McAfee Cloud Threat Detection

Mejore fácilmente las protecciones de Intel Security para neutralizar el malware avanzado e identificar las amenazas evasivas

Una amplia selección de las últimas técnicas de análisis, incluido el aprendizaje automático, identifica el malware y convierte las detecciones en acción, actualizando las protecciones para frustrar ataques similares en el futuro.

Ventajas principales:

- Reduzca el riesgo de que las amenazas desconocidas dañen su empresa.
- Aproveche el poder de los Big Data y el aprendizaje automático.
- Optimice las inversiones en seguridad.
- Simplifique el despliegue de análisis de amenazas avanzadas.

Las empresas libran una batalla incesante contra un malware cada día más inteligente que sigue eludiendo las defensas tradicionales. Las soluciones de detección avanzadas ayudan, pero pueden parecer complejas y caras para empresas que disponen de personal y recursos limitados. Además, la mayoría no se integran con la infraestructura de protección, por lo que permiten que aumente la ventana de vulnerabilidad mientras que los equipos de respuesta a penas si pueden actuar.

¿Qué es lo que las empresas necesitan? Detección avanzada y asequible que sea muy sencilla de desplegar y utilizar: McAfee® Cloud Threat Detection. Este práctico nuevo servicio se integra en las soluciones de Intel® Security existentes para neutralizar el malware e identificar las amenazas evasivas. Como solución en la nube, le permite aprovechar fácilmente la ingente potencia de computación que permite aplicar las últimas técnicas de análisis. Le permitirá mejorar la detección y optimizar las inversiones en seguridad existentes.

Detección integrada con la protección

Las soluciones de Intel Security constituyen su primera línea de defensa, eliminando el malware conocido y el malware potencial mediante herramientas avanzadas, como la emulación y el análisis de la reputación. Pero si no están seguras de si un archivo es malicioso, lo transfieren a la nube para un análisis en profundidad.

Máquinas contra el malware emergente y evasivo

Con McAfee Cloud Threat Detection, los motores de análisis estático se ponen a trabajar para extraer los detalles de los archivos. La amplia cobertura de tipos de archivos proporciona el contexto necesario para el software "gris" (greyware), identificando de manera eficaz tanto los archivos maliciosos como los limpios. Además, se lleva a cabo un análisis del comportamiento ya que el archivo también se ejecuta en un entorno aislado. Todo lo que hace el malware se graba, revisa y evalúa en busca de intenciones maliciosas. ¿Generó el archivo una carpeta aleatoria, copió un nuevo archivo en ella y eliminó el original? ¿Ocultó su información en URL desconocidas o sospechosas entre el tráfico a sitios web conocidos como Google, Amazon o Facebook? Estos son solo algunos ejemplos de comportamientos que el servicio McAfee Cloud Threat Detection puede utilizar para clasificar un archivo desconocido. Estos procesos también revelan metadatos, URL, nombres de archivos, ubicaciones de carpetas, etc., de los que informamos a los clientes para que puedan investigar y comprobar si se han visto afectados otros equipos.

intel Security

Aprendizaje automático supervisado

Gestionado y optimizado por McAfee Labs, cada paso del ciclo de análisis aprovecha el conocimiento de nuestros analistas, Big Data y aprendizaje automático. Los exhaustivos modelos de clasificación de nuestro sistema de Big Data alojado en la nube se han desarrollado y formado aprovechando la información acumulada durante más 25 años de datos y 2000 millones de archivos. La investigación activa y la interpretación constante de los resultados de la inspección alimentan el aprendizaje automático permanente para hacer evolucionar estos modelos a medida que cambian las técnicas y comportamientos de malware y avanzan las investigaciones.

La precisión como prioridad

Nuestra experiencia nos ha enseñado que un falso negativo o un falso positivo pueden ser dañinos y costosos. Por eso los sistemas que utilizamos incluyen comprobaciones y comparaciones con los archivos de sistema y certificados de firma más críticos para garantizar que las detecciones son precisas y a la vez fiables. Mientras el análisis avanzado detecta las amenazas emergentes, comparamos y asociamos los resultados con artefactos de malware y atributos contextuales y de comportamiento para minimizar los falso positivos. Esta es una de las ventajas que diferencia a nuestra combinación de análisis en la nube y numerosos recursos antimalware.

Detección en acción

McAfee Cloud Threat Detection notifica cada veredicto al sistema de origen, que aplica la directiva correspondiente, como poner en cuarentena una máquina o activar la protección para frustrar ataques similares. Además, se dispone de indicadores de peligro para investigarlos más a fondo, y de los datos necesarios para corregir y recuperarse tras un ataque. Las detecciones actualizan las reputaciones de McAfee Global Threat Intelligence (GTI) para acelerar la protección de todas las empresas con soluciones que utilizan GTI.

Rápido, asequible y adaptado a pequeñas empresas

Como servicio basado en la nube, solamente tiene que introducir la clave compartida cifrada de su producto de McAfee, por lo que el aprovisionamiento es rápido. Si dispone de sistemas distribuidos, no es necesario que redirija el tráfico a un centro de datos, basta con enviarlo a la nube. Nuestros expertos se encargan del mantenimiento diario e implementan las actualizaciones y ampliaciones de forma transparente. Al tratarse de una suscripción en la que el precio se basa en el volumen, no es necesaria ninguna inversión inicial, por lo que se elimina el principal obstáculo de compra para las PYMES, es decir, el coste.

Para obtener más información, visite **www.mcafee.com/es/products/cloud-threat-detection.aspx**.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com