McAfee Data Exchange Layer

Integración simple de aplicaciones, de tipo "una a varias", y comunicación instantánea

Las empresas y desarrolladores pueden ahora conectar, compartir datos y organizar fácilmente las tareas de seguridad entre varias aplicaciones mediante una plataforma de aplicaciones en tiempo real. Un nuevo kit de desarrollo de software (SDK) abierto reduce el trabajo de integración, la inestabilidad y los retrasos que obstaculizan la eficacia de la ciberseguridad.

Deje que McAfee DXL cambie su dinámica de seguridad

Reduzca los flujos de trabajo del ciclo de vida de amenazas
El intercambio de información casi instantánea y la organización de las tareas pueden reducir el tiempo necesario para detectar, contener y corregir las amenazas recién descubiertas.

Reduzca los retrasos, esfuerzos y la complejidad de la integración entre productos de seguridad y proveedores
Nuestra plataforma abierta le permite conectar productos de seguridad de varios proveedores sin sus propias aplicaciones y herramientas, sin esperar a las negociaciones entre proveedores. El poder de elegir está en sus manos.

Aumente el valor de las aplicaciones que despliega
Las aplicaciones pueden ahora compartir los datos sobre amenazas útiles que generan y aconsejar o actuar inmediatamente.

Es probable que esté pagando un precio por la integración. Las integraciones de tipo "una a una", las secuencias de comandos manuales y los procesos programados son las tres formas más comunes que utilizan los equipos de seguridad y sus proveedores para vincular aplicaciones. Estas tácticas obstaculizan la eficacia, la precisión y la velocidad necesarias para que los equipos de ciberseguridad consigan el máximo rendimiento. Limitan su capacidad para compartir inteligencia sobre amenazas, investigar incidentes y organizar las respuestas.

¿Qué se interpone en su camino? El sector de la seguridad no ha contado con una forma sencilla y segura de compartir datos de manera continuada y en tiempo real.

- La infraestructura de seguridad y de TI se ha construido durante muchos años a base de distintas tecnologías, proveedores y aplicaciones internas.
- Las integraciones de productos punto por punto y dirigidas por API son laboriosas de construir y difíciles de mantener cuando se amplían productos y formatos de datos.
- Para cada dos productos de seguridad que haya que integrar, se requiere el acuerdo, la negociación y la implementación de dos proveedores.
- Los modelos de sondeo y publicación de datos programados tradicionales añaden tiempo a cada transacción.

Un estándar y ecosistema abiertos

Existe un método más eficaz, y se está convirtiendo en un estándar abierto del sector como parte de la iniciativa Open Data Exchange Layer (OpenDXL). Los objetivos de la iniciativa OpenDXL son aumentar la flexibilidad y la simplicidad de la integración, y la oportunidad para los desarrolladores de mejorar las operaciones de seguridad de las empresas que la despliegan. La primera fase de la iniciativa ofrece un SDK para ampliar el acceso y uso de McAfee® Data Exchange Layer (DXL) a desarrolladores y participantes, incrementando exponencialmente el valor de una integración o despliegue de DXL.

Los desarrolladores utilizarán este SDK para crear o conectar aplicaciones que se ejecuten en la estructura de comunicación de DXL como una forma segura y en tiempo real de organizar datos y acciones en varias aplicaciones de distintos proveedores, así como en aplicaciones desarrolladas internamente. Evitamos las integraciones únicas producto a producto repetidas.

intel Security

Las aplicaciones sencillamente se publican y suscriben a temas de mensajes o realizan llamadas a servicios de DXL en una invocación solicitud/respuestas similar a las API RESTful. La estructura transmite los mensajes y llamadas inmediatamente, conectando su seguridad, las operaciones de TI y las soluciones internas en un sistema que funciona perfectamente.

Desde la aparición de DXL en 2014, una gran cantidad de proveedores se han unido al ecosistema DXL. Empresas, proveedores de servicios y organismos públicos ya lo utilizan para mejorar sus decisiones y actuar en menos tiempo. Esto reduce los costes operativos, simplifica la protección y la respuesta, y libera valiosos recursos del equipo de seguridad de tareas manuales e intervenciones tácticas de emergencia.

