

What is Extended Detection and Response (XDR)?

Extended Detection and Response (XDR) combines threat intelligence with the cybersecurity engine for best results. But how exactly does it benefit you?

Information gathering is the foundation of most successful cyberattacks. Threat actors spend time and resources learning about the target system and then exploiting its weakest points. To combat these malicious actors, you must spend a lot of energy observing and examining cyber threats to strengthen your defenses.

Extended Detection and Response (XDR) combines threat intelligence with the cybersecurity engine for best results. But how exactly does it benefit you?

What is Extended Detection and Response?

Extended Detection and Response (XDR) is a comprehensive and simple framework for managing network threats without spending too much. It provides various security tools in one package, allowing you to deploy the most suitable technique to tackle different types of threats.

Your network is under great threat amid the multitude of threats that cybercriminals are attacking from all angles. If you're not paying attention, you can spend all of your time and resources responding to threats and still not make significant progress. This can happen, especially as threat actors raise their attack standards, deploying advanced techniques every day.

XDR enhances threat management, from basic detection and prevention to deploying advanced tools to observe, troubleshoot, identify and extensively test threat actors to long-term and sustainable solutions.

How does Extended Detection and Response work?



Implementing security measures to protect your network against vulnerabilities is a fundamental requirement. You should manage your resources carefully, otherwise you may end up spending a lot of money without getting significant results. XDR guides you to increase security by combining strategies, tools, and resources to deliver favorable results every time.

There are 3 steps to apply XDR.

1. Aggregate data from multiple sources

Establishing strong network security starts with collecting relevant and complete data about your network. Even if you put in place provisions for collecting this data, organizing and analyzing it can be a daunting task.

XDR collects and analyzes data from multiple areas of your network including endpoints, traffic, clouds, etc. This data collation gives you background information about the actors. Instead of addressing the flaws on the surface, you can examine them more closely to understand how they happened and where they came from. You can integrate your system with an internal or external threat intelligence platform to receive confidential information about your activities.

External threats enter the system through endpoints. If you get hacked, it means your endpoint security is weak. XDR provides information that you can use to identify weak links, so you can strengthen them and prevent further attacks.

2. Detect unusual behavior

Cyber threats do not arise on their own; they are products or activities of cybercriminals. These people know the best ways to launch specific attacks, and because their methods work, they replicate them using similar methods.

Extended Detection and Response uses Machine Learning technology to detect threats by understanding and analyzing anomalous periodic behavior of threat actors. When such behaviors are constant over time, XDR's artificial intelligence (AI) engines pick them up and record them as samples. After establishing threat metrics, it can recognize those activities remotely.

3. Incident response

XDR is more than just a threat intelligence collection system. When it detects an intrusion, it disables it. If the threat has already affected your system, it will try to remedy the situation by preventing further damage.

The XDR system uses automation to act on predefined triggers. When there is a threat alert, its first task is to secure the endpoints as they are attack vectors used to enter and exit the system. In addition, XDR protects other security points that could be tools for an attack. This comprehensive security framework is a key factor that distinguishes XDR from similar Endpoint Detection and Response (EDR) functionality.

What are the benefits of Extended Detection and Response?



Cyberattacks may seem sudden, but in most cases, they don't happen by accident. Attackers build momentum by taking small steps to gather information and establish their presence before attacking. XDR allows you to detect those small steps before they develop into major attacks. Its benefits include the following.

Get extended visibility

Cyber threats and vulnerabilities thrive in blind spots. If they're out of your sight, chances are they're also out of your reach and are manifesting without your knowledge. This lack of visibility can lead to misdiagnosis, wrong implementation, and misuse of resources.

XDR provides complete network visibility, notifying you of all activity in the network. You know exactly how many devices and connections are accessing your system. From your profile, you can determine when strange elements appear on your digital base. Such a high level of awareness helps combat emerging vulnerabilities before they spread and escalate.

XDR visibility is the result of advanced monitoring tools it uses to monitor network traffic and other interactions around the clock. These automated systems use sensors to detect even the slightest odd activity.

Prioritize threat alerts

Incident response fatigue is a real problem, especially when you have a large network that regularly receives threats. Investigating every message you receive is one of those incident planning mistakes that you need to avoid. You'll barely have time to focus on other important aspects of your work, not to mention the resources you'll waste in the process.

While all threats are important, some are more serious than others, especially when they involve your most important data. XDR allows you to review threat alerts before acting by prioritizing sensitive data. There are low-, medium-, and high-level threats. Low-level threats don't have a significant impact on your network and can therefore be left for later, especially when you have to deal with medium and high-level threats.

Make data-driven decisions

Collecting and analyzing data gives you insights into the nature of cyber threats. Instead of making assumptions and going in the wrong direction, you are guided to take meaningful actions.

Efficient use of resources is as key in cybersecurity as it is in any other field. XDR plays an essential role in the classification of cyberspace, a process that manages your resources to address the most critical security issues that need immediate attention. It generates real-time data about network activities that you can analyze to identify areas that need your urgent attention.

You finished reading the article "**What is Extended Detection and Response (XDR)?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.