OpenDXL Integration Planning

Your current option for integration is:

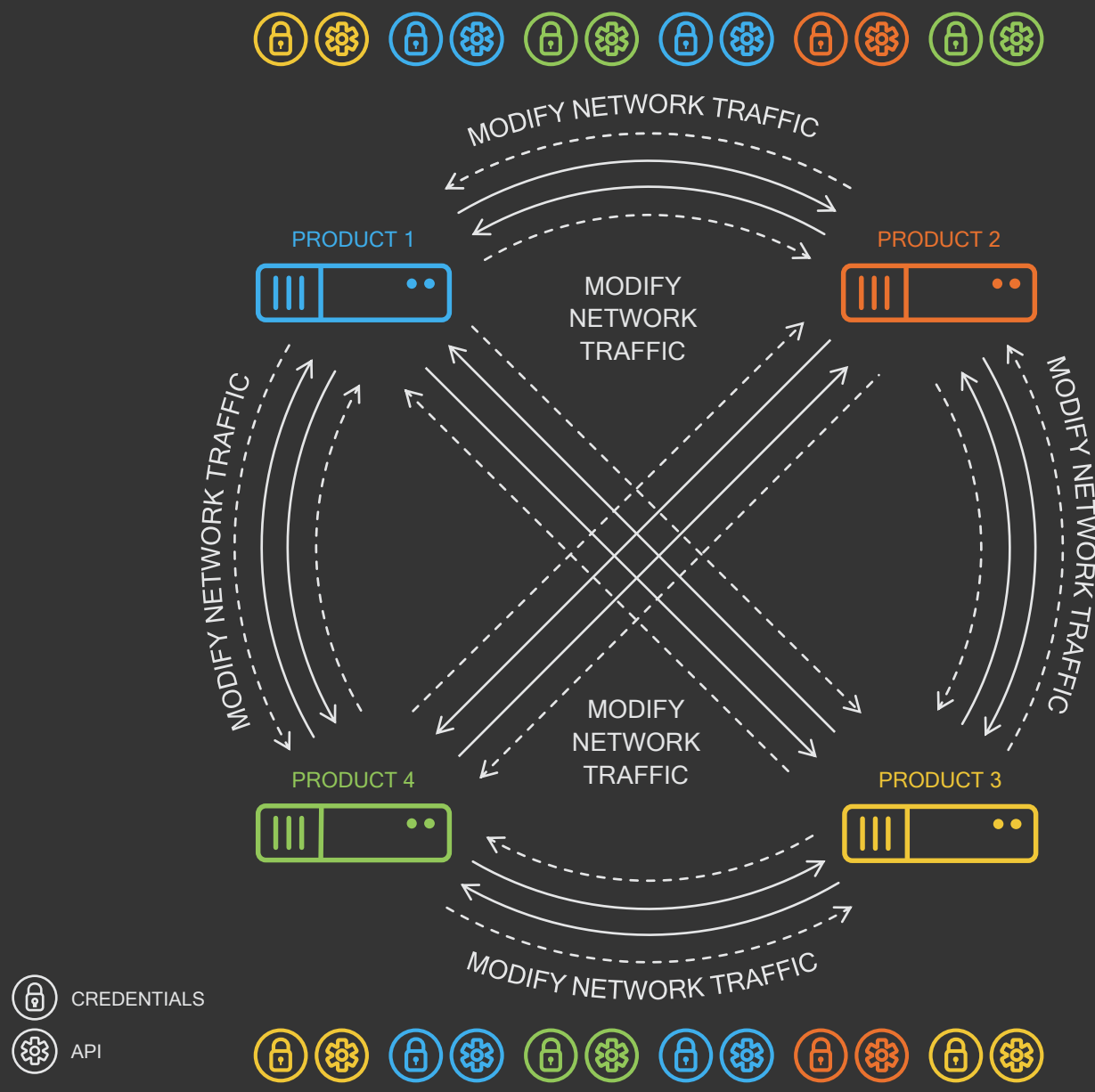
Expensive

Time-consuming

Fragile

Hard

We know integration isn't easy—or cheap. You're at the whim of your vendors' APIs and a simple change can blow up your system. It's just not a viable option.

