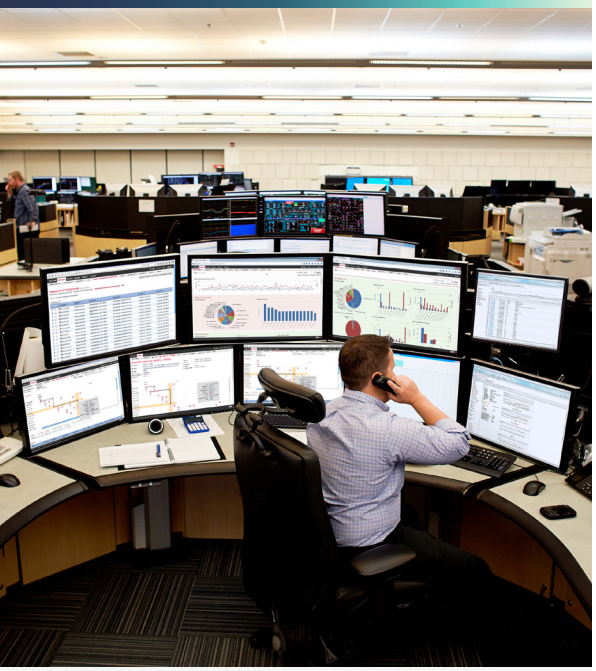
Guía rápida



Protección frente a malware avanzado para redes de Cisco

Prevención, detección y respuesta ante las brechas de seguridad para el mundo real

Las organizaciones reciben ataques con frecuencia y todos los días se producen casos de brechas en la seguridad. Los hackers crean malware avanzado que puede eludir incluso las mejores herramientas de detección centradas en un momento específico, como los firewalls y los sistemas de prevención de intrusiones. Estas herramientas examinan el tráfico en el punto de entrada a la red, pero no son tan efectivas como para detectar el 100% de todas las amenazas que intentan infiltrarse en la organización. Además, ofrecen poca visibilidad de la actividad que llevan a cabo las amenazas una vez han eludido las defensas de primera línea. Esto impide a los equipos de seguridad informática determinar el alcance de un riesgo potencial y detectar y frenar el malware antes de que provoque daños.

La protección frente a malware avanzado (AMP) de Cisco para redes va más allá de las funciones de detección centradas en un momento específico para proteger a las organizaciones antes, durante y después de un ataque.

- **Antes de un ataque,** AMP utiliza la mejor inteligencia de amenazas global para reforzar las defensas de la red.
- **Durante el ataque,** AMP utiliza esa inteligencia, firmas conocidas de archivos y tecnología de análisis dinámico de archivos para bloquear el malware que intenta infiltrarse en la red.
- **Después del ataque,** o después de que un archivo haya accedido a la red, AMP supervisa y analiza continuamente toda la actividad y el tráfico del archivo. Si un archivo muestra un comportamiento malicioso, AMP proporciona visibilidad detallada de la actividad de la amenaza, así como el control necesario para responder y contenerlo rápidamente.

AMP para redes no solo ofrece funciones de prevención de infracciones de seguridad, sino que, en caso de una intrusión que ha pasado desapercibida, proporciona funciones de detección de la brecha, respuesta y contención, todo ello de manera rentable y sin afectar a la eficiencia operativa.

Inteligencia de amenazas y análisis dinámico de malware

AMP para redes se basa en la colección más grande de inteligencia de amenazas en tiempo real y en el análisis dinámico de malware, todo ello suministrado por Collective Security Intelligence de Cisco y Security Intelligence and Research Group de Talos. Las ventajas que obtienen las organizaciones son:

- 1,1 millones de muestras entrantes de malware al día
- 1,6 millones de sensores globales
- 100 terabytes de datos al día
- 13 000 millones de solicitudes web
- 600 ingenieros, técnicos e investigadores
- Operaciones las 24 horas del día

Ventajas

- **Detecte y bloquee** los intentos de explotar vulnerabilidades, los archivos maliciosos y los archivos que infringen las políticas
- **Analice y registre continuamente** la actividad de los archivos para rastrear la difusión del malware y el alcance del riesgo
- **Correlacione eventos discretos** en los ataques coordinados
- **Obtenga visibilidad y control profundos** para detectar, analizar y contener rápidamente las infracciones de seguridad
- **Acceda a una inteligencia de amenazas global sin precedentes** para reforzar las defensas de la red
- **Gestione la solución** a través de la sencilla consola basada en navegador web de AMP, FireSIGHT Management Center

Características

Análisis continuo: Incluso después de que un archivo cruce el punto de control de la red, AMP continúa supervisando, analizando y registrando la actividad y el comportamiento del archivo para detectar rápidamente el malware que haya podido eludir las defensas de primera línea.