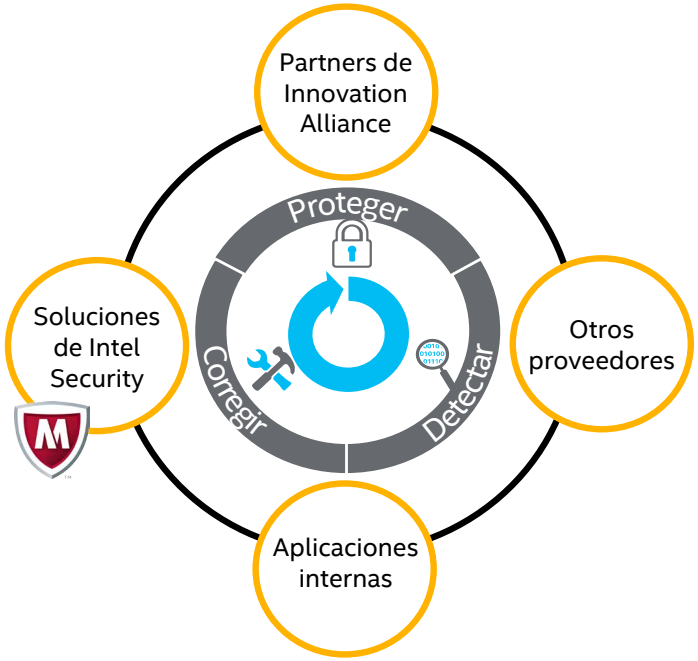

Figura 1. DXL ofrece un modelo de integración rápido y una estructura de comunicación en tiempo real.

Una integración para todas

A diferencia de las integraciones típicas, cada aplicación se conecta a la estructura de comunicación universal de DXL. De esta forma, el proceso de integración queda reducido a una única tarea. OpenDXL admitirá una amplia selección de idiomas, lo que permitirá a los desarrolladores crear integraciones con su entorno de desarrollo favorito. Una app publica un mensaje o solicitud de servicio; una o más apps utilizan el mensaje o responden a la solicitud de servicio. Al igual que en cualquier otro estándar, la interacción es independiente de la arquitectura propietaria subyacente de cada tecnología que se integra. Las integraciones son más simples gracias a esta abstracción de API y requisitos específicos de proveedores.

Además de crear integraciones DXL nativas, los desarrolladores también pueden incluir sus servicios para que interactúen entre ellos o encapsular la API de un producto comercial para que publique datos en DXL. Otros servicios puede escuchar los mensajes y llamadas DXL para enriquecer su funcionalidad con los últimos datos, o adoptar las acciones apropiadas. En el caso de una app más sofisticada, por ejemplo, una utilidad de la organización, este tipo de acciones puede cifrarse conjuntamente para encadenar un conjunto simultáneo de acciones.

Las empresas despliegan una integración y capa de comunicación estandarizada en su propia red, con un pequeño cliente DXL en cada host y una red de intercambio DXL que gestionará

el intercambio de mensajes. Todo el tráfico DXL permanece en la red de esa empresa, lo que ofrecerá privacidad de los datos y control operativo. Un modelo compatible con firewall mantiene una conexión entre el cliente y el servidor para disponer de acceso permanente a la última información que circula por la capa DXL. Si hay algo que cambia en la aplicación que publica o que recibe el mensaje, la capa de abstracción de DXL aísla el resto del despliegue del cambio, reduciendo el riesgo y los costes de mantenimiento de la integración.

Motor de ciberseguridad optimizado

El acceso a tipos de datos actualizados no disponibles hasta ahora puede revolucionar el sector de la seguridad. Sus analistas, equipos de respuesta y equipos operativos están deseando obtener y analizar datos, y actuar en función de esos datos en el menor tiempo posible. A sus proveedores y desarrolladores les encantaría ayudar, pero la integración puede quedar enredada en las complejidades o dependencias técnicas de las alianzas empresariales de sus proveedores.

Estos obstáculos desaparecen ahora, poniendo el poder y la capacidad de elección de nuevo en sus manos.

Sus operaciones de seguridad pueden beneficiarse ahora de datos como:

- Eventos de amenaza asociados a fraudes
- Cambios en la reputación de archivos y aplicaciones
- Dispositivos móviles y activos descubiertos
- Cambios en el comportamiento de redes y usuarios
- Alertas de "alta fidelidad"
- Datos de vulnerabilidades e indicadores de peligro

Los proveedores de software y de soluciones deberían considerar DXL como una infraestructura potente para acelerar las actividades de seguridad y de TI, y dotar de nuevas capacidades a su software y a los usuarios de sus empresas. Los nuevos tipos de datos pueden favorecer análisis más complejos. Las conclusiones pueden traducirse en escalación, contenimiento, corrección o intervención inmediatas. Cuando se examina detenidamente el intercambio de datos en tiempo real y la integración de procesos casi sin fricción, las oportunidades son claras.

Para obtener más información, visite **www.mcafee.com/es/solutions/data-exchange-layer.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