Extended Detection and Response (XDR) – A Beginner's Guide

SOPHOS
Cybersecurity evolved.

What is XDR?

Let's start by looking at the definition of XDR, as depending on who you ask the exact wording can vary.

- **Extended Detection and Response** is the most commonly used definition, being adopted by many analyst firms and cybersecurity vendors. 'Extended' refers to going beyond the endpoint and server, bringing in additional data sources such as firewall, email, cloud, mobile and others.
- **Cross-product Detection and Response** is another wording, referring to data being combined from multiple products and security layers.
- The third interpretation uses the 'X' in XDR as a mathematical variable that stands in for whichever data sources are being leveraged as part of the solution.

Whichever definition you use for XDR they all reference and make use of the same core components. The ability to access and query a range of data sources to give your organization greater visibility and context.

What does XDR do?

XDR is designed to give organizations a holistic view of their cybersecurity posture and IT environment with the ability to quickly pivot to deep investigation when further investigation is required.

Gartner states:

"The primary value propositions of an XDR product are to improve security operations productivity and enhance detection and response capabilities by including more security components into a unified whole that offers multiple streams of telemetry, presenting options for multiple forms of detection and concurrently enabling multiple methods of response."

Gartner, "Innovation Insight for Extended Detection and Response." (2020)

A commonly asked question is, "how is that different to EDR?" Indeed, XDR solutions should include the business critical question answering capabilities of EDR (Endpoint Detection and Response). That is, being able to get live data directly from an endpoint or server, as well as access to cloud data if a device is offline.

XDR builds upon that solid foundation by adding even more data and context that both increases visibility and gives the user even more insight during an investigation. This results in faster and more accurate incident detection and response. Additional data sources can include firewall, email, cloud and mobile information. For example, adding in firewall data makes it simple to correlate a malicious traffic detection by the firewall with a compromised endpoint, or to see which application is causing the office network connection to run slowly.

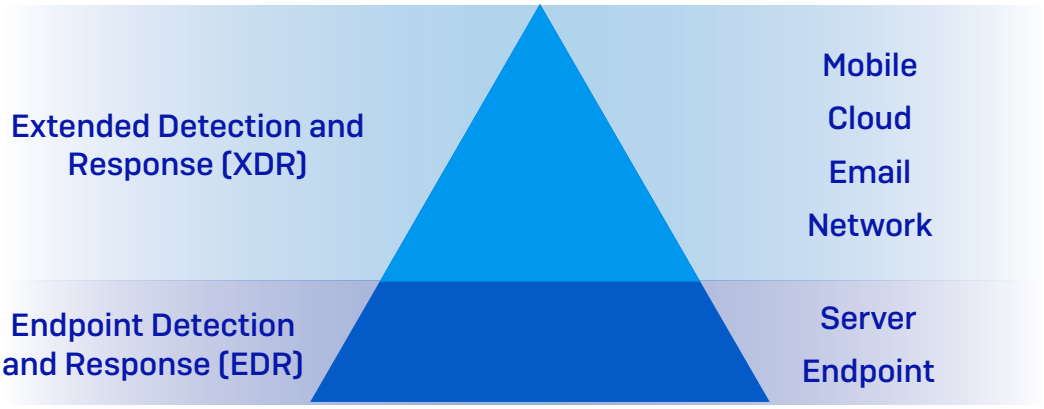
One of the most valuable ways to use XDR is to begin with the 'macro' spotlight that gives you the tools to quickly scan across your entire environment and highlight suspicious activity, anomalous behavior and other IT issues. When an issue is identified you can then hone-in on a device of interest, pulling live data or remotely accessing the device in order to dig deeper and take remedial action.

Extended Data Sources

As powerful as EDR tools are they are limited to detection and response on endpoints and servers. This isn't necessarily a bad thing. If you had to choose one place to focus your detection and response efforts your organization's endpoints and servers are a great choice.

However, there are things you can't do by working on them in isolation. After all, your IT environment is an interconnected web of networks, communication tools, mobile devices, cloud applications and more. To defend your IT infrastructure more comprehensively an integrated detection and response system is key. This is where XDR comes in.

XDR takes the idea of EDR and extends it. It goes beyond the endpoint and server, incorporating data from other security tools such as firewalls, email gateways, public cloud tools and mobile threat management solutions. XDR is an emerging technology so data sources and functionality varies between vendors, but this diagram gives a good starting point to understand what XDR adds onto EDR.



XDR use cases

The best way to explain the real world benefits of XDR is to look at how the functionality can help organizations in their day to day IT operations and threat hunting capabilities. Note that we have included EDR examples as your XDR solution should also cover those use cases.

	IT Operations	Threat hunting
EDR	• Why is a machine running slowly? • Which devices has known vulnerabilities, unknown services or unauthorized browser extensions? • Are there programs running that should be removed?	• What processes are trying to make a network connection on non-standard ports? • Show processes that have recently modified files or registry keys • List detected IoCs mapped the MITRE ATT&CK framework
XDR	• Identify unmanaged, guest and IoT devices • Why is the office network connection slow? Which application is causing it? • Look back 30 days for unusual activity on a missing or destroyed device	• Extend investigations to 30 days without bringing a device back online • Use ATP and IPS detections from the firewall to investigate suspect hosts • Compare email header information, SHAs and other IoCs to identify traffic to a malicious domain

How Sophos can help

Sophos XDR gives organizations a broad, holistic view of their entire cybersecurity environment with the ability to deep dive when required. In other words you get both the 10,000 feet, high level view and the granular detail as you need them.

XDR enabled solutions send endpoint, server, firewall, email and other data sources* to the Sophos Data Lake, a cloud repository for critical XDR and offline device data. It's a centralized location for all the data so you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.

Getting started is easy, with a library of pre-written, fully customizable queries so you can choose a category, add devices and start answering IT operations and threat hunting questions.

Gartner Innovation Insight for Extended Detection and Response, Peter Firstbrook, Craig Lawson,19th March 2020.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

*Cloud Optix and Sophos Mobile coming soon

Learn more at
Sophos.com/xdr

SOPHOS

21-04-06 WP (NP)