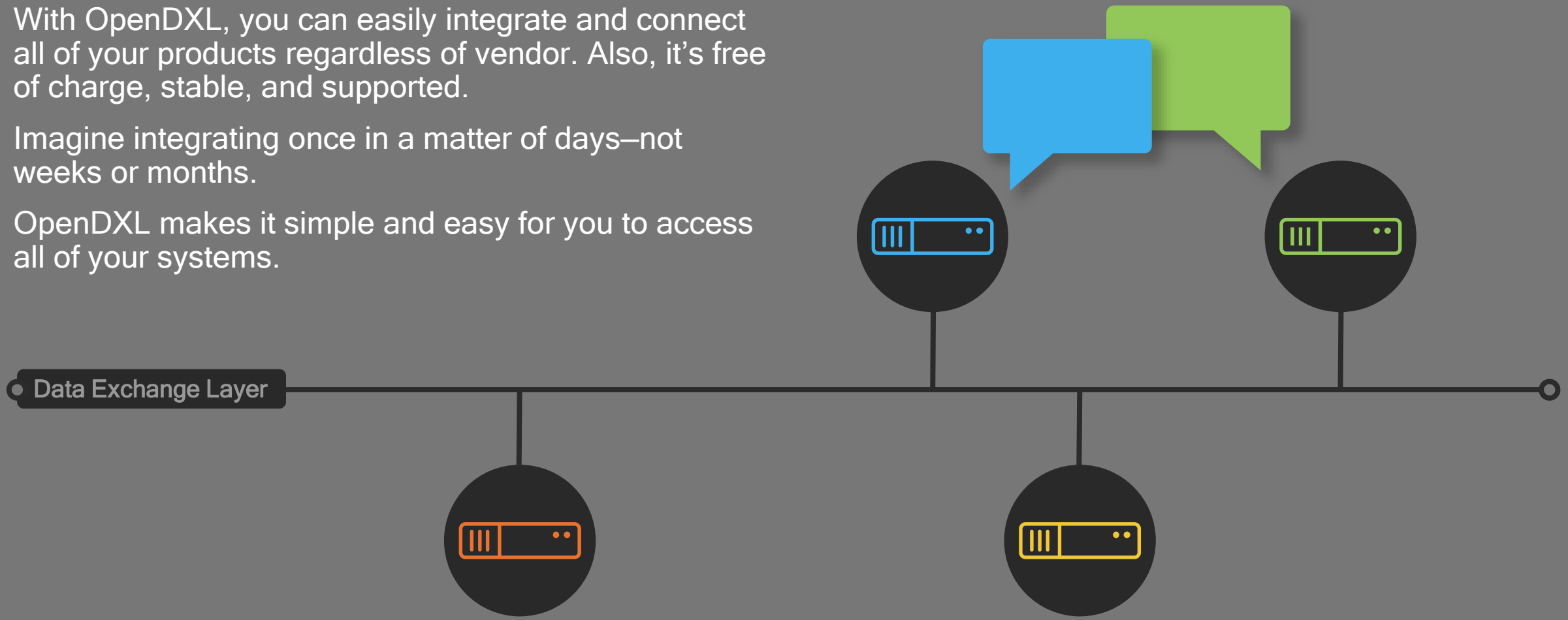


OpenDXL makes it simple

With OpenDXL, you can easily integrate and connect all of your products regardless of vendor. Also, it's free of charge, stable, and supported.

Imagine integrating once in a matter of days–not weeks or months.

