestamente “bueno” se vuelve “malicioso”, la capacidad de detectarlo y rebobinar el historial registrado para ver el origen de la amenaza y el comportamiento que tuvo. Posteriormente, AMP le ofrece funcionalidades incorporadas de respuesta y corrección para eliminar la amenaza. AMP también recuerda lo que ve, desde la firma de la amenaza hasta el comportamiento del archivo y registra los datos en la base de datos de inteligencia sobre amenazas de AMP a fin de fortalecer aún más las defensas de primera línea de tal modo que este archivo y otros similares no puedan volver a evadir la detección inicial.

Ahora los equipos de seguridad tienen el nivel de visibilidad y control profundos necesarios para detectar ataques con eficacia y descubrir el malware sigiloso; comprender y analizar el alcance de un riesgo; contener y corregir rápidamente el malware (incluso los ataques de día cero) antes de que puedan causar daño; además de evitar que se produzcan ataques similares.

Funciones principales

Las funcionalidades de análisis ininterrumpido y de seguridad retrospectiva de AMP son posibles gracias a estas sólidas funciones:

- **Indicadores de riesgo (IoC):** se correlacionan los eventos de telemetría y archivos y se plantean en un orden de prioridades como posibles violaciones activas. AMP correlaciona automáticamente los datos de eventos de seguridad de diversas fuentes, como eventos de malware e intrusiones, para que los equipos de seguridad puedan conectar los eventos con ataques coordinados de mayor magnitud, además de establecer un orden de prioridad de los eventos de alto riesgo.
- **Reputación de archivos:** se recopilan los análisis avanzados y la inteligencia colectiva a fin de determinar si un archivo está limpio o es malicioso, lo que permite una detección más precisa.
- **Análisis dinámico de malware:** un entorno muy seguro le permite ejecutar, analizar y poner a prueba el malware con el objetivo de detectar amenazas de día cero previamente desconocidas. La integración de la tecnología de análisis de malware dinámico y sandboxing de AMP Threat Grid en las soluciones de AMP redunda en un análisis más integral que se verifica en un conjunto más amplio de indicadores de comportamiento.
- **Detección retrospectiva:** se envían alertas cuando cambia la condición de un archivo después de un análisis extendido, lo que le brinda visibilidad y le permite reconocer el malware que evade las defensas iniciales.
- **Trayectoria del archivo:** realiza el seguimiento constante en el tiempo de la propagación de un archivo por todo su entorno a fin de lograr visibilidad y reducir el tiempo necesario para analizar el alcance de una violación de malware.
- **Trayectoria del dispositivo:** realiza el seguimiento constante de las comunicaciones y la actividad en los dispositivos y en el nivel del sistema para comprender rápidamente las causas y el historial de eventos que originaron un riesgo, además de los eventos posteriores.
- **Búsqueda elástica**: una búsqueda simple e ilimitada de datos de archivos, telemetría e inteligencia de seguridad colectiva le permite comprender rápidamente el contexto y el alcance de la exposición a un IoC o a una aplicación maliciosa.
- **Prevalencia:** muestra todos los archivos que se han ejecutado en toda su organización, ordenados de menor a mayor según su prevalencia, para ayudarlo a descubrir las amenazas que no fueron detectadas previamente, pero fueron percibidas por un pequeño grupo de usuarios. Los archivos ejecutados solo por unos pocos usuarios pueden ser aplicaciones maliciosas (por ejemplo, una amenaza avanzada dirigida y persistente) o aplicaciones cuestionables que posiblemente no desee tener en su red extendida.

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

- **IoC de terminales:** los usuarios pueden enviar sus propios IoC para capturar ataques dirigidos. Los IoC de terminales permiten que los equipos de seguridad desarrollen niveles más profundos de investigación de amenazas avanzadas menos conocidas que son específicas de las aplicaciones de su entorno.
- **Vulnerabilidades:** muestra una lista del software vulnerable de su sistema, los hosts que contienen ese software y los hosts que son más propensos a infectarse. Impulsado por el análisis de seguridad y la inteligencia sobre amenazas, AMP identifica el software vulnerable que es objeto de malware, la posible vulnerabilidad y arroja una lista de prioridades de hosts para revisar.
- **Control de ataques:** logra el control de archivos sospechosos o ataques y corrige una infección sin esperar una actualización de contenido. Características de la función de control de ataques:
  - Las detecciones simples personalizadas pueden bloquear rápidamente un archivo específico en todos los sistemas o en los sistemas que usted seleccione
  - Las firmas avanzadas personalizadas pueden bloquear las familias de malware polimórfico
  - Las listas de bloqueo de aplicaciones pueden aplicar políticas de aplicaciones o contener una aplicación en riesgo que se utiliza como gateway de malware y detener el ciclo de reinfección
  - Las listas blancas personalizadas permitirán garantizar que se sigan ejecutando las aplicaciones seguras, personalizadas y cruciales, bajo cualquier condición
  - La correlación del flujo de dispositivos detendrá las comunicaciones de devolución de malware en el origen, especialmente en el caso de terminales remotos fuera de la red corporativa

