Protección frente a malware avanzado de Cisco

Prevención, detección, respuesta y remediación de las brechas de seguridad en el mundo real

VENTAJAS

- Obtenga una inteligencia de amenazas global sin precedentes para reforzar las defensas de primera línea
- Obtenga una visibilidad detallada del origen y el alcance de un riesgo
- Detecte, responda y remedie rápidamente los problemas de malware
- Evite las costosas situaciones de reinfección y corrección
- Protección en cualquier lugar: en la red, los terminales, los dispositivos móviles, el correo electrónico y la Web, antes, durante y después de un ataque

El malware avanzado de hoy en día es sigiloso, persistente y puede eludir los sistemas de defensa tradicionales. Los equipos de seguridad se enfrentan al reto de protegerse de estos ataques porque sus tecnologías de seguridad no proporcionan la visibilidad y el control necesarios para detectar y eliminar rápidamente las amenazas antes de que se produzcan daños.

Las organizaciones reciben ataques con frecuencia, y los casos de brechas de seguridad aparecen constantemente en los titulares. La comunidad global actual de hackers crea malware avanzado y lo introduce en las organizaciones a través de un amplio abanico de vectores de ataque. Estos ataques polifacéticos y dirigidos pueden eludir incluso las mejores herramientas de detección centradas en un momento específico. Estas herramientas examinan el tráfico y los archivos en el punto de entrada de la red, pero ofrecen poca visibilidad de la actividad de las amenazas que consiguen eludir la detección inicial. Esto impide a los profesionales de la seguridad determinar el alcance de un riesgo potencial, así como frenar el malware antes de que provoque daños significativos.

La protección frente a malware avanzado (AMP) de Cisco es una solución de seguridad que responde a cada una de las necesidades que surgen durante todo el ciclo de vida del problema que supone el malware avanzado. No solo permite evitar brechas de seguridad, sino que proporciona la visibilidad y el control necesarios para detectar, frenar y remediar rápidamente las amenazas si eluden las defensas de primera línea, todo ello de manera rentable y sin afectar a la eficiencia operativa.

Descripción general de la protección frente a malware avanzado de Cisco

AMP es una solución de protección y análisis de malware avanzado integrada, basada en inteligencia y de clase empresarial. Proporciona protección completa para su organización a lo largo de todo el ciclo de ataque: antes, durante y después de un ataque.

- **Antes** de un ataque, AMP utiliza la inteligencia de amenazas global Collective Security Intelligence de Cisco, el Security Intelligence and Research Group de Talos y las fuentes de información sobre inteligencia de amenazas de AMP Threat Grid para reforzar las defensas y proteger los sistemas frente a las amenazas conocidas y emergentes.
- **Durante** el ataque, AMP utiliza esa inteligencia junto con las firmas conocidas de archivo y la tecnología de análisis dinámico de malware AMP Threat Grid de Cisco para identificar y bloquear los tipos de archivo que infringen las políticas y pretenden aprovecharse de las vulnerabilidades, y los archivos maliciosos que intentan infiltrarse en la red.
- **Después** del ataque o después de la inspección inicial de un archivo, la solución va más allá de las funciones de detección centradas en un momento específico, y supervisa y analiza de manera continua toda la actividad y el tráfico de los archivos, independientemente de su disposición, buscando cualquier indicio de comportamiento malicioso. Si un archivo con una disposición desconocida o que anteriormente era “buena” comienza a comportarse de forma inadecuada, AMP lo detectará y alertará inmediatamente a los equipos de seguridad con una indicación de riesgo potencial. A continuación, ofrece una visibilidad sin precedentes sobre dónde se ha originado el malware, que sistemas se han visto afectados y qué está haciendo dicho malware. También proporciona controles para responder rápidamente a las intrusiones y corregirlas con unos pocos clics. Esto ofrece a los equipos de seguridad el nivel profundo de visibilidad y control que necesitan para detectar rápidamente los ataques, determinar el alcance de un riesgo y frenar el malware antes de que se produzcan daños.

