Data Exchange Layer

Easy, one-to-many application integration and instant communication

Enterprises and developers can now easily connect, share data, and orchestrate security tasks across applications using a real-time application framework. A new, open software development kit (SDK) reduces the integration effort, fragility, and time delays that are holding back cybersecurity efficiency.

You are probably paying an integration tax. One-to-one integrations, manual scripts, and scheduled processes are the three most common ways security teams and their vendors link applications. These tactics stand in the way of the efficiency, accuracy, and speed required for cybersecurity teams to achieve maximum performance. They limit your ability to share threat intelligence, investigate incidents, and orchestrate response.

What is standing in the way? The security industry has not had a simple, secure way to share data persistently, in real time.

- Security and IT infrastructure has been built up over many years from disparate technologies, vendors, and in-house applications.
- Point-to-point, application programming interface (API)-led product integrations are time-consuming to build and difficult to maintain as you upgrade products and data formats.
- For two security products to integrate, two vendors have to negotiate, agree, and implement.
- Traditional polling and scheduled data-publishing models add time to each transaction.

An Open Standard and Ecosystem

There is a better way—and it is becoming an open industry standard as part of the open Data Exchange Layer (OpenDXL) initiative. The goals of the OpenDXL initiative are to increase integration flexibility, simplicity, and opportunity for developers and to improve security operations for organizations that deploy it. The OpenDXL initiative provides a software development kit (SDK) to expand access to and use of the Data Exchange Layer (DXL) to new developers and participants, exponentially increasing the value of a DXL integration or deployment.

Developers will use this SDK to create or connect applications that run over the DXL communication fabric as a secure, real-time way to orchestrate data

Let DXL Change Your Security Dynamics

- **Shorten the workflows of the threat defense lifecycle:** Nearly 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.

Connect With Us

and actions across multiple applications from different vendors as well as internally developed applications. We avoid repeated, one-off product-to-product integrations.

Applications simply publish and subscribe to message topics or make calls to DXL services in a request/response invocation similar to RESTful APIs. The fabric delivers the messages and calls immediately, connecting your security, IT, and in-house solutions into a well-functioning system. OpenDXL includes the open-sourced DXL client and broker: OpenDXL Client and OpenDXL Broker. This assures organization a true open source model for their communication layer between tools and intelligent sources.

Since DXL debuted in 2014, applications from more than 30 vendors have joined the DXL ecosystem with more than 100 integrations. Enterprises, service providers, and government organizations already use it to improve decisions and take action in less time. This lowers operating costs, streamlines protection and response, and frees valuable security team resources from manual tasks and tactical fire drills.

One Integration Rules Them All

Unlike typical integrations, each application connects to the universal DXL communication fabric. There is just one integration process instead of multiple efforts. OpenDXL will support a broad range of languages, enabling developers to create integrations using their favorite development environment. One application publishes a message or calls a service; one or more applications consume the message or respond to the service request. As is the goal for any standard, the interaction is independent of the underlying proprietary architecture of each integrating technology. Integrations are much simpler because of this abstraction from vendor-specific APIs and requirements.

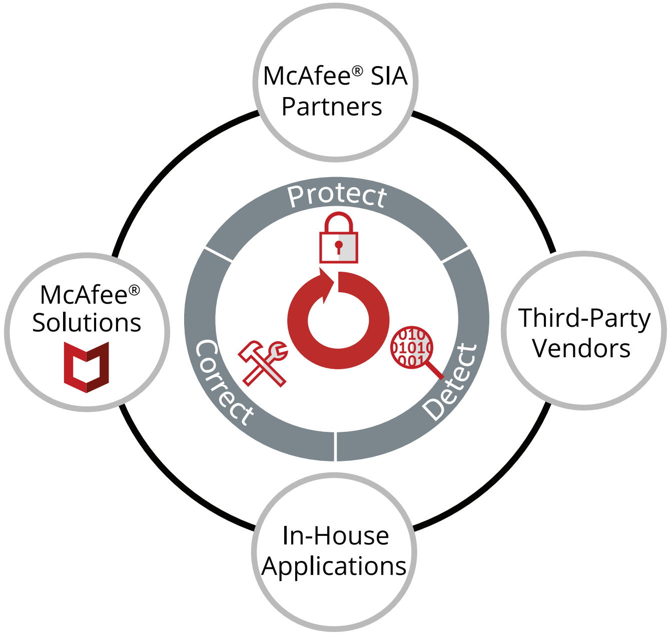

Figure 1. DXL provides a rapid integration model and real-time communication fabric.

In addition to creating native DXL integrations, developers can also wrap their services to interact or wrap the API of a commercial product to publish data onto DXL. Other services can listen to DXL messages and calls to enrich their functionality with the latest data or take appropriate action. For a more sophisticated application reflecting orchestration, these sorts of actions can be scripted together to drive a waterfall, or a simultaneous set of actions.

Enterprises deploy a standardized integration and communication layer on their existing network, with a small DXL client on each host and a DXL broker that will manage message exchanges. All DXL traffic is contained within that enterprise's network, offering data privacy and operational control. A firewall-friendly model maintains a connection between client and server for continuous access to the latest information flowing over the DXL. 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.

A Better Cybersecurity Engine

Access to previously unavailable types of up-to-the-minute data is a game changer for security. Your analysts, responders, and operational teams are already hungry to obtain, analyze, and take action on data in the least possible time. Your vendors and developers would are eager to help, but integration may become mired in technical complexities or dependencies on your vendor's business partnerships.

These obstacles now evaporate, placing power and choice back in your hands.

Your security operations can now get instant benefits from data such as:

- Deception threat events
- File and application reputation changes
- Mobile devices and assets discovered
- Network and user behavior changes
- High-fidelity alerts
- Vulnerability and indicator of compromise (IoC) data

Software and solution vendors should look to DXL as a potent framework for expediting security and IT activities and enabling new capabilities in their software and their customers' organizations. New data types can fuel more complex analytics. Conclusions can spark immediate escalation, containment, remediation, or intervention. When you look through the lens of real-time sharing of data and almost friction-less process integration, you see new opportunities.

Learn More

Get started at mcafee.com/dxl.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com