Protección frente a malware avanzado para terminales de Cisco

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

Los hackers crean malware avanzado que puede eludir incluso las mejores herramientas de detección centradas en un momento específico, como los antivirus y los sistemas de prevención de intrusiones. Estas herramientas no son tan efectivas como para detectar el 100% de todas las amenazas, además, ofrecen poca visibilidad de las amenazas que consiguen eludir la detección inicial. Esto impide a los equipos de seguridad informática determinar el alcance de un riesgo potencial y detectar y repeler el malware antes de que provoque daños.

La protección frente a malware avanzado (AMP) de Cisco® para terminales 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 su entorno informático.
- Después del ataque, AMP supervisa todas las actividades ejecutables y de los archivos para detectar el malware que haya podido eludir la detección inicial, y ofrece la visibilidad y el control necesarios para combatirlo rápidamente.

AMP de Cisco para terminales no solo evita las brechas de seguridad, sino que también detecta, contiene y remedia rápidamente las amenazas si consiguen eludir las defensas de primera línea, todo ello de manera rentable y sin afectar a la eficiencia operativa.

Ventajas

- **Detecte y supervise continuamente** el malware, tanto de manera inmediata como retrospectiva
- **Proteja** PC, Mac, dispositivos móviles y entornos virtuales
- **Registre la actividad del archivo** a lo largo del tiempo para rastrear la difusión del malware y el alcance del riesgo
- **Correlacione eventos discretos** en los ataques coordinados
- **Acceda a una inteligencia de amenazas global** para reforzar las defensas de la red
- **Obtenga visibilidad y control profundos** para detectar, analizar y remediar rápidamente las brechas de seguridad

Inteligencia de amenazas y análisis dinámico de malware

Cisco AMP se basa en una extensa colección de inteligencia de amenazas en tiempo real y en el análisis dinámico de malware, todo ello suministrado por Collective Security Intelligence de Cisco, Security Intelligence and Research Group de Talos y las fuentes de información de inteligencia de AMP Threat Grid.

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

24/7 Operaciones las 24 horas al día

Análisis continuo y seguridad retrospectiva: AMP continúa supervisando, analizando y registrando la actividad del archivo para detectar rápidamente el malware que haya podido eludir las defensas de primera línea, y permite determinar el alcance del riesgo y ofrecer una respuesta rápidamente.

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): 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 y a dar prioridad a los eventos de alto riesgo.

Trayectoria del dispositivo: Puede llevar a cabo un seguimiento continuo de las actividades de ejecución 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.

Prevalencia: AMP muestra todos los archivos que se han ejecutado en toda la organización, ordenados por prevalencia, para ayudarle a descubrir las amenazas que anteriormente habían pasado desapercibidas y que habían afectado solo a una pequeña cantidad de usuarios. Los archivos abiertos solo por una pequeña cantidad de usuarios podrían ser maliciosos.

Vulnerabilidades: AMP muestra una lista de software vulnerable en el sistema, los hosts que contienen dicho software y los hosts más susceptibles de correr riesgos. AMP identifica el software vulnerable que puede ser el blanco de los ataques y las potenciales vulnerabilidades de seguridad, y proporciona una lista ordenada según la prioridad de los hosts que necesitan parches.

Control de brotes: AMP le ayuda a controlar los archivos sospechosos o los brotes y a combatir una infección sin esperar a recibir una actualización de contenido. Además:

Bloquea rápidamente un archivo específico en todos los sistemas o únicamente en los seleccionados.

Bloquea las familias de malware polimórfico.

Contiene una aplicación que se encuentre en riesgo y que se utilice como puerta de entrada del malware y detiene el ciclo de reinfección.

Detiene las comunicaciones de "callback" del malware en el punto de origen, incluso en el caso de los terminales remotos que se encuentran fuera de la red empresarial.

Ayuda a garantizar que las aplicaciones fundamentales sigan ejecutándose suceda lo que suceda.

Para obtener más información sobre funciones adicionales, consulte **la hoja de datos de AMP para terminales.**

Los hackers crean malware avanzado que puede eludir incluso las mejores herramientas de detección centradas en un momento específico, como los antivirus y los sistemas de prevención de intrusiones. Estas herramientas no son tan efectivas como para detectar el 100% de todas las amenazas. Además, ofrecen poca visibilidad de las amenazas que consiguen eludir la detección inicial. Esto impide a los equipos de seguridad informática determinar el alcance de un riesgo potencial e detectar y repeler el malware antes de que provoque daños.

La protección frente a malware avanzado (AMP) de Cisco® para terminales 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.

Análisis continuo y seguridad retrospectiva

AMP de Cisco para terminales supervisa, analiza y registra continuamente la ejecución y actividad de los archivos, independientemente de su disposición, incluso después de la inspección inicial. Si AMP observa una actividad sospechosa, los equipos de seguridad recibirán una alerta y podrán ver el historial completo de la amenaza para obtener rápidamente respuestas a las siguientes preguntas:

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

Con unos pocos clics en la consola de gestión basada en navegador de AMP se puede bloquear el archivo para que no pueda ejecutarse en ningún otro terminal.

Además, dado que AMP sabe en qué otros terminales ha estado el archivo, puede retirarlo de la memoria y ponerlo en cuarentena para todos los demás usuarios. Los equipos de seguridad ya no tienen que volver a crear imágenes de sistemas completos para eliminar el malware.

Ese proceso lleva su tiempo y cuesta dinero y recursos. Con AMP, la remediación del malware es quirúrgica y no produce daños colaterales en los sistemas informáticos o en la empresa.

Además, AMP 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. Esto refuerza aún más las defensas de primera línea para que este archivo y otros similares no puedan eludir la detección inicial de nuevo.

Implementación

AMP de Cisco para terminales se gestiona a través de una sencilla consola basada en la Web. Se implementa a través del conector de terminal ligero de AMP, que no afecta el rendimiento de los usuarios, ya que el análisis se realiza en la nube y no en el terminal. La solución se ofrece como suscripción para los terminales como, por ejemplo, PC, Mac, dispositivos móviles y sistemas virtuales.

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 de Cisco para terminales a proteger la organización frente a ciberataques avanzados. Obtenga más información en: www.cisco.com/go/ampendpoint.

Contáctenos

Oficinas Centrales en América Cisco Systems, Inc. San José, CA | Oficinas Centrales en Asia Pacífico Cisco Systems (USA) Pte. Ltd. Singapur | Oficinas Centrales en Europa Cisco Systems International BV Amsterdam Holanda

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y fax están listados en el sitio de Cisco en la siguiente dirección web: www.cisco.com/go/offices.