

# Data Exchange Layer

## 轻松、一对多应用程序集成和即时通信

企业和开发者现在可以使用实时应用程序框架轻松在应用程序间连接、共享数据和编排安全任务。一种新的开放式软件开发包 (SDK) 降低了一直在阻碍网络安全的集成工作、脆弱性和时间延迟。

您或许正在支付整合税。一对一集成、手工脚本和计划过程是安全团队及其供应商链接应用程序时采用的三种最常见方法。这些战术阻碍了网络安全团队实现最高性能而必需的效率、准确性和速度。这限制了您分享威胁情报、调查事故和协调响应的能力。

哪些因素造成了阻碍？安全行业还没有一种简单、安全的方式来持久、实时地共享数据。

- 安全和 IT 基础设施多年来一直从不不同的技术、供应商和内部应用程序累积。
- 点到点、API 引导的产品集成在构建时不仅耗时，而且在您升级产品和数据格式时难以维护。
- 要让两种安全产品集成，两个供应商必须协商、达成一致并实施。
- 传统的投票和计划数据发布模型在每个事务中增加了时间。

### 开放标准和生态系统

有一种更好的方法，也正在成为一种开放行业标准，而且是 Open Data Exchange Layer (OpenDXL) 计划的一部分。OpenDXL 计划的目标是提高开发者的集成灵活性、简洁性和机遇，并且改善部署组织的安全运营。OpenDXL 计划提供了软件开发工具包 (SDK) 来将 Data Exchange Layer (DXL) 的访问和使用扩展到新开发者和参与者，从而以指数级提高 DXL 集成或部署的价值。

开发者将使用此 SDK 来创建或连接通过 DXL 通信结构运行的应用程序，以此作为一种安全、实时方法在不同供应商的多个应用程序以及内部开发应用程序之间协调数据和操作。我们避免重复的一次性产品与产品集成。

### 让 DXL 改变您的安全动态

- **缩短威胁防御生命周期的工作流程**  
几乎即时共享任务的信息和协调，这将降低检测、遏制和更正新识别威胁的时间。
- **减少安全产品和供应商之间的集成延迟、工作量和复杂性**  
我们的开放平台使您可以将来自多个供应商的安全产品与您自己的应用程序和工具互连，无需等待供应商协商。选择权在您的手中。
- **提高您部署的应用程序的价值**  
应用程序现在可以共享其生成的有用数据，并且可以立即引导或采取操作。

## 产品简介

应用程序只需要发布和订阅消息主题，或者以类似于 RESTful API 的方式，在请求/响应调用中调用 DXL 服务。这种架构可立即提供消息和调用，从而将您的安全、IT 和内部解决方案连接到功能正常的系统。OpenDXL 包括开源 DXL 客户端和代理：OpenDXL 客户端和 OpenDXL Broker。这样可以保证为组织的工具和情报源之间的通信层实施真正的开源模型。

自 DXL 在 2014 年首次提出以来，已经有 30 多家供应商和应用程序加入了 DXL 生态系统，集成数超过 100 个。企业、服务提供商和政府组织已经使用 DXL 来改善决策并在更少的时间内采取操作。这将降低运营成本，简化保护和响应，并让宝贵的安全团队资源不用再执行手动任务，也不会再在出现问题时匆忙应对。

### 一种统一的集成

与典型集成不同的是，每个应用程序连接到通用 DXL 通信架构。只有一个集成过程，避免重复工作。OpenDXL 将支持大量语言，使开发者能够使用自己喜爱的开发环境来创建集成。一个应用程序发布一条消息或调用一个服务；一个或多个应用程序使用消息或响应服务请求。与所有标准的目标一样，集成与每种集成技术的底层专有体系结构无关。由于来自特定于供应商的 API 和要求的抽象化，因此集成的复杂程度大大降低。

除了创建本机 DXL 集成之外，开发者还可以包装其服务以进行交互或者包装商业产品的 API 以将数据发布到 DXL。其他服务可以侦听 DXL 消息和调用，以使用最新数据来丰富其功

