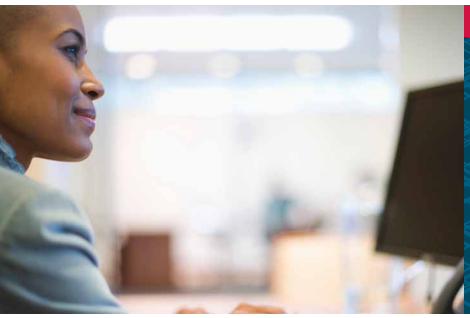

La evolución del panorama de la seguridad de equipos de sobremesa

El panorama de la seguridad de ordenadores de sobremesa ha evolucionado debido a muchos factores: el malware selectivo, las preocupaciones por una mejor experiencia del usuario final, el soporte de TI y los costes operativos. Tradicionalmente, la implementación de la seguridad de equipos de sobremesa es similar a la compra de una póliza de seguros teniendo en cuenta los posibles riesgos únicamente y dejando prácticamente de lado cualquier otro factor. En la configuración del entorno operativo común de la empresa (COE), la seguridad de los ordenadores de sobremesa ha supuesto un desafío para los equipos de TI, ya que se han visto obligados a encontrar el equilibrio entre la flexibilidad del usuario final y las necesidades de seguridad.

Entornos de ordenadores de sobremesa

Tal y como sugieren varios estudios, existen dos grupos distintos de entornos de ordenadores de sobremesa:

- *Usuarios estándar*: imágenes de tipo de COE restringidas, también conocidas como de función fija u ordenadores de sobremesa de imágenes comunes. En estos entornos, el usuario final no dispone de privilegios para instalar o desinstalar software.
  Ejemplo de imágenes COE: estaciones de trabajo en tiendas, hospitales y empresas financieras.
- *Usuarios avanzados*: usuarios con la capacidad de instalar su propio software.
  Ejemplo de usuarios avanzados: entornos de ingeniería y diseño gráfico.

En este informe, nos centraremos en el modelo de seguridad COE.

Desafíos actuales de la seguridad de ordenadores de sobremesa

En los últimos 20 años, a medida que hemos avanzado hacia una economía basada en el conocimiento, los desafíos relativos a mantener la fidelidad de la infraestructura de TI han aumentado enormemente. Se ha producido un aumento extraordinario en el número de muestras de malware detectadas por investigadores de seguridad en todo el mundo, de miles de muestras en un año a miles de muestra al día. A nivel operativo, la seguridad de los endpoints (ordenadores de sobremesa y portátiles) ha aumentado en complejidad y los responsables de la seguridad de TI advierten una mezcla de problemas relacionados con la seguridad operativa y otros basados en amenazas.

Explosión del malware

El espectacular aumento del malware en circulación constituye la principal preocupación de los responsables de la seguridad. Hay un aumento evidente en la complejidad y en el número de malware que generan varios vectores de ataque contra la infraestructura de TI.

Rendimiento

En segundo lugar, el rendimiento de las soluciones tradicionales sigue siguiendo una preocupación, en parte debido al importante aumento del número de firmas de malware.

Seguridad operativa

En tercer lugar, el aspecto operativo de la seguridad es una preocupación mayor. Cuando el malware consigue introducirse en un entorno de TI, debilita la infraestructura de seguridad. Además, las soluciones de seguridad basadas en firmas tradicionales pueden mostrarse incapaces de reducir la exposición a ataques de tipo zero-day y a las amenazas persistentes avanzadas (APT).

Proliferación de las aplicaciones no autorizadas

Por último, es esencial detener las aplicaciones no autorizadas que proliferan en los ordenadores de sobremesa de los usuarios finales. En mercados emergentes, esto también incluye impedir que el uso de software pirateado o sin licencia se extienda en el entono de la empresa.

Dificultades en cuanto a comportamiento en la administración de la seguridad

Desde el punto de vista del comportamiento, se produce una lucha constante en los entornos COE entre la necesidad del administrador de aplicar la seguridad y la del usuario final de disponer de un entorno seguro a la vez que flexible. Ambos objetivos deben alcanzarse sin comprometer la seguridad ni la productividad dentro de la empresa. Una solución necesita satisfacer los requisitos de seguridad del administrador y del usuario final por igual, sin comprometer el principio general de la productividad sostenida.

¿Hay soluciones?

Gracias a sus funciones de creación de listas blancas, McAfee® Application Control, unida a tecnología antivirus tradicional, ofrece una solución viable a muchos de estos problemas. McAfee Application Control supone una mejora sustancial respecto a la seguridad de ordenadores de sobremesa tradicional, ya que ofrece protección contra el malware junto con funciones de gestión de brotes mejoradas.

Listas blancas de aplicaciones

El sistema de creación de listas blancas se basa fundamentalmente en la identificación de los archivos "legítimos conocidos" de un entorno de TI, de manera que sean los únicos que se autoricen en el sistema. Su implementación tiene muchas variantes: por un lado tenemos los despliegues independientes y, por otro, la convivencia con una solución de creación de listas negras tradicional, como un antivirus. En este informe nos centramos en un entorno de TI con antivirus que puede enriquecerse mediante la incorporación de tecnología de creación de listas blancas.

