Trellix

DATA SHEET

Trellix Data Exchange Layer

One-to-many application integration and instant communication

Overview

Let DXL change your security dynamics

- **Shorten the threat defense lifecycle workflow:** Instant information sharing, and task orchestration helps shrink the time to detect, contain, and correct newly identified threats.
- **Reduce integration complexity across security products and vendors:** Our open platform lets you connect security products from multiple vendors with your own applications and tools. 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 be guided to take action immediately.

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

Many popular security tactics limit the efficiency, accuracy, and speed required for cybersecurity teams to achieve maximum performance. One-to-one integrations, manual scripts, and scheduled processes are the three most common ways security teams and their vendors link applications. But these choices limit your ability to share threat intelligence, investigate incidents, and orchestrate response.

What's standing in the way?

The security industry has not had a simple, secure way to share data continuously 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 API-led product integrations are time-consuming to build and difficult to maintain as you upgrade products and data formats.
- Traditional polling and scheduled data-publishing models add time to each transaction.
- For two security products to integrate seamlessly, they have to be integrated at the API level and implemented quickly. This holds true for all products across the board.

An open standard and ecosystem

There's a better way—and it's 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 an SDK to expand access to and use of the 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. It's a secure, real-time way to orchestrate data and actions for both internally developed applications and across multiple applications from different vendors. With the SDK, your organization can 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 OpenDXL Client and OpenDXL Broker. This assures your organization a true open source model for the 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 faster. This lowers operating costs, streamlines protection and response, and frees valuable security team resources from manual tasks and tactical fire drills.

Additionally, the Trellix Security Innovation Alliance (SIA) provides organizations with integrated security solutions that allow them to resolve more threats faster with fewer resources. SIA partners are screened for innovation, strategic value, and leadership in their market segments, which also complement the Trellix solution portfolio.

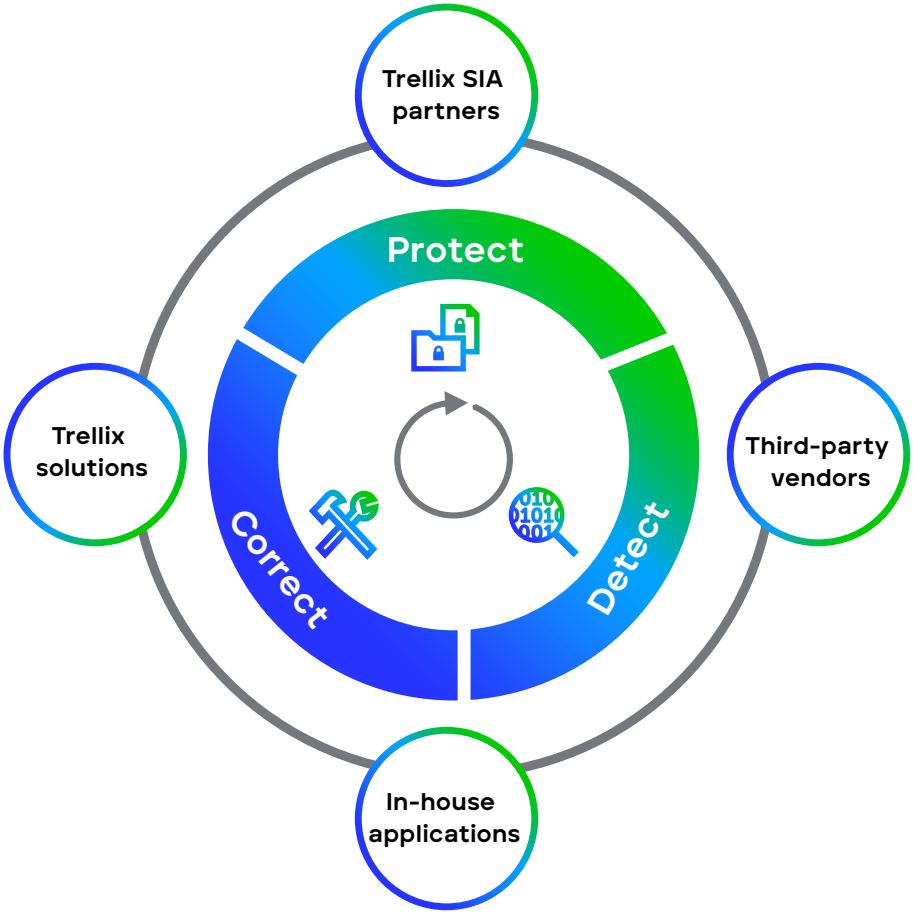

Figure 1. DXL provides a rapid integration model and real-time communication fabric

One integration, many benefits

Unlike typical integrations, each application connects to the universal DXL communication fabric. There's 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, and 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 technology. Integrations are much simpler because of this abstraction from vendor-specific APIs and requirements.

In addition to creating native DXL integrations, developers can also build 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 as quickly as possible. Your vendors and developers 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, including:

- 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 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 data sharing and almost frictionless process integration, you see new opportunities.

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.