能或者采取相应的操作。对于反映协调的更复杂应用程序，这些类型的操作可以一起脚本化，以驱动瀑布或者操作的并发集合。

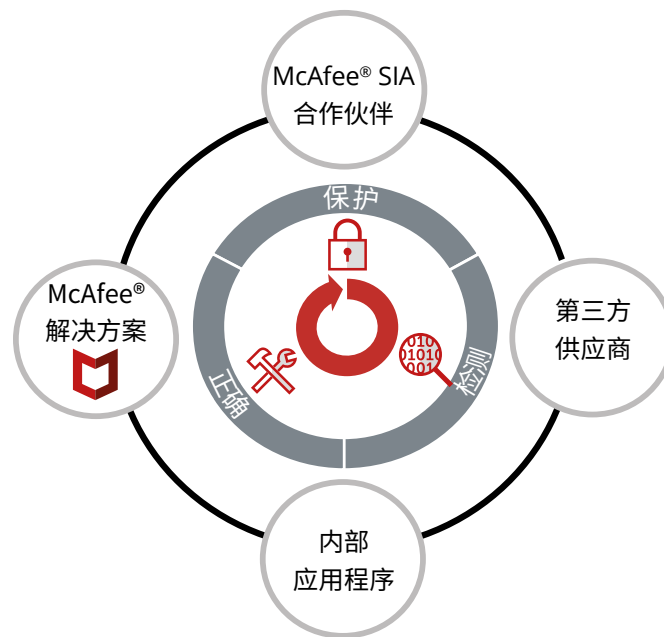


图 1. DXL 提供快速集成模型和实时通信架构。

企业在其现有网络中部署标准化集成和通信层，小型 DXL Client（安装在每个主机上）和 DXL 代理将负责管理消息交换。所有 DXL 流量均包含在企业网络中，可提供数据隐私和运营控制。防火墙友好的模型可保持客户端与服务器的连接，以持续访问流经 DXL 的最新信息。如果发布或接收应用程序自身时发生某些更改，则 DXL 抽象层会将其余部署与更改隔离，以降低集成维护的风险和成本。

## 产品简介

### 更好的网络安全引擎

对于安全性而言，能够访问先前不可用类型的最新数据成为了游戏规则改变者。您的分析师、响应者和运营团队已经迫不及待要在可能的最短时间内获取、分析和处理数据。您的供应商和开发者将乐意帮忙，但集成可能陷入技术复杂性或者依赖于供应商的业务合作关系这一困境。

这些障碍现在已烟消云散，您重新掌控了权利与选择。

您的安全运营现在可以立即通过数据获得优势，比如：

- 欺骗威胁事件。
- 文件和应用程序声誉改变。
- 发现移动设备和资产。
- 网络和用户行为改变。
- 高保证警报。
- 漏洞和感染指标 (IoC) 数据。

软件和解决方案供应商应将 DXL 视为强有力框架，用以加速安全和 IT 活动以及在其软件及其客户的组织中实现新功能。新数据类型可以推动更复杂的分析。结论可以触发立即提升、遏制、补救或干预。从实时分享数据和几乎无冲突流程集成的角度来看，您将发现新机遇。

### 了解更多信息

---

在 [www.mcafee.com/cn/solutions/data-exchange-layer.aspx](http://www.mcafee.com/cn/solutions/data-exchange-layer.aspx) 了解入门知识。



北京市东城区北三环东路 36 号  
北京环球贸易中心 D 座 18 层, 100013  
电话: 8610 8572 2000  
[www.mcafee.com/cn](http://www.mcafee.com/cn)

McAfee、迈克菲和 McAfee 徽标是 McAfee, LLC 或其分支机构在美国和/或其他国家/地区的注册商标或商标。其他商标和品牌可能是其各自所有者的财产。  
Copyright © 2018, McAfee, LLC. 4131\_1018  
2018 年 10 月