The Case for Open XDR

X Means Everything

OPEN XDR SUMMIT

The current model for cybersecurity is broken. It consists of acquiring and deploying a lot of stand-alone tools, each with its own console, to analyze logs or traffic and detect anomalies that could be threats. In this model, it's up to each security analyst to communicate with other analysts to determine whether each tool's individual detection (each of which, by itself, may look benign), can correlate with other detections from other tools to reveal a complex attack.

This model forces enterprises to create complex security stacks consisting of SIEM, SOAR, EDR, NDR and more, for the purpose of instrumenting the enterprise, identifying threats, responding to threats, and managing risk. Acquiring all of these tools and managing their licenses is complex and expensive, and the manual correlation required to compare each tool's detections leaves a lot of gaps in the overall security infrastructure.

Analysts are often bombarded with false positives by these systems as well, causing "alert fatigue" and job dissatisfaction. Even enterprises that declare themselves satisfied with their existing SIEM and other tools will admit that the amount of time and energy they have poured into standing up a multi-tool security infrastructure isn't delivering the requisite results.

The Case for XDR

XDR, or eXtended Detection and Response, has become a catch-all definition for any technology performing detection and response, because in the acronym, X is really a variable. While X can represent "Endpoint+" or "Network+", that disregards the present pain of the enterprise of siloed tools, uncorrelated data, and alert fatigue. The whole goal of XDR is to address this pain, and therefore X has to mean "Everything." Everything, then, implies a platform approach to covering the entire attack surface through detection and response.

This platform approach can fix today's broken model by converting siloed tools into a unified toolset, converting uncorrelated data into a living correlated representation of the attack surface, and converting alert fatigue into peace of mind. How a technology realizes this goal is the key architectural question. There are two types of XDR today: Open and Native.

Open vs. Native XDR

- Open XDR is delivered via an open architecture capable of leveraging existing security tools' telemetry and response capabilities across the attack surface

- Native XDR is delivered from a single vendor's security tool suite that provides telemetry and response across the attack surface

Regardless of the architectural approach of an XDR platform, it must satisfy the following technical requirements in order to be considered XDR:

- **Deployability** – Cloud-native microservice architecture for scalability, availability and deployment flexibility

- **Data Fusion** – Normalized and enriched data across the entire attack surface including network, cloud, endpoints, applications and identity

- **Detection** – Real time, high-fidelity across multiple security tools

- **Correlation** – Correlated detections resulting in context-aware incidents

- **Intelligent Response** – One-click or automated response from the same platform
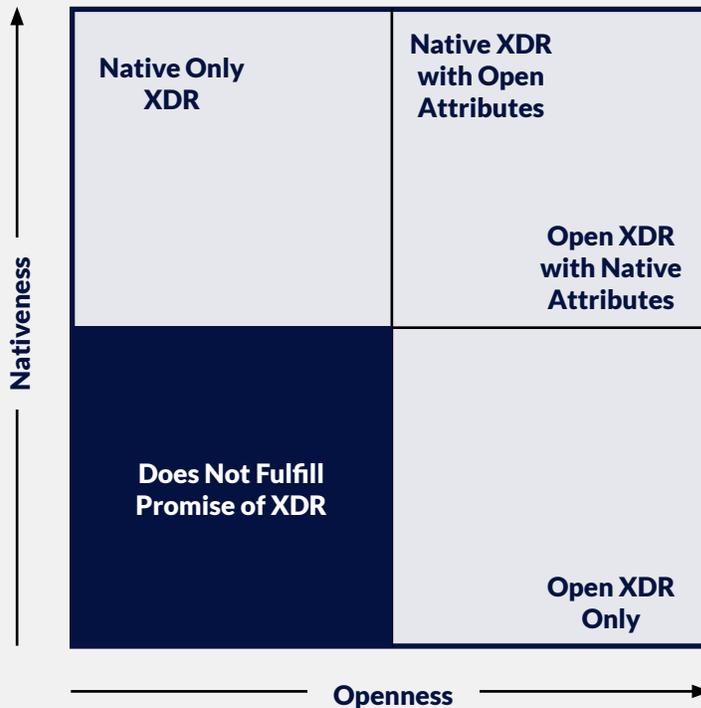
XDR Architectures Compared

	Open XDR	Native XDR
INTELLIGENT RESPONSE	**Responds to Existing Tools** — Integrates with Existing SOAR or Provides SOAR Funcionality	**Responds to Built-in Tools** — Built-in SOAR Responds to Built-in Tools
CORRELATION	**Correlates Detections** — Approach Will Vary by Vendor – ML, Rule-based, etc.	**Correlates Detections** — Approach Will Vary by Vendor – ML, Rule-based, etc.
DETECTION	**Generates Detections** — Detects on Tool Alerts and/or Raw Data via ML and/or Rules	**Generates Detections** — Detects on Tool Alerts and/or Raw Data via ML and/or Rules
DATA FUSION	**Fuses Existing Tools*** — CROWDSTRIKE, Barracuda, tenable, okta, aws	**Fuses Built-in Tools** — Native Vendor FW, Native Vendor Endpoint
DEPLOYABILITY	**Flexible Deployment** — SaaS, Private Cloud, On Prem	**Flexible Deployment** — SaaS, Private Cloud, On Prem

A common misconception about Open vs. Native XDR is that they are mutually exclusive types of XDR. They are not. An XDR platform can be fully Open, and partially Native. For example, an XDR platform can have a few built-in tools from its vendor while openly integrating with the existing tools from the other vendors. This enables a Composable Security strategy, the ability to leverage the existing tools while allowing the customer to sunset some of them when and where they see fit.

Dimensions of XDR

Native Only XDR	**Native XDR with Open Attributes**
	Open XDR with Native Attributes
Does Not Fulfill Promise of XDR	**Open XDR Only**

↑ **Nativeness**

→ **Openness**

The composition of Open vs. Native XDR that a platform takes in its approach is a means to an end: specifically, how the platform goes about performing detection and response across the entire attack surface. Buyers of XDR need to view the architectural approach as a means to an end and make the best decision for their enterprise.

The Ideal XDR is Open

There will be some enterprises that have no issue moving their entire security stack over to a single vendor, and adopting a closed, Native XDR platform. There will also be some enterprises that care less about covering the entire attack surface, and only want detection and response for their endpoints, for example. In this case they should pursue an EDR-based Native XDR platform.

However, for most enterprises, an Open XDR platform must be looked at as the top priority. Why? Because no single vendor will ever be able to create or acquire the best cloud, endpoint,

network, identity, etc. tools, so a Native-only XDR platform won't be best-of-breed. In addition, it's extremely likely that the enterprise has already invested significant capital and effort in deploying existing security tools – it won't want to abandon those investments, so a closed, Native XDR solution wouldn't interact with those tools and wouldn't capture the entire attack surface at that enterprise. If an Open XDR platform has some Native attributes to cover certain areas of the attack surface for growing enterprises, great. But it must be Open first.

In the end, if an enterprise wants to define and execute a Composable Security strategy and get all of XDR's technical requirements delivered through a platform, a fully Open XDR platform is the only realistic way to do so.