McAfee Application Data Monitor

Detecte las amenazas ocultas con la inspección de la capa de aplicaciones.

El dispositivo McAfee® Application Data Monitor amplía los límites de la seguridad y el cumplimiento de normativas más allá de la administración de registros, y extiende la supervisión hasta la capa de aplicaciones. Ahora puede examinar detenidamente el contenido de las aplicaciones con el fin de obtener máxima visibilidad del uso que se hace de su red.

El dispositivo McAfee Application Data Monitor descodifica una sesión de aplicaciones completa hasta la capa 7, ofreciendo un análisis global, desde los protocolos subyacentes y la integridad de las sesiones hasta el contenido de las propias aplicaciones (como el texto de un mensaje de correo electrónico o sus adjuntos). Este nivel de detalle permite analizar con gran precisión el uso real de las aplicaciones, pudiendo al mismo tiempo implementar directivas de aplicaciones y detectar el tráfico malicioso encubierto.

Esta inspección en profundidad facilita el cumplimiento de normativas, ya que permite realizar un seguimiento de todos los datos confidenciales de la red. Cuando el dispositivo McAfee Application Data Monitor detecta una infracción, conserva todos los detalles de la sesión de esa aplicación para utilizarlos en respuestas a incidentes y análisis forenses, o por si fueran necesarios para demostrar el cumplimiento de las normativas.

Al mismo tiempo, el dispositivo ofrece visibilidad de las amenazas que pueden hacerse pasar por aplicaciones legítimas:

- Amenazas avanzadas en la capa de aplicaciones
- Uso no autorizado o robo de datos confidenciales
- Ataques dirigidos u originados en "puntos ciegos" de seguridad
- Uso de código heredado peligroso
- Robo o uso indebido de credenciales de usuario
- Transmisión de datos confidenciales a través de cualquier aplicación
- Procesos empresariales interrumpidos

Principales ventajas

- Descodifica la sesión de aplicaciones completa, hasta la capa 7, para cientos de aplicaciones
- Incluye reglas de detección prediseñadas para datos confidenciales y sometidos a normativas
- Admite el uso de diccionarios definidos por el usuario y reglas para la personalización
- Genera una completa pista de auditoría de eventos de aplicaciones para demostrar el cumplimiento de normativas
- Funciona de forma pasiva para evitar interferencias con las aplicaciones
- Se integra con McAfee Enterprise Security Manager para facilitar la correlación del contenido de las aplicaciones con los eventos y otras fuentes de datos
- Opciones de distribución flexible e híbrida, que incluyen dispositivos físicos y virtuales

Pérdida de datos e infracciones de cumplimiento de normativas

El dispositivo McAfee Application Data Monitor detecta si se está transmitiendo información confidencial a través de adjuntos de correo electrónico, mensajes instantáneos, transferencias de archivos, envíos HTTP o cualquier otra aplicación, y le notifica inmediatamente de forma que pueda detenerse la pérdida de datos.

Con la configuración predeterminada del dispositivo puede detectar datos confidenciales, como información de tarjetas de crédito y números de documentos de identidad. Además, puede personalizar las funciones de detección de McAfee Application Data Monitor definiendo sus propios diccionarios de información confidencial. El dispositivo McAfee Application Data Monitor detectará sin problemas ese tipo de datos, alertará al personal adecuado y registrará la infracción para mantener una pista de auditoría.

Descubrimiento de documentos

El dispositivo McAfee Application Data Monitor identifica más de 500 tipos de documentos en su tránsito por la red a través del correo electrónico, chat, programas P2P, recursos compartidos de archivos u otros medios. Este dispositivo descubre los documentos sea cual sea su extensión, incluidos los que se ocultan bajo un tipo de extensión distinto para sortear los gateways de correo y los dispositivos de detección y prevención de intrusiones (IDS/IPS). Se descubren asimismo los documentos incorporados a otros documentos, así como los archivados, comprimidos y codificados, mediante criterios como el nombre de archivo y la operación que se está llevando a cabo.

Amenazas en la capa de aplicaciones

Las nuevas y sofisticadas amenazas aprovechan las vulnerabilidades de las aplicaciones empresariales de uso común para penetrar en su red y extraer datos confidenciales. Aunque estas amenazas en la capa de aplicaciones son difíciles de detectar mediante el uso de firewalls y sistemas tradicionales de detección y prevención de intrusiones (IDS/IPS), el dispositivo McAfee Application Data Monitor es capaz de examinar el contenido completo de una aplicación, incluidos los protocolos subyacentes, para detectar cargas útiles ocultas, malware e incluso canales de comunicación encubiertos; por ejemplo, un ejecutable incrustado en un documento PDF.