Inteligencia de amenazas global y análisis dinámico de malware

AMP se basa en una inteligencia de amenazas global y un análisis dinámico de malware sin precedentes. El ecosistema Collective Security Intelligence de Cisco, el Security Intelligence and Research Group de Talos y las fuentes de información sobre inteligencia de amenazas de AMP Threat Grid representan el conjunto de inteligencia de amenazas y análisis de Big Data en tiempo real líder del sector. Estos datos pasan de la nube al cliente AMP para que cuente con la última inteligencia de amenazas para defenderse de manera proactiva frente a las mismas. Las ventajas que obtienen las organizaciones son:

- 1,1 millones de muestras entrantes de malware al día
- 1,6 millones de sensores globales
- 100 TB de datos al día
- 13 000 millones de solicitudes web
- 600 ingenieros, técnicos e investigadores
- Operaciones durante todo el día

AMP correlaciona archivos, comportamientos, datos de telemetría y actividades con esta sólida base de conocimientos que se complementa con información de contexto para detectar rápidamente el malware. Los equipos de seguridad se benefician del análisis automatizado de AMP, ya que ahorra tiempo a la hora de buscar actividades infractoras y proporciona la inteligencia frente amenazas más actual en todo momento para analizar, priorizar y bloquear rápidamente los ataques sofisticados.

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

- Fuentes de información de gran precisión y con información de contexto en formatos estándar para lograr una perfecta integración con las tecnologías de seguridad actuales.
- Análisis de millones de muestras cada mes y comparación de las mismas con más de 350 indicadores de comportamiento, lo que genera miles de millones de artefactos.
- Una puntuación sencilla de las amenazas para ayudar a los equipos de seguridad a priorizarlas.

AMP utiliza toda esta inteligencia y los análisis para informar al responsable de la toma de decisiones de seguridad o para tomar las medidas necesarias de manera automática en su nombre. Por ejemplo, al contar con una inteligencia constantemente actualizada, el sistema puede bloquear el malware conocido y los tipos de archivo que infringen las políticas, poner en la lista negra las conexiones que han sido identificadas como maliciosas de manera dinámica y bloquear los intentos de descargar archivos de sitios web y dominios categorizados como maliciosos.

Análisis continuo y seguridad retrospectiva

La mayoría de sistemas antimalware basados en la red y los terminales examinan los archivos solo en el momento en que atraviesan un punto de control de la red extendida. A partir de ahí, el análisis se detiene. Pero el malware es cada vez más sofisticado y se ha vuelto muy habilidoso para eludir esta detección inicial. Las técnicas de suspensión, el polimorfismo, el cifrado y el uso de protocolos desconocidos son solo algunas de las estrategias que se utilizan para que el malware pase desapercibido. Uno no puede defenderse de algo que no puede ver y así es cómo se producen la mayoría de las brechas de seguridad importantes. Los equipos de seguridad no ven estas amenazas en el momento de entrada y, en consecuencia, desconocen su presencia en el sistema una vez han conseguido acceder. No cuentan con la visibilidad necesaria para detectarlas y frenarlas rápidamente y, al poco tiempo, el malware ha cumplido su objetivo y ha producido daños.

Cisco AMP es diferente. La determinación del momento específico de entrada, la detección preventiva y los métodos de bloqueo no son eficaces al 100%, por lo que AMP analiza continuamente los archivos y el tráfico incluso después la inspección inicial. AMP supervisa, analiza y registra todas las actividades de los archivos y las comunicaciones en los terminales, los dispositivos móviles y la red para descubrir rápidamente las amenazas sigilosas que muestran un comportamiento sospechoso o malicioso. Al primer síntoma de problemas, AMP avisa retrospectivamente a los equipos de seguridad y proporciona información detallada sobre el comportamiento de la amenaza para que se pueda dar respuesta a las preguntas de seguridad esenciales como, por ejemplo:

- ¿De dónde proviene el malware?
- ¿Cuál fue el método y el punto de entrada?
- ¿Dónde ha estado y a qué sistemas ha afectado?
- ¿Qué ha hecho la amenaza y qué está haciendo ahora?
- ¿Cómo frenamos la amenaza y eliminamos la causa raíz?

Con esta información, los equipos de seguridad pueden entender rápidamente qué ha sucedido y pueden utilizar las funciones de contención y de remediación de AMP para emprender una acción. Con unos pocos clics en la sencilla consola de gestión basada en navegador, los administradores pueden contener el malware bloqueando el archivo para que no pueda ejecutarse nunca más en ningún otro terminal. Además, dado que AMP sabe dónde ha estado el archivo, puede retirar el archivo de la memoria y ponerlo en cuarentena para todos los demás usuarios. En caso de una intrusión de malware, los equipos de seguridad ya no tienen que volver a crear imágenes de sistemas completos para eliminar el malware. Ese proceso lleva su tiempo, cuesta dinero y recursos e interrumpe las funciones empresariales críticas. Con AMP, la corrección del malware es quirúrgica y no produce daños colaterales en los sistemas informáticos o en la empresa.

