McAfee
Together is power.

# Data Exchange Layer (DXL)

**Q: What is the Data Exchange Layer?**

**A:** Data Exchange Layer (DXL) is a secure, real-time way to unite data and actions across multiple applications from different vendors as well as internally developed applications. It helps enterprises:

- Shorten the workflows of the threat defense lifecycle. Near-instant sharing of information and orchestration of tasks can shrink time to detect, contain, and correct newly identified threats.
- Reduce integration delays, effort, and complexity across security products and vendors. Our open platform lets you connect security products from multiple vendors with your own applications and tools, without waiting for vendor negotiations. The power of choice is in your hands.
- Increase the value of the applications you deploy. Applications can now share the useful threat data they generate and guide or take action immediately.

## Why DXL?

**Q: How is DXL different from existing and alternative approaches?**

**A:** One-to-one integrations, manual scripts, and scheduled processes are the three most common ways security teams and their vendors' link applications. DXL replaces these slow, unidirectional, and manual integration processes with a fast and simple communication fabric that allows for bidirectional sharing with other connected systems. Instead of a series of individual integrations, all components connect to DXL. Apps simply publish and subscribe to message topics or make calls to DXL services in a request/response invocation like RESTful application programming interfaces (APIs). The fabric delivers the messages and calls immediately, connecting an enterprise's security, IT, and in-house solutions into a well-functioning system. If something in the publishing or receiving application itself changes, the DXL abstraction layer insulates the rest of the deployment from the change, reducing risk and costs of integration maintenance. The beauty of the DXL is that you integrate once to the DXL fabric and then have access to all the applications that are on the fabric—no more one-to-one integrations.

**Q: How does using DXL make a partner or customer's software better?**

**A:** DXL allows a partner or customer's software to "speak the same language." This results in a swifter and more efficient exchange of information throughout the infrastructure, as communication across DXL is uniform.

Connect With Us

## DXL Background

**Q: What is the history of DXL?**

**A:** DXL was a technology developed by McAfee originally in 2014 for internal use to optimize speed and effectiveness of product integrations. It was so successful the technology was made available to McAfee® Security Innovation Alliance partners in 2015 to optimize the speed and effectiveness of third-party integrations.

Building on the success of internal and partner integrations, McAfee announced in November 2016 the OpenDXL initiative, making DXL technology available to the entire industry. Anyone is free to integrate their products or home-grown solutions with DXL, whether they are a McAfee customer or partner or not. The OpenDXL initiative allows for open sourcing the DXL client, making the DXL broker freely available as a Docker container and launching the community driven opendxl.com website.

## Embracing DXL

**Q: What does an enterprise need to deploy DXL?**

**A:** Enterprises deploy a standardized integration and communication layer over their existing network, with a small DXL client and one or more DXL broker(s) that will manage message exchanges. View the ***DXL Architecture Guide*** for additional references and suggestions on deploying a DXL environment.

**Q: How do you manage DXL?**

**A:** DXL may be managed via the McAfee® ePolicy Orchestrator® (McAfee ePO™) console or deployed and managed as a Docker broker. The brokers managed via McAfee ePO platform can be chained together for scalability. The Docker broker is available on opendxl.com and is a single broker.

**Q: What is the price of DXL?**

**A:** DXL is free. It comes with any McAfee product, and, for non-McAfee customers, the Docker version of DXL can be downloaded for free on opendxl.com

**Q: What are the types of integrations people are doing with DXL?**

**A:** Current partners have different types of DXL integrations that can be found **here**. Enterprises can use the software development kit (SDK) for a variety of integrations and you can find more **information here**.

## OpenDXL

**Q: What is OpenDXL?**

**A:** The Open Data Exchange Layer (OpenDXL) is an initiative enabling developers to leverage the DXL technology in order to connect products throughout security infrastructure. OpenDXL provides an open, simple way to integrate technologies from different vendors with each other and with in-house developed applications for gaining unprecedented

real-time access to incredibly critical security intelligence and context. This new data access, with data delivered in microseconds, is helping drive new functionality—such as more precise analysis and orchestration of security actions with IT systems—and opens integrations between competitors and small developers that would typically not happen under standard market conditions. To help the industry accelerate the threat defense lifecycle, we have made available an OpenDXL Software Developer Kit (SDK) and the open source web community infrastructure. This enables more partners and developers within companies, colleges, and even competitors to gain the real-time, one-to-many integration benefits of OpenDXL.

Ultimately, OpenDXL brings the integration capability to everyone—customers, non-customers, partners, non-partners, and competitors.