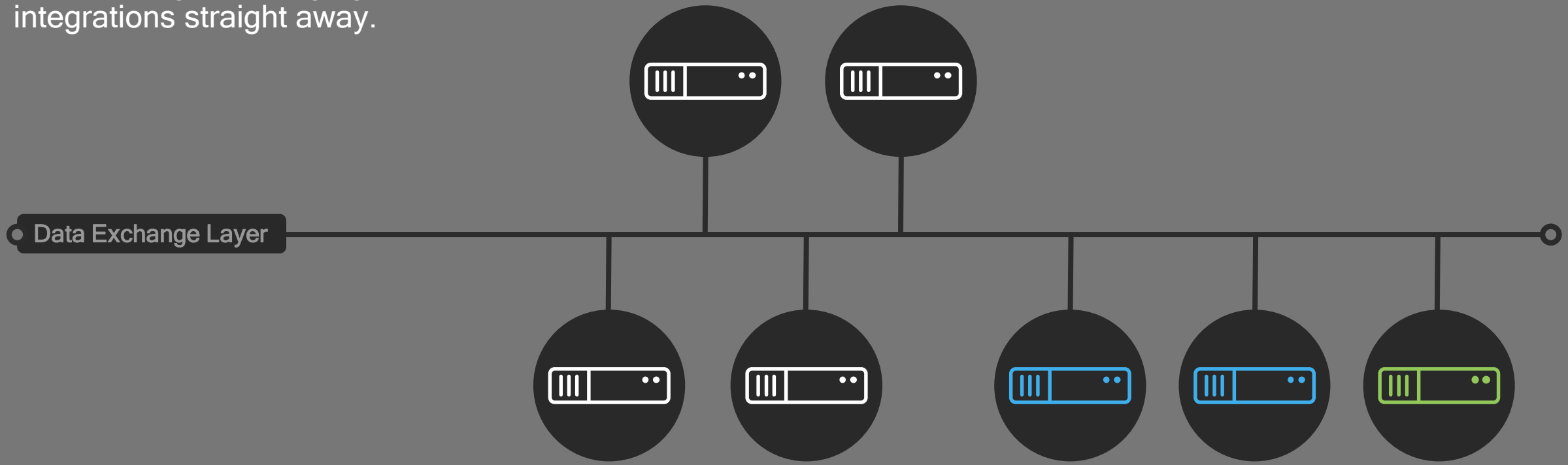
OpenDXL makes it simple and easy for you to access all of your systems.



Integrating products with native DXL integrations

Products with native DXL integrations are already connected to DXL with no work on your part.