Opciones de implementación para la protección en todas partes

Los cibercriminales lanzan sus ataques a través de una variedad de puntos de ingreso a las organizaciones. Para lograr una verdadera eficacia a la hora de capturar ataques sigilosos, las organizaciones necesitan visibilidad sobre la mayor cantidad de vectores de ataque posibles. Por lo tanto, la solución AMP puede implementarse en diversos puntos de control en toda la red extendida. Las organizaciones pueden implementar la solución del modo y en el lugar que deseen para satisfacer sus necesidades de seguridad específicas. Las opciones son:

Nombre del producto	Detalles
Cisco AMP para terminales	Protección de PC, Mac, dispositivos móviles y entornos virtuales con el conector ligero de AMP, sin afectar el rendimiento de los usuarios.
Cisco AMP para redes	Implementa AMP como solución basada en la red integrada con los dispositivos de seguridad NGIPS FirePOWER™.
Cisco AMP en ASA con servicios FirePOWER	Implementa las funcionalidades de AMP integradas con el firewall Cisco ASA.
Dispositivo virtual de la nube privada Cisco AMP	Implementa AMP en las instalaciones como solución con aislamiento de aire, especialmente diseñada para organizaciones con requisitos elevados de privacidad que restringen el uso de una nube pública.
Cisco AMP en CWS, ESA o WSA	Las funcionalidades de AMP pueden activarse con el objetivo de proporcionar análisis de malware y funciones retrospectivas para Cisco Cloud Web Security (CWS), Email Security Appliance (ESA) o Web Security Appliance (WSA).
Cisco AMP Threat Grid	AMP Threat Grid se integra con Cisco AMP para realizar el análisis de malware dinámico mejorado. También puede implementarse como solución independiente de inteligencia sobre amenazas y análisis de malware dinámico.

¿Por qué Cisco?

Ya no cabe preguntarse si su organización será objeto de una violación o no; es una cuestión de tiempo. La detección en un momento determinado por sí sola no basta para garantizar una eficacia del 100% en la detección preventiva y el bloqueo de todos los ataques. El malware avanzado y sigiloso y los piratas cibernéticos que lo crean pueden vencer sus defensas en un momento determinado y poner en riesgo cualquier organización en cualquier momento. Incluso si bloquea el 99% de las amenazas, con una sola alcanza para generar una violación a la seguridad. Por lo tanto, en caso de violación, las organizaciones deben estar preparadas y contar con herramientas que detecten rápidamente una intrusión, responder a ella y corregirla.

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Cisco AMP es una solución integrada de protección y análisis de malware avanzado de clase empresarial, que está impulsada por servicios de inteligencia. Proporciona inteligencia sobre amenazas globales para reforzar las defensas de la red, ofrece motores de análisis dinámico para bloquear los archivos maliciosos en tiempo real y tiene la capacidad de controlar y analizar constantemente todo el comportamiento y el tráfico de los archivos. Estas funcionalidades brindan un nivel de visibilidad inigualable sobre la actividad de las posibles amenazas y, luego, el control necesario para detectar, contener y eliminar rápidamente el malware. Usted obtiene protección antes, después de un ataque y en el transcurso de este. La solución también puede implementarse en toda la empresa extendida: en la red, los terminales, los dispositivos móviles, el correo electrónico, las gateway de la web y los entornos virtuales, para que su organización pueda mejorar la visibilidad en los puntos de ingreso de ataques cruciales e implementar la solución del modo y en el lugar que desee a fin de satisfacer sus necesidades de seguridad específicas.

Pasos siguientes

Para obtener más información sobre Cisco AMP o ver demostraciones de productos, testimonios de clientes y validaciones de terceros, visite http://www.cisco.com/go/amp.

Sede central en América
Cisco Systems, Inc.
San José CA

Sede Central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Holanda

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y los números de fax están disponibles en el sitio web de Cisco en **www.cisco.com/go/offices**.

Cisco y el logotipo de Cisco son marcas comerciales o marcas comerciales registradas de Cisco y/o sus filiales en los Estados Unidos y otros países. Para ver una lista de las marcas registradas de Cisco, visite la siguiente URL: www.cisco.com/go/trademarks. Las marcas comerciales de terceros mencionadas en este documento pertenecen a sus respectivos propietarios. El uso de la palabra "partner" no implica que exista una relación de asociación entre Cisco y otra empresa. (1110R)

Impreso en EE. UU. C22-734228-00 04/15

© 2015 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.