Ficha Técnica no oficial de MPS-MKC a sus partners.

McAfee MVISION

Nueva solución para los Endpoint https://www.youtube.com/watch?v=OV_jrJZcTak

McAfee® MVISION es la nueva familia y generación de productos de McAfee, construida como una potente solución de ciber-seguridad complementada con una administración sencilla y centralizada.

Dos suites, flexibilidad para cada necesidad: Mvision es una solución con **dos categorías** que ofrecen una seguridad completa a sus usuarios, **Standard y Plus**, la diferencia está en los complementos adicionales para satisfacer los requerimientos específicos de las organizaciones.

Mvision Standard

MVISION Standard Todo incluido

Administración Saas u on-premise de seguridad avanzada para endpoint.

MVISION ePO
Administración SaaS
Listo para desplegar en minutos

ePO on-premise
Despliegue y utilice en su data center.
En caso de no querer usar Mvision ePo

MVISION Endpoint
Windows 10. Administre Windows Defender + McAfee

Endpoint Security (ENS)
Seguridad para: Windows, MacOS, Linux.
En caso de no tener Windows 10 o no querer utilizar MVISION Endpoint
ENS incluye Adaptative Threat Protection (ATP)

* & Device Control*

* Solo ePo on-premise.

Ficha Técnica no oficial de
MPS-MKC a sus partners.

Mvision Plus

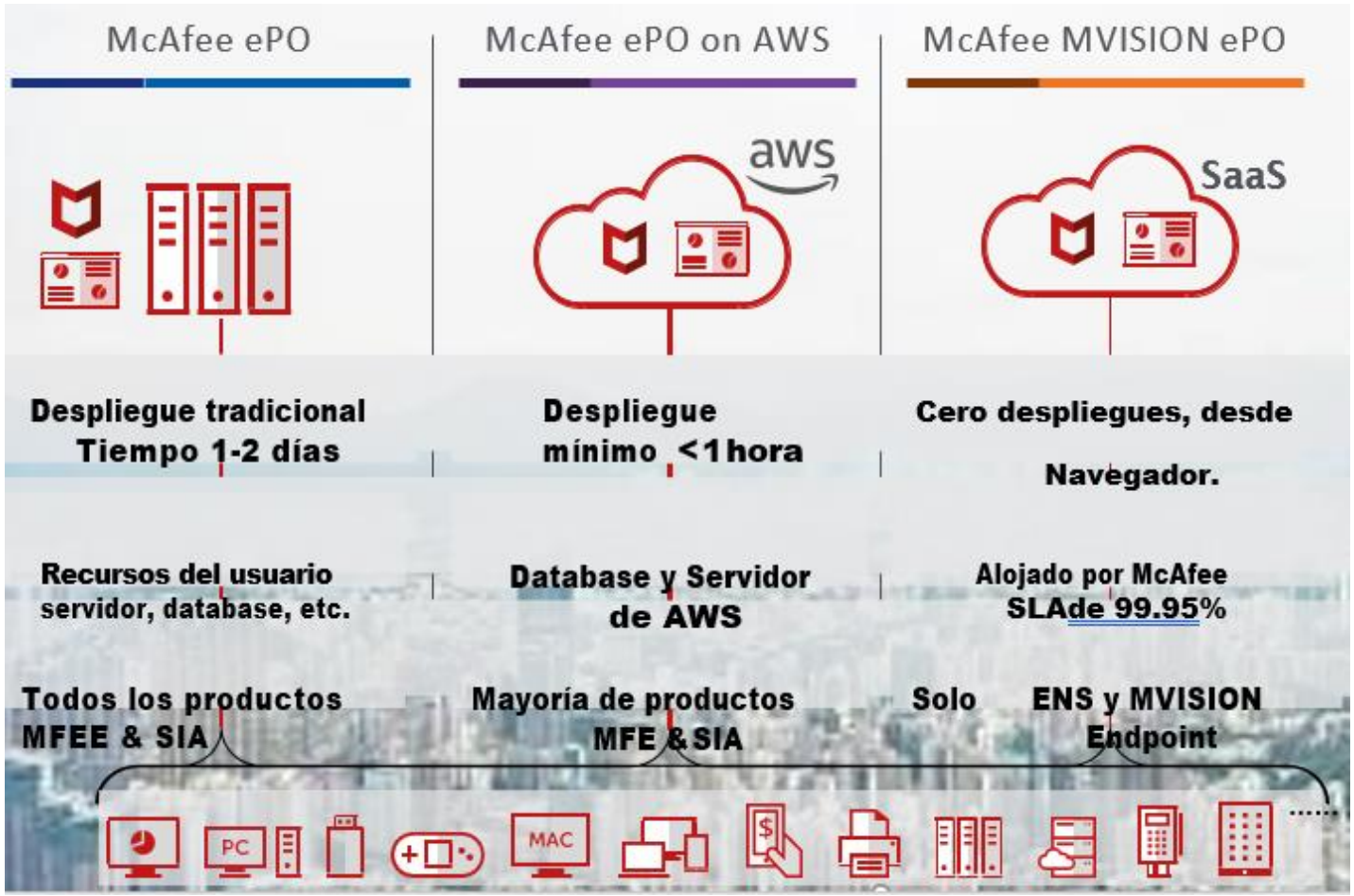
Descripción de los componentes:

