Client Question Video: What Is Extended Detection and Response, and Why Should I Care?

Published 28 October 2021 - ID G00739343 - 2 min read

By Analyst(s): Peter Firstbrook

Initiatives: Infrastructure Security

Extended detection and response, or XDR, is on every security vendor’s marketing these days. But what is XDR and why do you need it? Is it an architecture or a product, and will it replace stuff you already have? This video explains what you need to know about XDR and what you should do about it.

Overview

XDRs can be defined as a tool to provide a common detection, alert management and incident response capability across multiple security products. The goal of XDRs is to enable better visibility across multiple security tools and faster, more accurate incident response, because these tools share data and are integrated with APIs to provide for semiautomated response capability across multiple tools. This short video will explain the basics of XDR and what you should do about it.

Recommended by the Authors

Innovation Insight for Extended Detection and Response

Magic Quadrant for Endpoint Protection Platforms

Hype Cycle for Endpoint Security, 2021

Emerging Technologies: Critical Insights for Endpoint Detection and Response

Magic Quadrant for Security Information and Event Management