Modo de observación

McAfee Application Control ofrece una función operativa llamada "modo de observación". En este modo no se efectúa la implementación; únicamente se supervisan las versiones de McAfee Application Control. Puede activarse una vez que se ha instalado McAfee Application Control y se ha llevado a cabo el análisis de inventario. Como parte del despliegue inicial de una empresa, este modo puede ayudar a crear directivas que ayuden a identificar el incumplimiento de los estándares de seguridad y las excepciones operativas válidas.

Cuando se despliega junto con una herramienta antivirus tradicional, el modo de observación permite al antivirus seguir siendo la herramienta de seguridad principal. Esto ayuda al administrador de seguridad a mantener la supervisión de los activos de TI al tiempo que permite al antivirus ocuparse de la seguridad real en los endpoints de los usuarios. En conjunto, esto redunda en un aumento de la productividad del usuario del ordenador de sobremesa y en un mejor conocimiento del estado de seguridad por parte de los administradores de TI.

Reputación de archivos con McAfee Global Threat Intelligence™ (McAfee GTI™)

McAfee Application Control también incluye las funciones de reputación de archivos de McAfee GTI; además, puede incorporar el inventario de archivos completo de los endpoints al software McAfee® ePolicy Orchestrator® (McAfee ePO™). Este inventario se contrasta entonces con las calificaciones de reputación de archivos recibidas del servidor de McAfee GTI. Esto proporciona una función, que se ejecuta offline y con transferencia de carga, para identificar los archivos de la empresa como malware o susceptibles de causar problemas. Si un archivo es identificado como malware, la interfaz de McAfee ePO ofrece un único panel que permite encontrar fácilmente la ubicación de todas las instancias del malware en el entorno de TI.

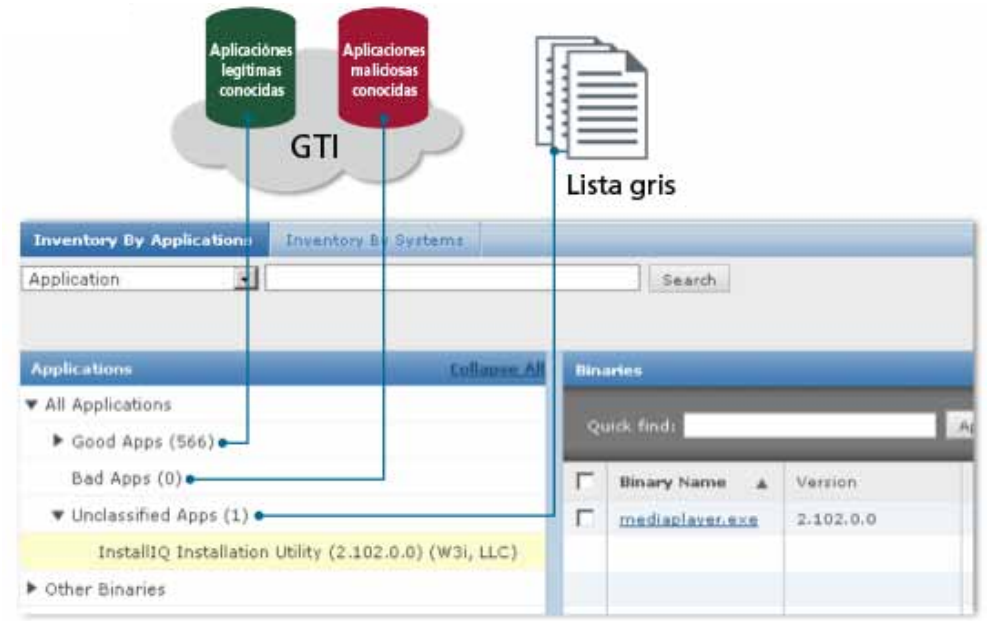

Figura 1. La reputación de archivos de McAfee GTI clasifica todas las aplicaciones de la empresa.

Resistencia a brotes de malware

La capacidad de McAfee Application Control de operar en modo de observación, con el antivirus como software de seguridad principal, proporciona una ventaja sin precedentes a la hora de oponer resistencia a los brotes de malware y facilita al administrador pasar del modo de observación al modo de implementación, y viceversa, en función de las circunstancias. En el momento en que se sospecha un brote de malware, pasar McAfee Application Control al modo de implementación blinda el estado de los sistemas en toda la infraestructura de TI, impidiendo de esta forma que el malware avance dentro de la empresa. Esto, junto con la capacidad de administrar la detección de malware basándose en el inventario del software McAfee ePO, posibilita una corrección simplificada y oportuna de las máquinas infectadas.