You can begin leveraging these integrations straight away.



Your Product

Integrating all other products

Service Wrappers

Create

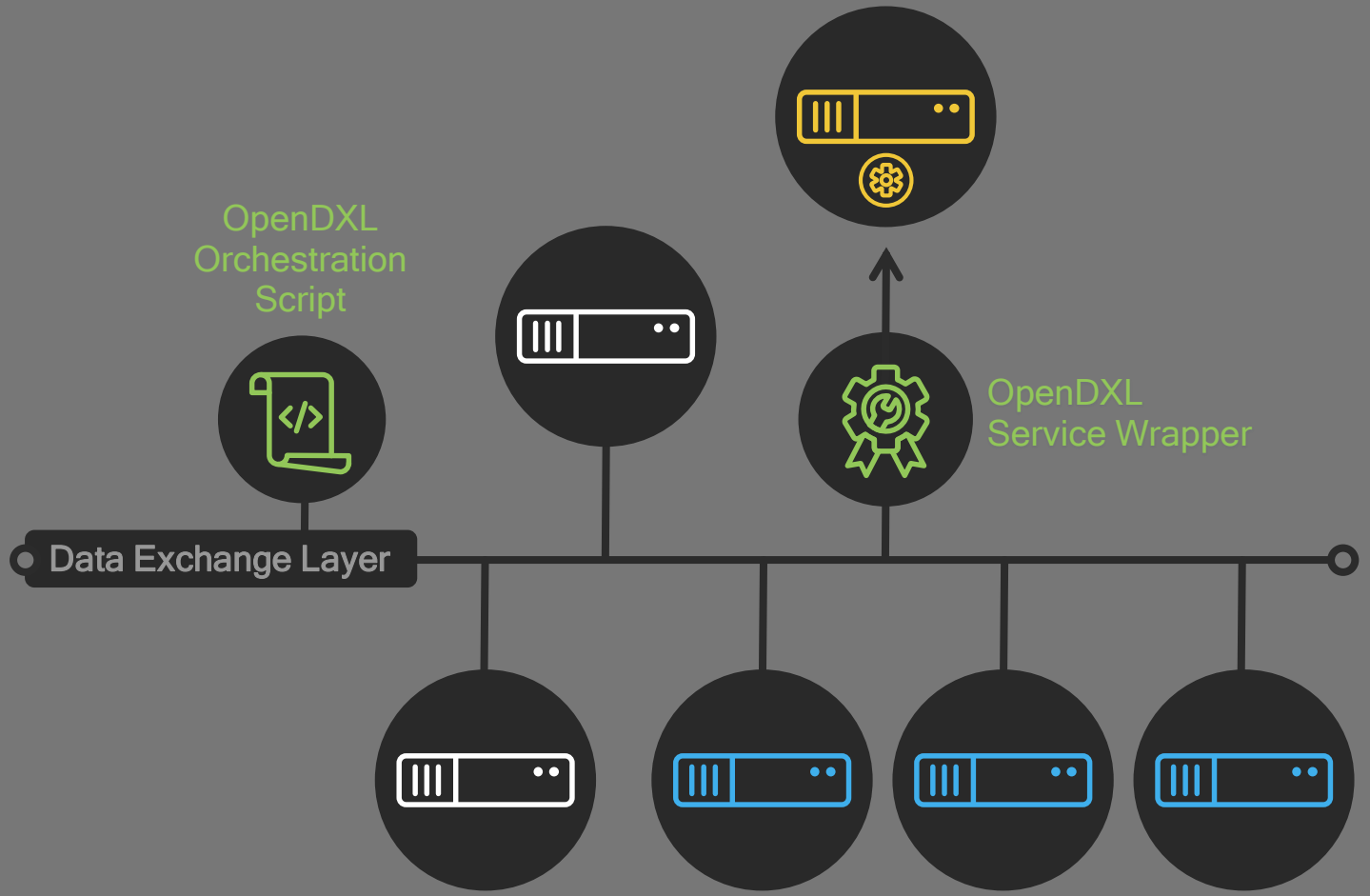
Let's say you have a third party product that needs to be integrated into the DXL but it doesn't have a native DXL integration.

