Data Exchange Layer

Integração fácil de um para vários aplicativos e comunicação instantânea

Empresas e desenvolvedores agora podem conectar, compartilhar dados e coordenar tarefas de segurança facilmente entre aplicativos utilizando uma estrutura de aplicativos em tempo real. Um kit de desenvolvimento de software (SDK) novo e aberto reduz o trabalho de integração, a fragilidade e os atrasos que limitam a eficiência da segurança cibernética.

Você provavelmente está pagando uma taxa de integração. Integrações de um para um, scripts manuais e processos agendados são as três maneiras mais comuns pelas quais as equipes de segurança e seus fornecedores vinculam aplicativos. Essas táticas são obstáculos para a eficiência, a precisão e a velocidade necessárias para que as equipes de segurança cibernética obtenham o máximo em desempenho. Elas limitam a sua capacidade de compartilhar inteligência contra ameaças, investigar incidentes e coordenar respostas.

Qual é o obstáculo? O setor de segurança não tinha uma maneira simples e segura de compartilhar dados persistentemente, em tempo real.

- A infraestrutura de TI e de segurança foi construída ao longo de muitos anos a partir de diversas tecnologias, fornecedores e aplicativos próprios.
- Integrações de produtos ponto a ponto, via API, são de construção demorada e manutenção difícil à medida que você atualiza produtos e formatos de dados.
- Para que dois produtos de segurança se integrem, dois fornecedores precisam negociar, entrar em acordo e implementar.
- Modelos tradicionais de polling e publicação programada de dados agregam tempo a cada transação.

Um ecossistema e padrão aberto

Há uma maneira melhor — e ela está se tornando um padrão aberto do setor, como parte da iniciativa Open Data Exchange Layer (OpenDXL). Os objetivos da iniciativa OpenDXL são aumentar a flexibilidade de integração, a simplicidade e as oportunidades para os desenvolvedores e aprimorar as operações de segurança para as organizações que a implementam. A iniciativa OpenDXL oferece um kit de desenvolvimento de software (SDK) para expandir o acesso e o uso do Data Exchange Layer (DXL) para novos desenvolvedores e participantes, aumentando exponencialmente o valor de uma distribuição ou integração DXL.

Deixe que o DXL mude a dinâmica da sua segurança

- **Encurte os fluxos de trabalho do ciclo de vida da defesa contra ameaças:** O compartilhamento quase instantâneo de informações e a coordenação de tarefas podem reduzir o tempo de detecção, contenção e correção de ameaças recém-identificadas.
- **Reduza os atrasos, o trabalho e a complexidade da integração entre produtos e fornecedores de segurança:** Nossa plataforma aberta permite conectar produtos de segurança de múltiplos fornecedores aos seus próprios aplicativos e ferramentas, sem esperar por negociações com os fornecedores. O poder da escolha está em suas mãos.
- **Aumente o valor dos aplicativos que você distribui:** Os aplicativos agora podem compartilhar os úteis dados sobre ameaças que eles geram e orientar ou realizar ações imediatamente.

Os desenvolvedores utilizarão esse SDK para criar ou conectar aplicativos executados sobre a malha de comunicação DXL como uma maneira segura e em tempo real de coordenar dados e ações em múltiplos aplicativos de diferentes fornecedores, bem como aplicativos desenvolvidos internamente. Com isso evitamos integrações repetidas e isoladas de um produto com outro.

Os aplicativos simplesmente publicam e assinam tópicos de mensagens ou fazem chamadas a serviços DXL em uma invocação do tipo requisição/resposta, semelhante às APIs RESTful. A malha entrega as mensagens e chamadas imediatamente, conectando as suas soluções de segurança, TI e próprias em um sistema bem coordenado. O OpenDXL inclui o cliente e o agente DXL de código aberto: OpenDXL Client e OpenDXL Broker. Isso assegura para a organização um autêntico modelo de código aberto para a camada de comunicação entre ferramentas e fontes inteligentes.

Desde o advento do DXL, em 2014, aplicativos de mais de 30 fornecedores uniram-se ao ecossistema DXL, com mais de 100 integrações. Empresas, provedores de serviços e órgãos governamentais já o utilizam para aprimorar decisões e realizar ações em menos tempo. Isso reduz os custos operacionais, agiliza a proteção e a resposta e evita que recursos preciosos da equipe de segurança fiquem presos em tarefas manuais e treinamentos para emergências.

Uma integração que governa tudo

Diferentemente de integrações típicas, cada aplicativo se conecta à malha de comunicação universal DXL. Há apenas um processo de integração em vez de vários.