Consola de Administración - McAfee ePolicy Orchestrator (ePo)

1. Mvision ePo, 2. McAfee ePo (on-premise), 3. McAfee ePo in AWS

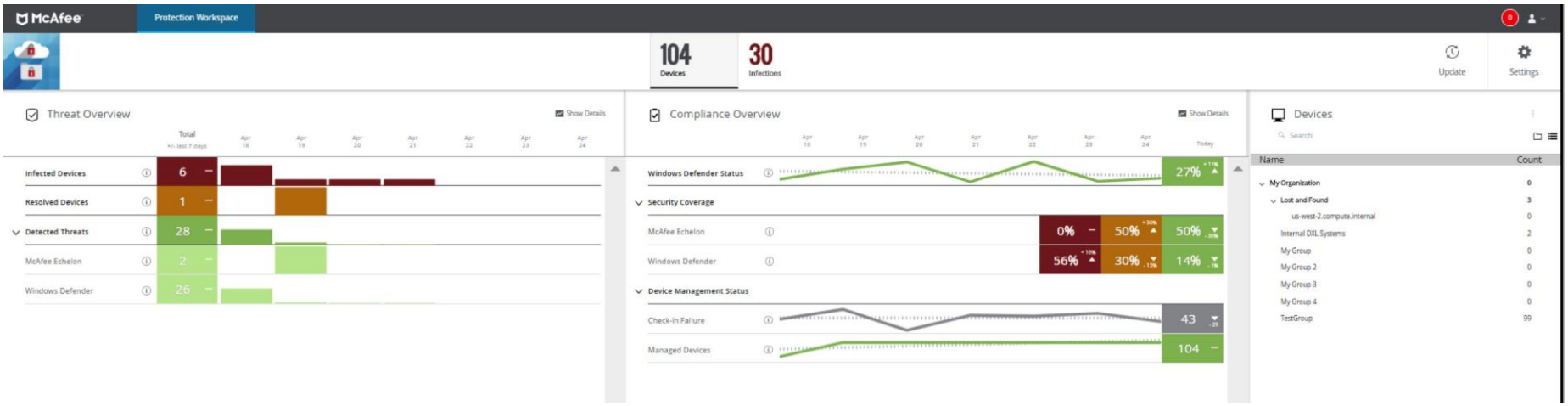
La administración de la seguridad implica complicadas combinaciones entre varias herramientas y una gran cantidad de datos. Esto ofrece una ventaja al adversario ya que le da más tiempo para aprovechar las deficiencias no detectadas entre herramientas, por lo que pueden hacer más daño. El equipo de ciberseguridad es limitado y necesita ser