Or, that you have a proprietary product you've developed internally…

OpenDXL makes it easy for you to create your own DXL integrations.

By creating a Service Wrapper, any products with a REST API can be integrated into the DXL.

You can either create this Service Wrapper yourself…



Integrating all other products

Service Wrappers

Use previously created

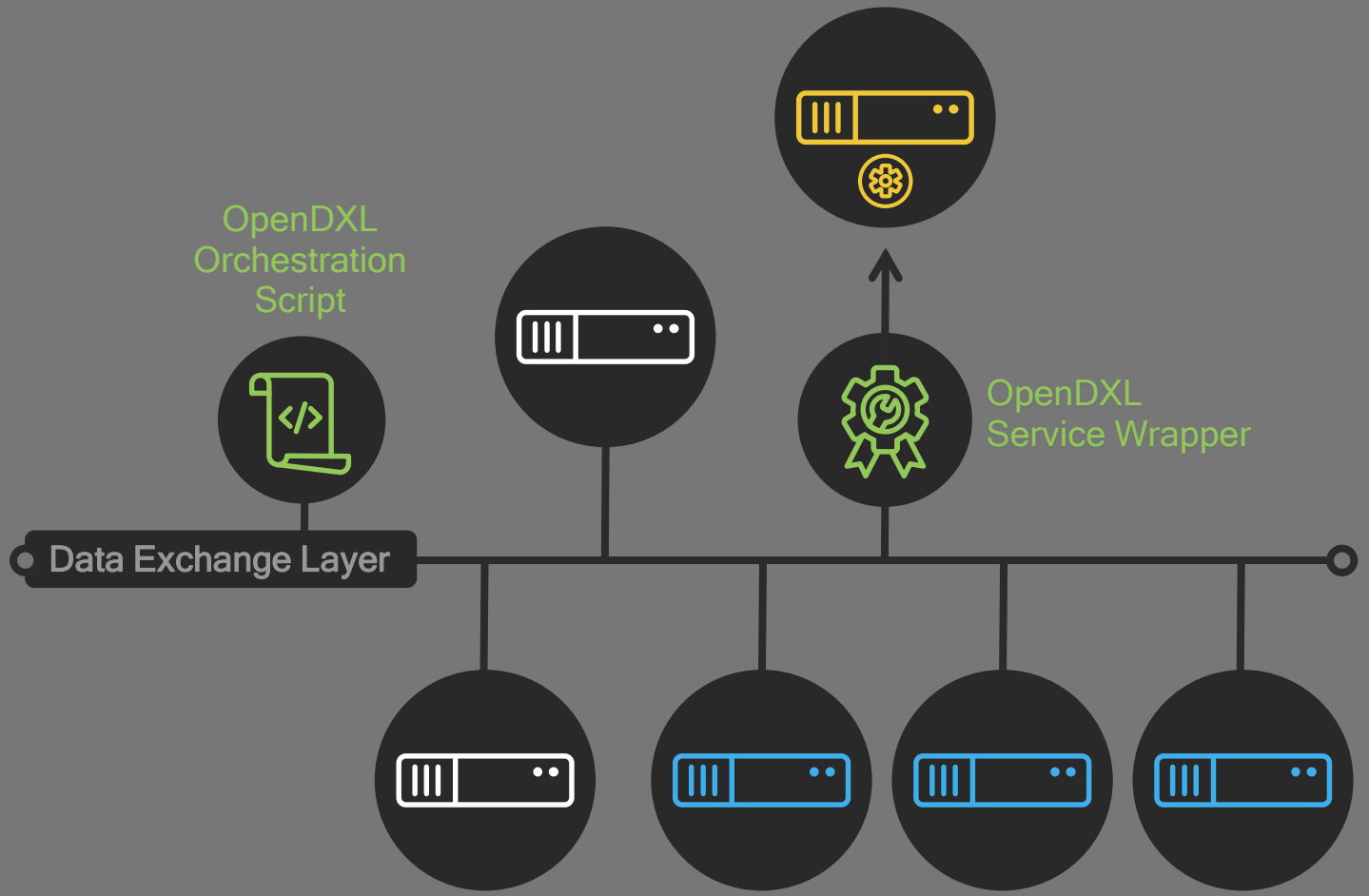
Or you can use one that's already created by another member of the DXL community.