O OpenDXL oferece suporte para uma ampla gama de linguagens, permitindo que os desenvolvedores criem integrações utilizando seus ambientes de desenvolvimento favoritos. Um aplicativo publica uma mensagem ou chama um serviço; um ou mais aplicativos consomem a mensagem e respondem à requisição de serviço. A integração é independente da arquitetura própria subjacente de cada tecnologia de integração, como é o objetivo de qualquer padrão. As integrações são muito mais simples devido a essa abstração de requisitos e APIs específicos de cada fornecedor.

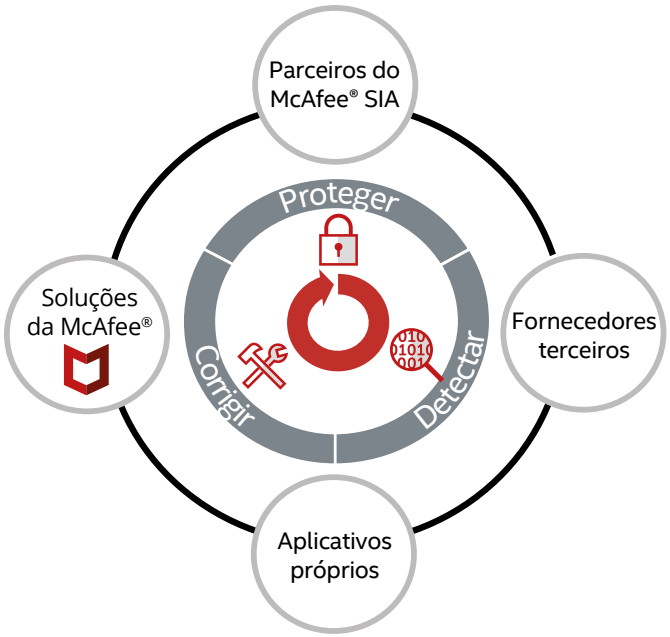

Figura 1. O DXL proporciona um modelo de integração rápida e uma malha de comunicação em tempo real.

Além de criar integrações DXL nativas, os desenvolvedores também podem elaborar seus serviços para interagir ou envolver a API de um produto comercial para publicar dados no DXL. Outros serviços podem ouvir mensagens e chamadas DXL para enriquecer sua funcionalidade com os dados mais recentes ou tomar as providências apropriadas. Para uma coordenação mais sofisticada dos aplicativos envolvidos, esses tipos de ações podem ser reunidas em um script para desencadear uma cascata (ou seja, um conjunto simultâneo) de ações.

As empresas distribuem uma camada padronizada de integração e comunicação em sua rede existente, com um pequeno cliente DXL em cada host e um negociador DXL que gerencie intercâmbios de mensagens. Todo o tráfego DXL fica contido dentro da rede dessa empresa, oferecendo privacidade de dados e controle operacional. Um modelo compatível com firewall mantém uma conexão entre cliente e servidor para acesso contínuo às mais recentes informações que fluem por DXL. Se algo mudar na publicação ou recebimento do próprio aplicativo, a camada de abstração do DXL isolará dessa mudança o restante da distribuição, reduzindo o risco e os custos da manutenção da integração.

Um mecanismo de segurança cibernética melhor

O acesso a tipos de dados atualizados até o último minuto, que antes não estavam disponíveis, muda totalmente as regras do jogo. Os seus analistas, encarregados de resposta a incidentes e equipes operacionais já estão ansiosos por obter, analisar e realizar ações com base em dados no menor tempo possível. Seus fornecedores e desenvolvedores adorariam ajudar, mas a integração pode esbarrar em complexidades técnicas ou na dependência de parcerias comerciais dos seus fornecedores.

Esses obstáculos agora se dissiparam, colocando o poder e a escolha novamente nas suas mãos.

Agora suas operações de segurança podem se beneficiar instantaneamente de dados como:

- Eventos de ameaças enganosas.
- Mudanças de reputação de arquivos e aplicativos.
- Ativos e dispositivos móveis descobertos.
- Mudanças de comportamento de redes e usuários.
- Alertas de alta fidelidade.
- Dados de vulnerabilidade e indicadores de comprometimento (IoC).

Os fornecedores de software e de soluções devem encarar o DXL como uma estrutura poderosa para agilizar atividades de TI e de segurança e viabilizar novas capacidades em seu software e nas organizações de seus clientes. Novos tipos de dados podem alimentar análises mais complexas. Conclusões podem desencadear escalação, contenção, correção ou intervenção imediata. Quando olhamos pela lente do compartilhamento de dados em tempo real e integração quase perfeita de processos, o que vemos são oportunidades.

Saiba mais

Comece já em **www.mcafee.com/br/solutions/data-exchange-layer.aspx**.

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br