facultado para orquestar de forma sencilla entornos de ciberseguridad complejos.
Su empresa necesita responder rápidamente a las amenazas en cualquier tipo de dispositivos a fin de minimizar el daño, y el equipo directivo exige que se demuestre la eficacia de la seguridad. La plataforma de administración McAfee® ePolicy Orchestrator® (McAfee ePO™) —disponible in situ y desde la nube (con dos modelos: SaaS o IaaS)— ayuda a eliminar el esfuerzo y el tiempo dedicados a la administración de la seguridad, limita las posibilidades de cometer errores y ayuda a los responsables a responder más rápido y con más eficacia.



1. **Mvision ePo:** La consola de McAfee MVISION ePO le permite conseguir visibilidad crítica, así como definir e implementar automáticamente directivas para garantizar un adecuado estado de seguridad en toda su empresa. Además, excluye la necesidad de mantener una infraestructura de seguridad in situ, permitiendo a los profesionales de la seguridad centrarse exclusivamente en la seguridad. Como oferta SaaS, McAfee MVISION ePO elimina la configuración y mantenimiento de la infraestructura de seguridad, lo que le permite centrarse exclusivamente en supervisar y controlar todos los dispositivos.

Sencillamente acceda desde un navegador con sus credenciales y administre su seguridad. Una solución con una interfaz mejorada siendo más agradable visualmente, sencilla y fácil de usar.

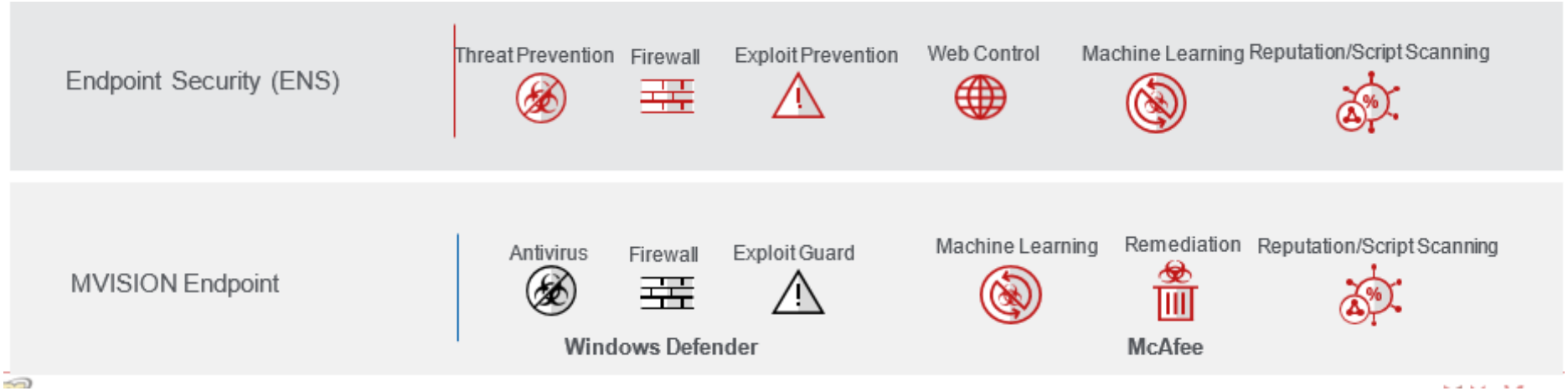


Adicionalmente, la plataforma ampliable de McAfee MVISION ePO administra una gran cantidad de dispositivos, incluidos los que tienen controles nativos. McAfee mejora y administra conjuntamente la seguridad ya integrada en Microsoft Windows 10 para ofrecer una protección optimizada. McAfee MVISION ePO proporciona una experiencia de administración común con directivas compartidas para los dispositivos Microsoft Windows 10 y todos los dispositivos de la empresa para garantizar la coherencia y la simplicidad.