(And if you create a Service Wrapper for a product, we hope you'd take advantage of the "open" community and share it with others.)

This ease of integration means you have the power to say "yes" to whatever products you want to integrate–without being held captive by the whims of vendors. It's a path forward where, previously, there was no path.

What previously took months, now takes hours or a few days.

And this complete integration allows you to get more value out of products you've already purchased for your environment.



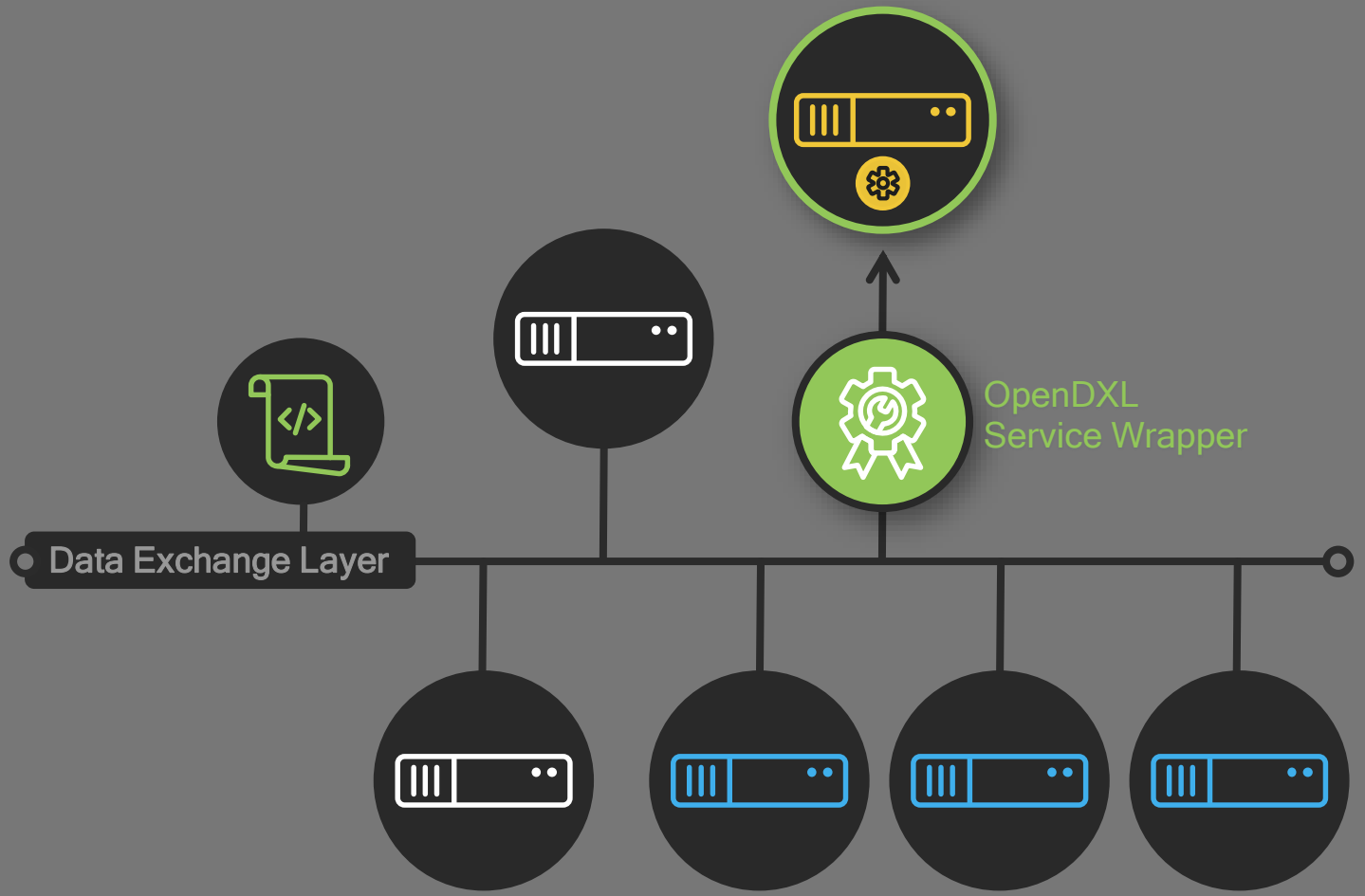
Reacting to API changes

One of the key benefits of the Service Wrapper kicks in if that third party product's API were to change.

Before, if you had a complex web for product integrations, this API change would likely shatter those integrations.

To restore integration, you'd have to fix countless points along your custom integration.

With OpenDXL, though, you need only alter the third party product's Service Wrapper to keep it connected to the fabric. It's that easy.



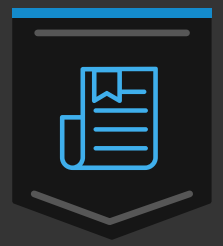
Four Key capabilities that OpenDXL allows you to do

Publish an event

Receive an event

Ask a question

Take action



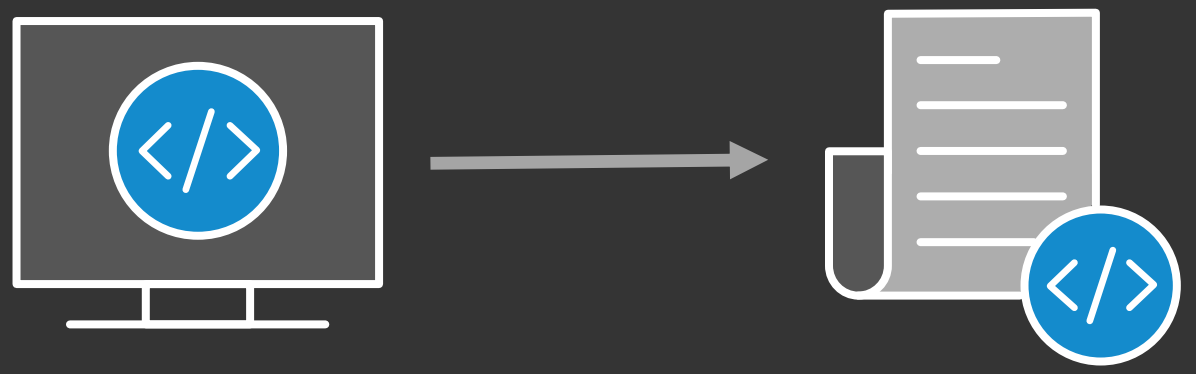
Publish an event

You can publish an event.

This means that you are allowing information to go out of the system to inform other products.