Anomalías de protocolos

La detección de anomalías identifica amenazas inminentes, lo que permite reducir el riesgo y minimizar las pérdidas. Mientras que las soluciones de seguridad tradicionales se limitan a analizar los flujos de red, el dispositivo McAfee Application Data Monitor va un paso más allá. Nosotros examinamos los comportamientos ocurridos en la red con el fin de detectar anomalías dentro de las aplicaciones y protocolos, de esta forma, podemos ofrecer una metodología de detección de riesgos más proactiva y eficaz.

Sin interferencia con las aplicaciones

El dispositivo McAfee Application Data Monitor opera en un puerto SPAN, por lo que no interfiere en la fiabilidad o el rendimiento de las aplicaciones, ni introduce latencia.

Compatibilidad con más de 500 aplicaciones y protocolos

- **Protocolos de red de bajo nivel:** TCP/IP, UDP, RTP, RPC, SOCKS e DNS, entre otros
- **Correo electrónico:** MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- **Correo web:** AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook y MySpace
- **Mensajería instantánea:** AOL, ICQ, Jabber, MSN, SIP y Yahoo
- **Protocolos de transferencia de archivos:** FTP, HTTP, SMB y SSL
- **Protocolos de compresión y extracción:** BASE64, GZIP, MIME, TAR, ZIP, etc.
- **Compresión de archivos:** RAR, ZIP, BZIP, GZIP, Bin-hex y archivos codificados con UUEncode.
- **Paquetes de instalación:** paquetes de Linux, archivos .cab de InstallShield y archivos .cab de Microsoft
- **Archivos de imagen:** GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, mapas de bits, Visio, Digital RAW e iconos de Windows
- **Archivos de audio:** WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio y SHOUTCast, entre otros
- **Archivos de vídeo:** AVI, Flash, QuickTime, Real Media, MPEG-4 , Vivo, Digital Video (DV) y Motion JPEG, entre otros

Integrado en su infraestructura

Mientras que la mayoría de las soluciones de supervisión de redes funcionan de forma aislada, el dispositivo McAfee Application Data Monitor trabaja de manera conjunta con otros sistemas de seguridad de la información. A través de McAfee Enterprise Security Manager, se conecta al resto de su infraestructura de seguridad para simplificar las operaciones de seguridad, mejorar la eficacia global y reducir costes. Puede integrar la detección de pérdidas y fraude con exhaustivos análisis, inspección de redes o supervisión de eventos de base de datos, entre otros.

Ejemplos de casos de uso

El dispositivo McAfee Application Data Monitor puede detectar actividades no autorizadas de naturaleza muy variada, así como infracciones de directivas, robos y actos fraudulentos. A continuación se enumeran algunos ejemplos:

Robo de información confidencial

Un empleado que inició una sesión como jruiz@empresa.com envió un mensaje de correo electrónico a complice@gmail.com. El mensaje de correo electrónico contenía un archivo llamado shoo.doc que incluía las palabras "fórmula secreta". El mensaje se envió a las 12:20 desde el host desktop0232 (192.168.0.36) mediante el servidor SMTP (10.0.2.13), con el siguiente asunto: lo tengo.

Uso de aplicaciones no autorizadas

Un empleado infringió una directiva al realizar una transferencia de archivos de música a través de una aplicación para compartir archivos P2P que había instalado. Envió archivos de gran tamaño durante el horario de trabajo, consumiendo gran cantidad de ancho de banda. Una investigación más detallada reveló que el empleado realizaba estas actividades con frecuencia. Utilizaba Jabber e IRC, y ejecutaba un servidor web no autorizado en su ordenador.

Cyberslacking en el lugar de trabajo

Un empleado se dedica también a operar en bolsa en secreto. A lo largo de su jornada laboral, se conecta a sitios para realizar transacciones bursátiles durante una hora por la mañana y otra por la tarde, de media. Además, utiliza el sistema VoIP (SIP) de la empresa para realizar una media de seis llamadas al día y pasa horas en Yahoo! Messenger como "operadorluis" chateando con "operadorjose" y "operadorjuan".

Usuario de contraseñas sencillas

De acuerdo con la política de seguridad de su empresa, deben utilizarse contraseñas seguras en todas las cuentas de usuarios del sistema y de aplicaciones. La administración de las cuentas de Microsoft Active Directory es muy estricta. Sin embargo, se están usando decenas de contraseñas poco seguras en servidores FTP que se utilizan desde el exterior, servidores de correo y aplicaciones web críticas que no emplean Active Directory.

Compatibilidad con más de 500 aplicaciones y protocolos (continuación)

- **Otras aplicaciones y archivos:** bases de datos, hojas de cálculo, faxes, aplicaciones web, fuentes, archivos ejecutables, aplicaciones de Microsoft Office, juegos y herramientas de desarrollo de software
- **Otros protocolos:** : impresora de red, acceso shell, VoIP y P2P

Más información

Para obtener más información, visite **www.mcafee.com/es/products/siem/index.aspx**.

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es

61322ds_app-data-monitor_0914
SEPTIEMBRE DE 2014