**Q: What is the difference between DXL and OpenDXL?**

**A:** DXL is the technology, and OpenDXL is the initiative.

**Q: What is the difference between DXL broker versus the broker on opendxl.com?**

**A:** The DXL brokers are deployed and managed via the McAfee ePO console; multiple brokers of this type can be chained together. The broker available on opendxl.com is a single broker deployed as a Docker container.

## Embracing OpenDXL

**Q: What type of licensing is required for OpenDXL?**

**A:** The OpenDXL client is released under an Apache 2.0 license.

**Q: Where is the OpenDXL SDK located?**

**A:** The OpenDXL SDK is located on opendxl.com

**Q: Why is the OpenDXL Python client important?**

**A:** Openness and flexibility in software options and integrations helps customers adapt more readily and adopt new ideas, technologies, and capabilities more quickly at a lower cost. The OpenDXL Python client has gone through thorough validation and testing, which means enterprises can rely confidently on this software as they develop their OpenDXL integrations. Also note that the software is open source, so no support is offered or promised.

**Q: What are the OpenDXL wrappers?**

**A:** OpenDXL wrappers provide the capability of taking an existing products REST API and wrapping it to expose it on the DXL as a service. Once exposed, all products that are on the DXL can integrate with the wrapped product without needing to know the inner workings of the underlying API, as everything speaks the same language. This integration effort is much less than a direct integration with that product's API.

**Q: How to I obtain a wrapper?**

**A:** Opendxl.com has many pre-built OpenDXL wrappers ready to be downloaded and used.

## CUSTOMER FAQ

**Q: Can I create a wrapper for my products?**

**A:** Yes, we encourage you to contribute to this ecosystem. An example of how easy it is to create an OpenDXL wrapper is available **here**.

**Q: What is the McAfee ePO console management wrapper?**

**A:** The new wrapper for McAfee ePO console management APIs opens up easy, fast options to use industry leading McAfee ePO software to apply policies, tag systems, move groups, and trigger actions on their applications. These are the most frequent and most valuable integration capabilities available within the McAfee ePO console web APIs, and permit more applications to leverage centralized and efficient management with a lightweight integration process.

**Q: Are there any testing or certification programs?**

**A:** With our McAfee Security Innovation Alliance partners, there is a mandatory certification process. Integrations published on opendxl.com are not subject to certification testing.

**Q: How will OpenDXL control access to data?**

**A:** This will be in each customer's hands and set through policy.

**Q: How can I be sure my data doesn't get into the wrong hands?**

**A:** DXL is designed so that the data stays within each discrete instance. Communication over the DXL fabric is secured via TLS version 1.2 and PKI mutual authentication. The fabric also supports topic-level authorization to restrict which clients can publish messages to a topic and which clients can receive messages on a particular topic. For example, the DXL clients embedded in the McAfee Threat Intelligence Exchange servers are the only ones authorized to publish reputation change events to the topic /mcafee/event/tie/file/ repchange.

**Q: What is the difference between DXL and STIX/ TAXII?**

**A:** Let's start by separating Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) into their functional areas. STIX is a format of data used to describe indicators of compromise (IoCs). It is the STIX file that contains all of the useful information that enterprises use. TAXII is merely the transport layer utilized to transport STIX files, so in that respect, TAXII is similar to DXL with the big exception that TAXII is only used to transport STIX files, not data in other formats. Conclusion: TAXII is very narrow in its focus.

Contrast that to DXL. DXL is also a transport layer but has a much broader range of capabilities and therefore use cases. It can transport STIX data as a DXL message to deliver on the IoC use case, but it is also so much more, as it is able to transport data in any format—for example, threat data, reputation data, vulnerability data, alerts, and so on. The power of DXL is to function as a transport layer abstracted from the format of data being delivered. Conclusion: Not only can DXL transport STIX data, it can transport data from a variety of formats.

## McAfee DXL and OpenDXL Integrations

**Q: Why did McAfee and Cisco decide to integrate DXL and pxGrid?**

**A:** Cisco's pxGrid operationally functions in a very similar way to DXL. pxGrid has more of a network focus, whereas DXL has more of an endpoint focus and integrating these two fabrics brings the best of both worlds to the industry. For example, now pxGrid integrated network devices can pass information of newly discovered machines joining the network through to DXL and invoke automatic security software deployment through McAfee ePO software.

**Q: What is a common use case for McAfee ePO platform and DXL integration?**

**A:** McAfee ePO platform and DXL integration delivers an automated incident response capability by automatically reacting to threat events, sending data to DXL to disseminate among connected products for action.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847 8766
www.mcafee.com