An example could be a firewall detecting a suspicious communication.

Example:



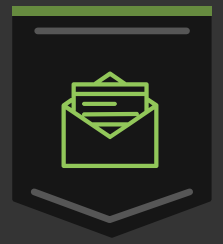
Publisher

Message

Firewall detects a suspicious outbound communication

A new file is detected

A new file is copied to a file share

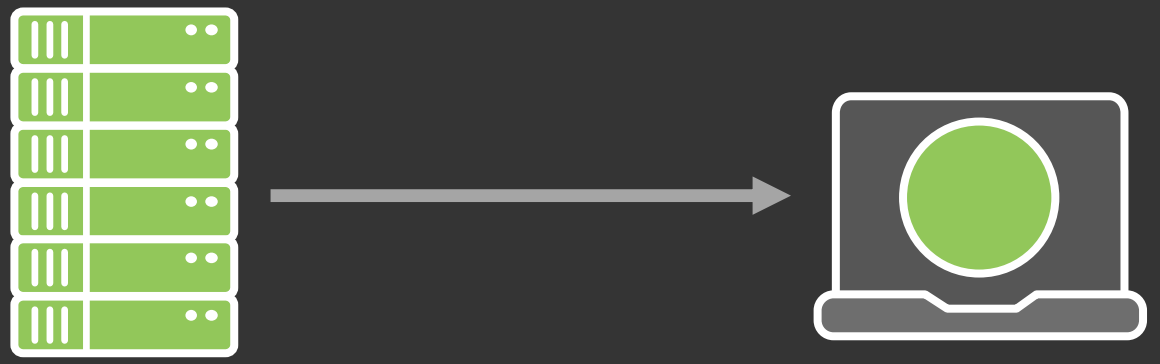


Receive an event

You can receive an event by subscribing to ”news” related to the event.

You could be alerted to a new file, or that a file was copied or shared.

Example:



Be alerted that firewall detects suspicious communication

Be alerted to a new file

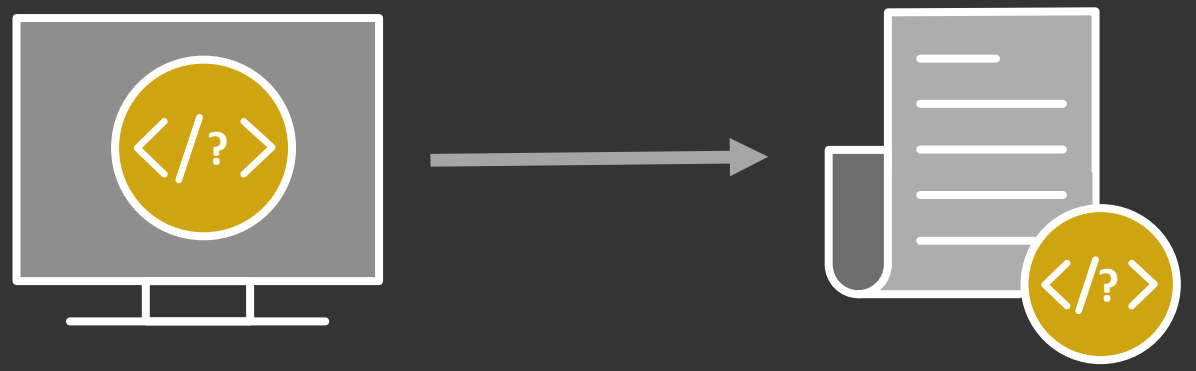
Be alerted that a new file was copied to file share

Ask a question

You can query a service.

This is a one-to-one message where your DXL routes the query and waits for a response. You can find out the reputation of a file, if security is installed on a system, or anything you or anything you need to know about.

Example:



Publisher

Message

“What is the reputation of this file?”