Interactividad del usuario con listas blancas dinámicas

Por último, si McAfee Application Control se despliega en modo de implementación y, por lo tanto, con un mayor nivel de seguridad, el usuario final debe enviar solicitudes al departamento de TI para permitir cambios en sus máquinas. Esta es básicamente la parte dinámica de la creación de listas blancas, canalizada a través de una interacción bien definida entre el usuario y el administrador. Gracias a esta funcionalidad, McAfee Application Control es capaz de ofrecer una mayor seguridad al tiempo que administra la experiencia del usuario al mismo nivel que con una herramienta antivirus tradicional.

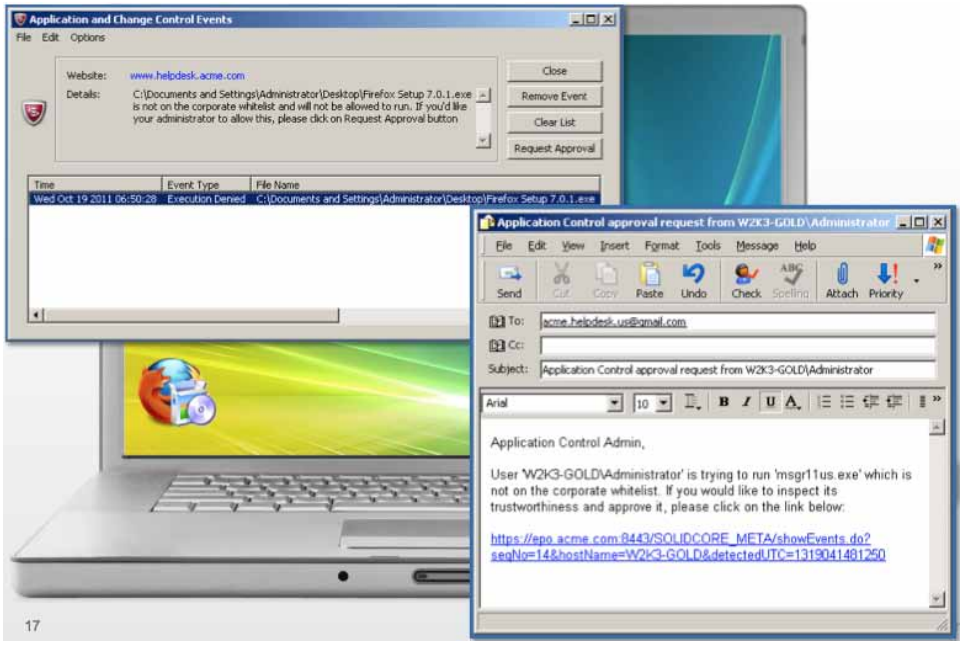

Figura 2. Notificaciones y solicitud de aprobación de ordenadores de sobremesa para aplicaciones no incluidas en la lista blanca.

Administración de aplicaciones no autorizadas

En los mercados emergentes, el contexto de la seguridad también está definido por la capacidad de localizar el software no autorizado e inseguro en un entorno de TI. Puesto que el inventario está disponible a nivel del software McAfee ePO, es posible exportarlo y reconciliarlo con una lista de software seguro aprobado por la empresa. Los datos delta entre la lista de software aprobado por la empresa y la lista de inventario exportada por el software McAfee ePO pueden utilizarse para identificar infracciones de directivas de seguridad generales y requisitos de licencia, según el caso.

Conclusión

La creación de listas blancas de aplicaciones está evolucionando hacia una capa de defensa principal viable para determinados sistemas de ordenadores de sobremesa. Cuando se utiliza junto con soluciones antivirus existentes, no solo ofrece una defensa sólida frente a las amenazas emergentes, como las APT y el malware selectivo, sino que contribuye además a reducir los costes operativos mediante el control de la extensión de las aplicaciones no autorizadas. Con las mayores ventajas de la creación de listas blancas de aplicaciones y las mejoras tecnológicas recientes que facilitan la implementación de listas blancas, los administradores pueden esperar un modelo de seguridad de equipos de sobremesa más simple.

McAfee, Inc.

McAfee, empresa subsidiaria propiedad de Intel Corporation (NASDAQ:INTC), es líder en tecnología de seguridad. McAfee tiene el firme compromiso de afrontar los más importantes retos de seguridad. La compañía proporciona servicios y soluciones probados y proactivos que ayudan a proteger redes, dispositivos móviles y sistemas en todo el mundo, permitiendo a los usuarios conectarse a Internet, navegar por la Web y realizar compras online de forma más segura. Gracias a la tecnología Global Threat Intelligence (Inteligencia Global de Amenazas), McAfee proporciona protección en tiempo real mediante sus soluciones de seguridad, permitiendo a las empresas, usuarios particulares, organismos públicos y proveedores de servicios cumplir con la normativa, proteger datos, prevenir interrupciones, identificar vulnerabilidades y controlar cualquier tipo de amenaza que pueda poner en peligro su seguridad. En McAfee enfocamos todos nuestros esfuerzos en la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes. www.mcafee.com/es

McAfee
An Intel Company

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8535
www.mcafee.com/es