Seguridad retrospectiva: Si un archivo considerado anteriormente "desconocido" o "bueno" muestra un comportamiento malicioso, AMP envía una alerta retrospectiva y muestra el historial registrado de la actividad de ese archivo para que pueda determinar el alcance del riesgo y ofrecer una respuesta rápida.

FireSIGHT Management Center de Cisco: Obtenga visibilidad de su entorno a través de un único panel de control que le permitirá ver la información sobre la actividad de las amenazas, los hosts, los sistemas operativos, las aplicaciones, los usuarios, los archivos y la geolocalización.

Análisis de malware dinámico y sandboxing: El entorno altamente seguro permite ejecutar y analizar malware comparándolo con un gran conjunto de indicadores de comportamiento para descubrir amenazas de día cero anteriormente desconocidas.

Indicadores de compromiso (IoC): AMP correlaciona automáticamente los datos de los eventos de seguridad procedentes de diversas fuentes, como archivos, telemetría, intrusiones y eventos de malware, y les otorga una prioridad como brechas activas potenciales. Esto ayuda a los equipos de seguridad a conectar los eventos con ataques coordinados más grandes y a dar prioridad a los eventos de alto riesgo.

Trayectoria del archivo: Se lleva a cabo un seguimiento continuo de la propagación de los archivos para obtener visibilidad y reducir el tiempo necesario para determinar el alcance de una brecha de seguridad por malware.

Integración con Cisco AMP para terminales: AMP para redes es compatible con AMP para terminales y permite obtener mayor visibilidad de la actividad ejecutable en los terminales y correlacionar los eventos de red con los eventos de terminal.

Con esta información, AMP produce inteligencia procesable, como puntuaciones de amenazas para ayudar a los equipos de seguridad a priorizar las respuestas. AMP correlaciona automáticamente archivos, comportamientos, datos de telemetría y actividades con esta sólida base de conocimientos que se complementa con información de contexto para bloquear el malware que intenta infiltrarse en la red. Proporciona a los equipos de seguridad mayor información sobre las amenazas que se encuentran en la red y permite una respuesta más rápida y sencilla ante los incidentes.

Análisis continuo y seguridad retrospectiva

AMP para redes supervisa, analiza y registra continuamente todas las actividades de los archivos, independientemente de su disposición, incluso después de la inspección inicial en el punto de control de la red. Si AMP observa actividades sospechosas o maliciosas, o si un archivo supuestamente "bueno" se vuelve "malo", envía a los equipos de seguridad una alerta retrospectiva y una indicación del nivel de riesgo. AMP también proporciona visibilidad sobre qué es lo que ha sucedido exactamente. Los equipos de seguridad pueden ver el historial completo de las amenazas (rebobinando la actividad del malware) y obtener rápidamente respuestas a las preguntas de seguridad esenciales, como:

- ¿De dónde proviene el malware?
- ¿Qué sistemas se han visto afectados?
- ¿Qué está haciendo la amenaza?
- ¿Cómo la detenemos?

Gracias a la función Trayectoria del archivo, los equipos de seguridad pueden rastrear la transmisión del archivo a través de la red observando una representación visual de las transferencias del mismo a lo largo del tiempo, así como información adicional acerca del archivo. A continuación, resulta sencillo bloquear estos archivos y comunicaciones maliciosos con una simple actualización de las políticas y una lista personalizada de detecciones. Tiene la capacidad de actuar en el momento que usted decida, sin necesidad de esperar a recibir una actualización por parte del proveedor.

El análisis continuo y la seguridad retrospectiva entran en acción y proporcionan a los equipos de seguridad la visibilidad y el control necesarios para detectar, responder y contener rápidamente las amenazas.

Implementación

AMP para redes se administra a través de FireSIGHT™ Management Center de Cisco, una sencilla consola de administración basada en Web. Se implementa mediante suscripción en el sistema de prevención de intrusiones de última generación (NGIPS) FirePOWER de Cisco, que abarca una amplia gama de funciones de red y de procesamiento.

Siguientes pasos

Póngase en contacto con un representante de ventas o un partner de canal de Cisco para obtener más información sobre cómo puede ayudarle AMP para redes a proteger la organización frente a ciberataques avanzados. Obtenga más información en www.cisco.com/go/ampnetwork.

C45-731875-01 03/15