Video: https://www.youtube.com/watch?v=YfJqA12upvQ

2. **McAfee ePo (on-premise):** El software McAfee ePO ofrece funciones de administración flexibles y automatizadas que le permiten identificar, gestionar y responder rápidamente a las vulnerabilidades, cambios en los estados de seguridad y amenazas conocidas desde una sola consola. La plataforma McAfee ePO dispone de funciones avanzadas integradas para aumentar la eficacia del personal de las operaciones de seguridad en su esfuerzo por mitigar una amenaza o realizar un cambio para restaurar el cumplimiento de directivas. La respuesta automática de McAfee ePO puede activar una acción en función de un evento que se haya producido.

Seguridad en el Endpoint - Mvision Endpoint o Endpoint Security (ENS)



1. McAfee MVISION Endpoint Una defensa unificada que aprovecha, refuerza y administra la seguridad básica de sistemas Windows 10, Server 2016 y Server 2019.

Las organizaciones que buscan alternativas más sencillas y asequibles a las plataformas de seguridad para endpoints (EPP) con todas las funciones están optando por el uso de la seguridad nativa del sistema operativo, como Windows Defender. Sin embargo, aunque Defender ofrece la protección básica esencial, sigue siendo necesario aplicar contramedidas avanzadas, como el aprendizaje automático, para disponer de una defensa global frente a las sofisticadas amenazas sin archivos y basadas en malware de tipo zero-day. La clave del éxito es aprovechar, reforzar y administrar la seguridad que ya incluyen los entornos de computadoras de escritorio y servidores Windows, sin introducir la complejidad derivada del uso de varias consolas.

Q: ¿Cómo está protegida su organización de ataques de Ransomware?

A: Mvision tiene el Sistema Rollback remediation, con el cual se puede regresar al estado previo de archivos, lo que hace este componente es volver en el tiempo dando pasos hacia atrás y recuperar los archivos. Lo que es muy útil cuando un ransomware también ataca los back ups o copias de seguridad. https://players.brightcove.net/21712694001/S1o50VS1l_default/index.html?videoId=5804515852001
.

Q: ¿Las soluciones de seguridad que usted posee tienen machine learning o inteligencia artificial?

A: Lo que sucede con soluciones básicas o gratuitas es que solo defienden sus dispositivos de amenazas reconocidas en bases de datos, pero en la vida real constantemente se generan nuevas amenazas que pueden no estar incluidas en estas bases de datos, lo que hace la IA de Mcafee es entender el comportamiento de los archivos para detectar posibles ataques. Adicionalmente, a diferencia de las alternativas que se limitan a una forma de machine learning, McAfee puede realizar análisis de malware estático, de comportamiento y sin archivos para una mayor protección contra amenazas y disminuir los falsos positivos .

https://players.brightcove.net/21712694001/S1o50VS1l_default/index.html?videoId=5810411874001

2. McAfee Endpoint Security (ENS) Seguridad para todos los sistemas operativos (Windows, Mac, Linux)

Se comunica con varias tecnologías de protección de endpoints en tiempo real para analizar y colaborar frente a las amenazas nuevas y avanzadas, bloqueándolas rápidamente antes de que afecten a sus sistemas y usuarios. • Protección antimalware de categoría empresarial, líder del sector, con protección integrada contra amenazas de tipo zero-day.

Seguridad para dispositivos móviles - Mvision Mobile

Proteja a sus empleados y sus dispositivos móviles con McAfee® MVISION Mobile, una solución que detecta amenazas y vulnerabilidades en dispositivos Apple iOS o Google Android, en las redes a las que están conectados y las aplicaciones que los usuarios han descargado.

Las capacidades de detección proporcionan protección si el dispositivo está en línea o no. MVISION Mobile utiliza capacidades de aprendizaje automático alimentadas por miles de millones de puntos de datos de millones de dispositivos para identificar amenazas y ataques actuales o inminentes, incluidos los nunca vistos antes.