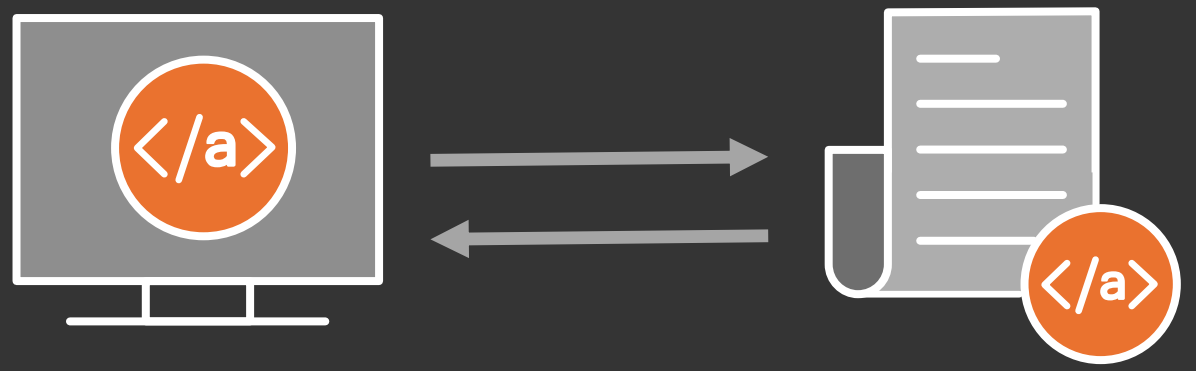
“Where has this file run in my environment before?”

“Is security installed on this system?”

Take action

DXL can take action in response to a query or a news subscription for information about an event.

Example:



Set the reputation of a file

Tag computer to begin security response to file

Begin remediation

Planning Checklist

Take a look at how these steps play out in real life when there are real security issues to solve.

The Four Steps

How will you leverage these capabilities?

Use this simple, repeatable, four-step planning checklist.

1. Identify the problem to solve
2. List the products involved
3. Simply describe what you want to happen
4. Map those actions to one of the four client capabilities

Basic example

Prevent malicious files from running in the company environment

Basic example

Prevent malicious files from running in the company environment

1 Identify the problem to solve

"I want to stop files that I know are malicious from running in my company environment."

2 List the products involved

For this basic example, the only product involved is your Threat Intelligence Exchange.

3 Simply describe what you want to happen

"When I have identified a file that I know to be bad, I want my entire environment to be told about."

4 Map those actions to one of the four client capabilities

Of the four client capabilities (publish an event, receive an event, ask a question, and take action), this one corresponds to PUBLISH AN EVENT (Threat Intelligence Exchange publishes that a file is malicious).

Moderately complex example

Manage all laptops on your network with your security management tool

Moderately complex example

Manage all laptops on your network with your security management tool

1 Identify the problem to solve

When laptops are found on my company's network that aren't managed by my security management tool, I want to make them managed by my security management tool.

2 List the products involved

There are two products involved: your System Discovery Tool and your Security Management Tool.

3 Simply describe what you want to happen

Simply put: "When my System Discovery Tool discovers a system connecting to my network, I want it to discover if the system is currently managed by my Security Management Tool and, if it's not, to tell the Security Management Tool to bring it under management."

4 Map those actions to one of the four client capabilities

This problem requires three of the client capabilities:

1. Receive an Event. You want it to pay attention to a "new system connecting to the network" event.
2. Ask a Question. You're asking: is this laptop currently managed?
3. Take action. If a laptop is not currently managed, you want to manage this system and install the required security products.

Complex example

Dealing with malicious files entering the company network via the FTP file transfer site

Complex example

Dealing with malicious files entering the company network via the FTP file transfer site

1 Identify the problem to solve

Malicious files are entering your company network via your FTP file transfer site and you want to deal with those files.

2 List the products involved

Three products: FTP File Share, Threat Intelligence Exchange, and Sandbox Scanner.

3 Simply describe what you want to happen

"When a file is copied to our FTP File Share, ask my Threat Intelligence Exchange about the file's reputation. If the file is known to be malicious, delete it. If the file has never been seen before, send it to my Sandbox Scanner."

4 Map those actions to one of the four client capabilities

The first script would play out as:

- Receive an Event. Listen for "new file copied to share" event.
- Ask a question. What is this file's reputation, Threat Intelligence Exchange?
- Act. If the file is malicious, delete it.
- Act. If the file has never been seen before, send the file to my Sandbox Scanner.
- The second script would be:
- Receive an Event. Listen for the "File Scan Results" event.
- Act. If the file scan indicates the file is malicious, delete the file via the FTP File Share.

OpenDXL

opendxl.com