Estas son las ventajas del Análisis Continuo, la Detección Continua y la Seguridad Retrospectiva: otorgan la capacidad de registrar la actividad de cada archivo presente en el sistema y, si un archivo supuestamente “bueno” se transforma en “malo”, ofrecen la capacidad de detectarlo y rebobinar el historial registrado para ver el origen de la amenaza y el comportamiento que ha tenido. A continuación, AMP proporciona funciones incorporadas de respuesta y remediación para eliminar la amenaza. AMP también recuerda todo lo que ve, desde la firma de las amenazas hasta el comportamiento de los archivos, y registra los datos en la base de datos de inteligencia de amenazas de AMP para reforzar aún más las defensas de primera línea, de modo que este archivo y otros parecidos no puedan eludir la detección inicial de nuevo.

Así, los equipos de seguridad tienen el nivel profundo de visibilidad y control que necesitan para detectar los ataques y descubrir el malware sigiloso de forma rápida y eficiente; entender y determinar el alcance de un riesgo; contener y remediar rápidamente el malware (incluso los ataques de día cero) antes de que pueda producirse ningún daño, y evitar que se produzcan ataques similares.

Características principales

La capacidades de análisis continuo y seguridad retrospectivas de AMP son posibles gracias a estas robustas funciones:

- **Indicadores de compromiso (IoC):** Los eventos de archivos y de telemetría se correlacionan y se les da prioridad como brechas activas potenciales. AMP relaciona automáticamente datos de eventos de seguridad de varias fuentes, como los eventos de intrusiones y malware, para ayudar a los equipos de seguridad a conectar los eventos con ataques coordinados de mayor envergadura y también a dar prioridad a los eventos de alto riesgo.
- **Reputación del archivo:** Se recopilan los análisis avanzados y la inteligencia colectiva para determinar si un archivo está limpio o es malicioso, lo que permite una detección más precisa.
- **Análisis dinámico de malware:** Un entorno altamente seguro ayuda a ejecutar, analizar y llevar a cabo pruebas con malware para descubrir amenazas de día cero anteriormente desconocidas. La integración del sandboxing y de tecnologías de análisis dinámico de malware de AMP Threat Grid en las soluciones de AMP permite un análisis más completo que se compara con un grupo mayor de indicadores de comportamiento.
- **Detección retrospectiva:** Se envían alertas cuando la disposición de un archivo cambia después de un análisis pormenorizado, lo que proporciona características y visibilidad del malware que ha eludido las defensas iniciales.
- **Trayectoria del archivo:** Se lleva a cabo un seguimiento continuo de la propagación de los archivos en el entorno para obtener visibilidad y reducir el tiempo necesario para determinar el alcance de una brecha de seguridad por malware.
- **Trayectoria del dispositivo:** Se lleva a cabo un seguimiento continuo de las actividades y las comunicaciones que se producen en un dispositivo y a nivel del sistema para comprender rápidamente las causas principales y el historial de los eventos que desembocan en un riesgo para la seguridad.
- **Elastic Search:** Una búsqueda sencilla y sin límites de datos de inteligencia de seguridad colectiva, telemetría y archivos contribuye a conectar el contexto y el alcance de una exposición con un indicador de compromiso o una aplicación maliciosa.
- **Prevalencia:** Muestra todos los archivos que se han ejecutado en toda la organización, ordenados por prevalencia de menor a mayor, para ayudarle a descubrir las amenazas que anteriormente habían pasado desapercibidas y que habían afectado solo a una pequeña cantidad de usuarios. Los archivos ejecutados solo por una pequeña cantidad de usuarios podrían ser aplicaciones maliciosas (por ejemplo, una amenaza dirigida persistente avanzada) o cuestionables, de las que no es conveniente tener en la red extendida.

- **IoC de terminal:** Los usuarios pueden enviar sus propios IoC para detectar los ataques dirigidos. Estos IoC de terminal permiten a los equipos de seguridad llevar a cabo investigaciones más profundas de amenazas avanzadas menos conocidas específicas de las aplicaciones de su entorno.
- **Vulnerabilidades:** Muestra una lista de software vulnerable en el sistema, los hosts que contienen dicho software y los hosts más susceptibles de correr riesgos. AMP, que se basa en nuestra inteligencia de amenazas y nuestros análisis de seguridad, identifica el software vulnerable que puede ser el blanco de los ataques de malware y las potenciales vulnerabilidades de seguridad, y proporciona una lista ordenada según la prioridad de los hosts que necesitan parches.
- **Control de brotes:** Controle los archivos sospechosos o los brotes y remedie una infección sin esperar a recibir una actualización de contenido. En la función de control de brotes:
  - Las detecciones sencillas personalizadas pueden bloquear rápidamente un archivo específico en todos los sistemas o únicamente en los seleccionados.
  - Las firmas personalizadas avanzadas pueden bloquear las familias de malware polimórfico.
  - Las listas de bloqueo de aplicaciones pueden imponer políticas de aplicación o contener una aplicación que se encuentre en riesgo y que se utilice como puerta de entrada del malware, y detener el ciclo de reinfección.
  - Las listas blancas personalizadas garantizan que las aplicaciones seguras, personalizadas o fundamentales sigan ejecutándose suceda lo que suceda.
  - La correlación de flujos de dispositivos detendrá las comunicaciones de “callback” del malware en el punto de origen, especialmente en el caso de los terminales remotos que se encuentran fuera de la red empresarial.

