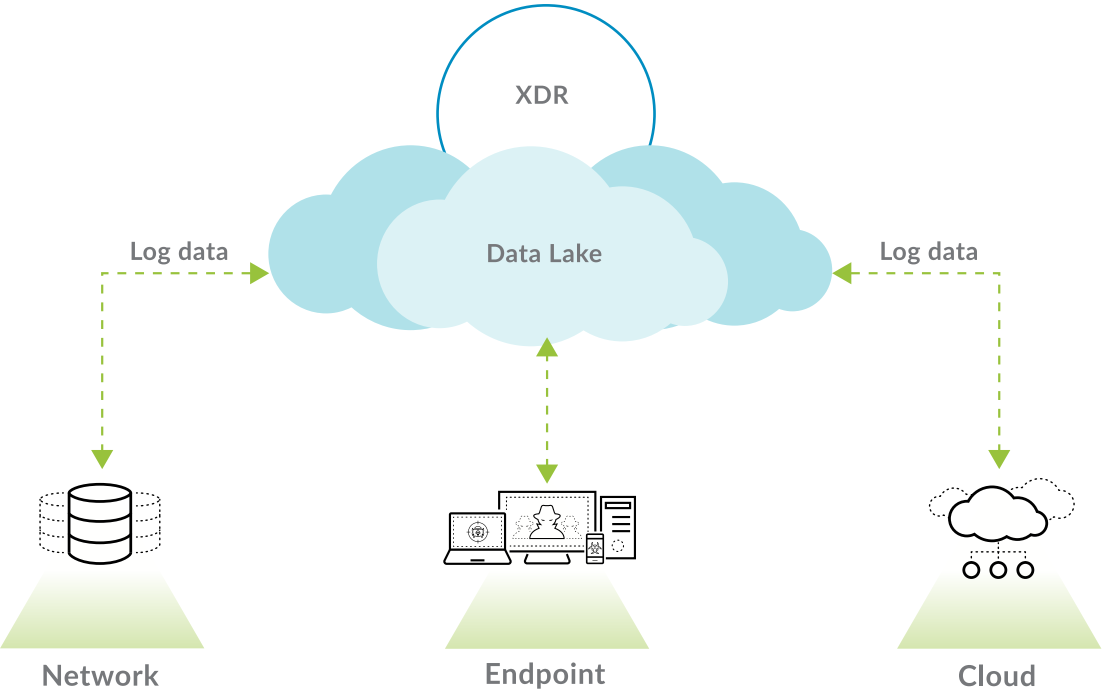
CORTEX XDR™

BY PALO ALTO NETWORKS

What Is XDR?



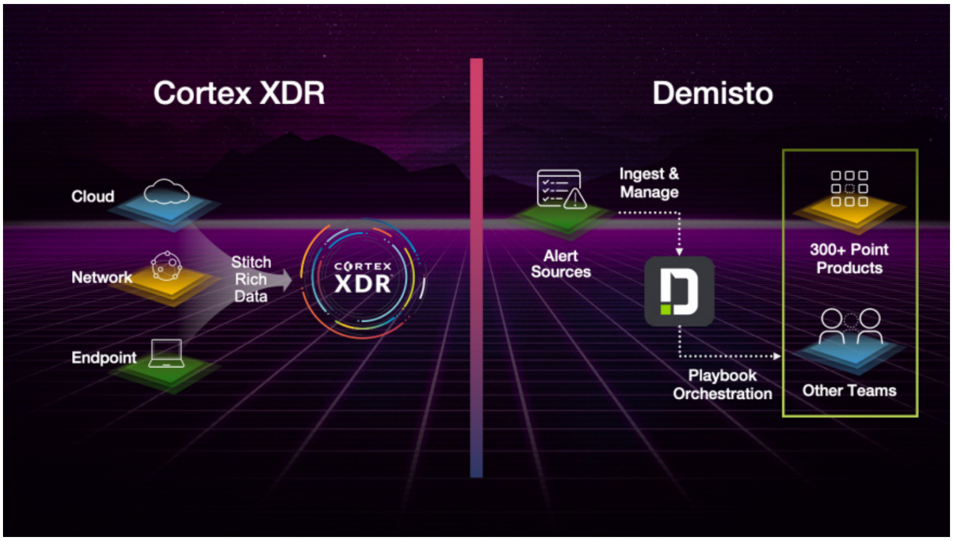
There's been a lot of buzz about XDR as of late – and not just from us. Analysts, competitors, seemingly everyone is talking about XDR these days. However, in the classic security industry problem of every product sounding basically the same, we are often asked to clarify.

What is XDR? How does it differ from, complement and/or integrate with endpoint detection and response (EDR), endpoint protection platforms (EPP), network traffic analysis (NTA) or name-your-other-security-tool? What are the key criteria to look for when evaluating an XDR product?

The short answer is that the “X” in XDR is a variable that stands for “anything,” meaning XDR solutions, at their core, are detection and response platforms that can take good data from network sensors, endpoint sensors and cloud sensors, and perform analysis on that data in a central location. Our visionary CTO and co-founder Nir Zuk coined this category in 2018, recognizing that the existing detection and response tools on the market were too narrowly focused to serve security teams' evolving needs. XDR products are designed to detect and stitch together all the available information on any threats that have evaded prevention to provide security analysts with detailed analysis of any attack that is underway. This information allows a security team to react to and resolve incidents quicker, and also allows the team to be more proactive with threat hunting.

For the long answer, read the e-book *XDR: Enterprise-Scale Detection and Response,* which you can download for free. This goes into everything you need to know about what an XDR solution is and how to evaluate it for inclusion in your security toolkit, including:

- Shortcomings of legacy detection and response products, and how XDR addresses them.
- Required capabilities of XDR to protect against attackers who have used cloud and automation to become more powerful and sophisticated.
- The definition and defining characteristics of XDR solutions.
- Key use cases for XDR and how to use it to refine your overall security operations.
- A detailed RFP checklist for evaluating XDR tools.



We truly embrace the principles outlined in this e-book as we continue to improve upon our own industry-leading XDR product, Cortex XDR. With Cortex XDR, we are able to automate huge chunks of triage, investigation and response processes, and give analysts all the information that they need to make informed decisions on the stuff that can't be automated. We've been able to group disparate alerts into "incidents" to reduce the alert load by 50x, and we, on average, speed up the investigation process by 8x. Compared to the old incident response process, which centered around a log collector and a pile of siloed analysis tools, we've seen that XDR is dramatically more efficient, effective and scalable.

That's just the start.

We recently released Cortex XDR 2.0, which has taken several additional powerful steps toward eliminating blindspots, reducing alert fatigue and simplifying management. Our executives Nir Zuk, chief technology officer, and Lee Klarich, chief product officer, were featured on a fast-action launch streamcast on Dec. 10, going into much more detail about what's included in Cortex 2.0 and what it means for you. Watch "The Future of Endpoint Security Starts Here" and learn more about how we're leading the way to better security operations.

To view this content online, visit blog.paloaltonetworks.com/2019/12/cortex-what-is-xdr.

CORTEX XDR™
BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com