Otros componentes:

1. **Data Exchange Layer (DXL):** La estructura de comunicación de Data Exchange Layer (DXL) conecta y optimiza las acciones de seguridad de productos de varios proveedores, así como de las soluciones desarrolladas internamente.
2. **Threat Intelligence Exchange (TIE),** solo ePo on-premise: McAfee® Threat Intelligence Exchange actúa como agente de reputación para permitir la detección y respuesta a amenazas adaptable. Combina inteligencia local de las soluciones de seguridad de su empresa, con datos sobre amenazas globales, externos, y comparte esta inteligencia colectiva con todo su ecosistema de seguridad, lo que permite a las soluciones intercambiar información y actuar en función de la inteligencia compartida.
3. **Adaptative Threat Protection (Real Protect y Dynamic Application Containment):** **Real Protect (RP)** es un método sin firma para determinar si un archivo es malicioso al comparar sus características con comportamientos de malware conocidos. A diferencia de la tradicional detección basada en firmas, ya no necesitamos conocer la familia o variante de malware para determinar si el archivo es malo. Es importante entender que, si bien las firmas pueden determinar con casi certeza que un objeto es malicioso, este método es reactivo en naturaleza y lleva tiempo desarrollar nuevas firmas. Además, las organizaciones necesitan tiempo para aplicar actualizaciones a sus puntos finales.

Dynamic Application Containment (DAC) permite a los administradores proteger la capa más allá de la tradicional categorización

de amenazas "bien conocido / mal conocido", por medio de examinar "grayware" o procesos desconocidos. Esto es particularmente importante ya que las amenazas se vuelven más sofisticados y difíciles de clasificar. El enfoque tradicional de solo AV para proteger el punto final simplemente ya no es suficiente. DAC le permite evaluar desconocidos y aplicaciones potencialmente inseguras, permitiendo que el proceso se ejecute en el sistema, mientras limita las acciones que puede tomar.

4. **Application Control (Solo ePo on-premise):** Los ejecutables desconocidos poseen más amenazas que nunca. McAfee® Application Control brinda protección sin firmas contra el malware de día cero y las amenazas persistentes avanzadas (APT) a través de inteligencia artificial, lista blanca de aplicaciones, reputación de archivos y protección de memoria. Crea y mantiene una lista blanca dinámica de archivos binarios compuesta de ejecutables, archivos DLL, controladores y scripts localmente en cada sistema Los archivos de la lista blanca están protegidos y no se pueden eliminar ni modificar a menos que un cambio es "confiable". El modelo de confianza especifica actualizadores, editores, instaladores, de confianza directorios, usuarios confiables y ventanas de tiempo por las cuales se pueden hacer cambios. Tenga en cuenta que los cambios de confianza se agregan dinámicamente a la lista blanca de las soluciones desarrolladas internamente.

Device Control (Solo ePo on-premise): Los dispositivos USB, reproductores MP3, CD, DVD y otros soportes extraíbles, aunque útiles, constituyen una amenaza real para su organización. Su reducido tamaño y su enorme capacidad de almacenamiento facilitan que los datos confidenciales de clientes y la propiedad intelectual salgan de su empresa y caigan en malas manos a raíz de robos o pérdidas. ¿Cómo saber quién almacena qué y en qué tipo de dispositivo? Y aunque las personas tengan permiso para usar los datos, ¿cómo puede estar seguro de que los mantienen protegidos?

McAfee® Device Control protege los datos importantes impidiendo que salgan de su empresa en soportes extraíbles, como dispositivos USB, Apple iPods, dispositivos Bluetooth, o CD y DVD grabables. Le facilita las herramientas necesarias para supervisar y controlar las transferencias de datos desde todas las computadoras de escritorio y portátiles, independientemente de dónde vayan los usuarios y los datos confidenciales, aunque no estén conectados a la red de la empresa.

McAfee™
Together is power.

jamaya@mps.com.co
www.mcafee.com

4293_0519
MAY 2019