Opciones de implementación para disponer de protección en cualquier lugar

Los ciberdelincuentes lanzan sus ataques a las organizaciones a través de diferentes puntos de entrada. Para ser realmente eficaces a la hora de detectar ataques sigilosos, las organizaciones necesitan visibilidad en tantos vectores de ataque como sea posible. Por lo tanto, la solución AMP se puede implementar en diferentes puntos de control de la red extendida. Las organizaciones pueden implementar la solución cómo y dónde deseen, de manera que satisfaga sus necesidades específicas de seguridad. Entre las opciones, se incluyen las siguientes:

Nombre del producto	Detalles
AMP de Cisco para terminales	Proteja PC, Mac, dispositivos móviles y entornos virtuales con el conector ligero de AMP que no afecta al rendimiento de los usuarios.
AMP de Cisco para redes	Implemente AMP como solución basada en la red integrada en los dispositivos de seguridad NGIPS FirePOWER™ de Cisco.
Cisco AMP en ASA con FirePOWER Services	Implemente las funciones de AMP incorporadas en el firewall Cisco ASA.
Dispositivo virtual de nube privada de Cisco AMP	Implemente AMP como una solución in situ tipo Air-Gap especialmente diseñada para organizaciones con estrictos requisitos de privacidad que impidan el uso de una nube pública.
Cisco AMP en CWS, ESA o WSA	En caso de contar con Cloud Web Security (CWS), Email Security Appliance (ESA) o Web Security Appliance (WSA) de Cisco, pueden activarse las funciones de AMP para proporcionar funciones retrospectivas y análisis de malware.
AMP Threat Grid de Cisco	AMP Threat Grid se integra con Cisco AMP para proporcionar un análisis dinámico mejorado del malware. También puede implementarse como una solución de análisis dinámico de malware y de inteligencia de amenazas independiente.

¿Por qué Cisco?

Ya no se trata de una cuestión de si va a sufrir una brecha en la seguridad o no, sino más bien de cuándo la va a sufrir. Las soluciones de detección centradas en un momento específico nunca son eficaces al 100% a la hora de localizar y bloquear de forma preventiva todos los ataques. El malware avanzado y sigiloso y los hackers que lo crean pueden eludir este tipo de defensas y poner en riesgo a cualquier organización en cualquier momento. Incluso si se consigue bloquear el 99% de las amenazas, solo hace falta una de ellas para generar una brecha de seguridad. Por lo tanto, en caso de que se produzca una brecha en la seguridad, las organizaciones tienen que estar preparadas y disponer de herramientas que permitan detectar, responder y remediar rápidamente una intrusión.

Cisco AMP es una solución de protección y análisis de malware avanzado integrada, basada en inteligencia y de clase empresarial. Proporciona inteligencia de amenazas global para reforzar las defensas de la red, motores de análisis dinámico para bloquear los archivos maliciosos en tiempo real y capacidad para supervisar y analizar continuamente el comportamiento y el tráfico de los archivos. Estas funciones ofrecen una visibilidad sin precedentes de las actividades de las amenazas potenciales, así como el control necesario para, a continuación, detectar, contener y eliminar rápidamente el malware. Obtendrá protección antes, durante y después de un ataque. La solución también puede implementarse en toda la empresa de manera extensiva: en la red, los terminales, los dispositivos móviles, el correo electrónico, las gateways web y los entornos virtuales, de modo que la organización pueda aumentar la visibilidad de los puntos de entrada cruciales de los ataques, así como implementar la solución cómo y dónde desee de manera que satisfaga sus necesidades específicas de seguridad.

Siguientes pasos

Para obtener más información sobre Cisco AMP o para ver demostraciones de los productos, testimonios de los 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,
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, números de teléfono y fax se encuentran en la Web de Cisco en **www.cisco.com/go/offices**.

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