FORTINET

POINT OF VIEW

Consolidate Cybersecurity Vendors to Accelerate Detection and Response

Use Extended Detection and Response (XDR) as a Unifying Architecture

More Vendors Means More Complexity

Organizations of all shapes and sizes are increasingly embracing digital transformation, cloud-delivered applications, remote work, and more. While this adoption of new technologies offers many benefits to enterprises—and has arguably been essential over the past few years—the inevitable downside is the expansion of the organization's attack surfaces. As a result, many organizations are seeing their security operations grow in complexity, which puts a strain on even the most capable and well-staffed security and IT teams.

However, consolidation doesn't just mean purchasing multiple individual security products from a single vendor. Instead, organizations should look for products sourced from the same vendor that actually work together a part of a converged solution, like XDR.

75% of organizations are pursuing cybersecurity vendor consolidation today.[1]

By 2023, more than 80% of organizations plan to have XDR.[2]

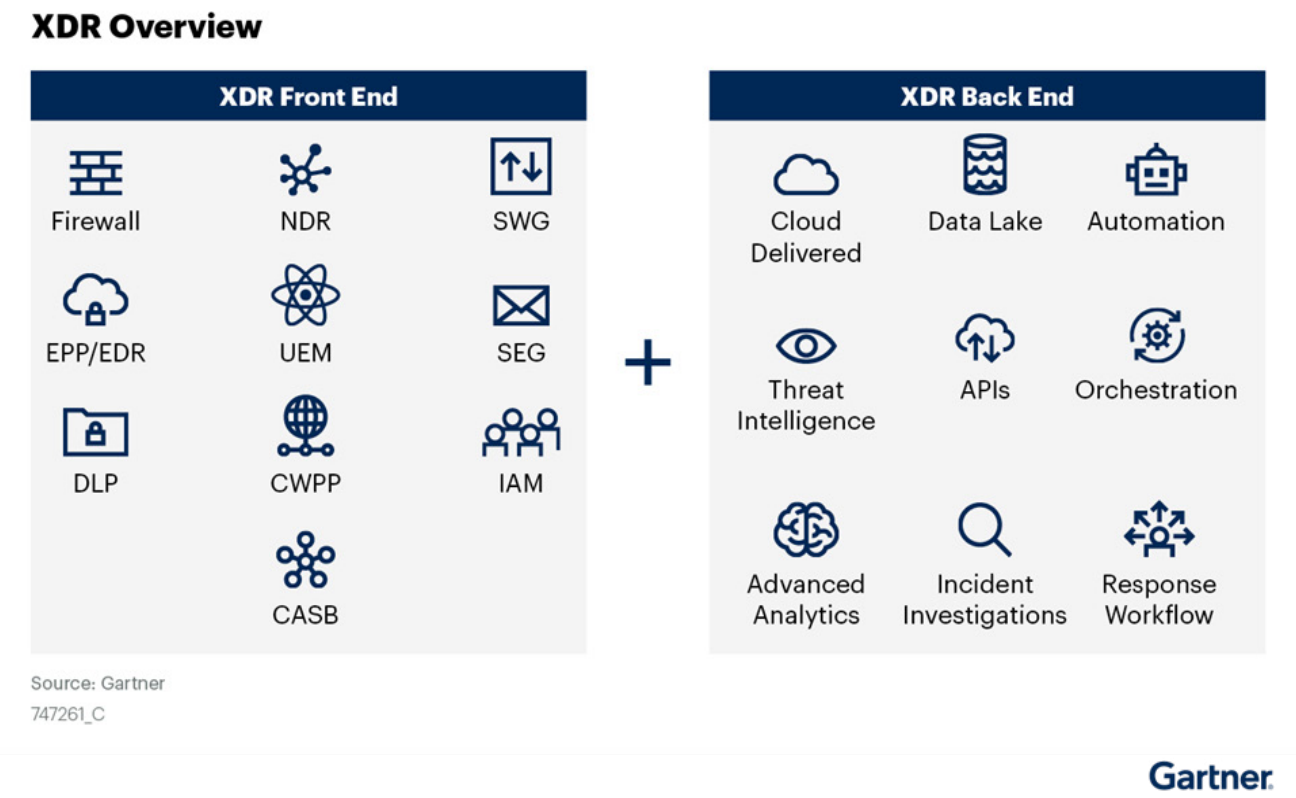
What Is XDR?

XDR is a natural extension of the endpoint detection and response (EDR) concept, in which behaviors that occur after threat prevention are further inspected for potentially malicious, suspicious, or risky activity that warrant mitigation. The difference is simply the location (endpoint or beyond) where the behaviors occur. Specifically, XDR requires:

- Multiple security controls that feed telemetry about digital activity for correlation and analysis
- Analytics to correlate, enrich, and assess the bigger picture provided by the multi-product telemetry to detect potential cybersecurity incidents
- Artificial intelligence (AI) to speed investigation to confirm and classify actual incidents
- Orchestration and automation to coordinate response actions across (and beyond) the aforementioned security controls
- Native integration, curated analytics, and pre-defined automation that enable the system to work largely on its own

It's arguably the last aspect that differentiates XDR from existing security monitoring products, most of which have the potential to be powerful but are often too resource intensive for most organizations.

Gartner® visualizes XDR requirements in its Market Guide for Extended Detection and Response[3] within two categories: front-end and back-end components.[4]



Source: Gartner
747261_C

XDR solutions are increasingly popular as organizations recognize the inefficiencies, and in many cases ineffectiveness, of security infrastructures that are composed of many individual "best-of-breed" security products deployed from different vendors over time. Common challenges arising from this point-product approach include:

- **Gaps in security:** With each product operating in its own silo, opportunities often arise for cyberattacks to enter in between.
- **Too much security information:** With each product generating individual alerts and other information, security teams can easily miss indicators of cyberattacks.
- **Uncoordinated response:** With each product operating independently, it falls on the human operator to share information and coordinate response actions manually.

Based on these experiences, many organizations are looking to consolidate security vendors and products in favor of integrated solution sets.

How XDR Can Benefit Your Organization

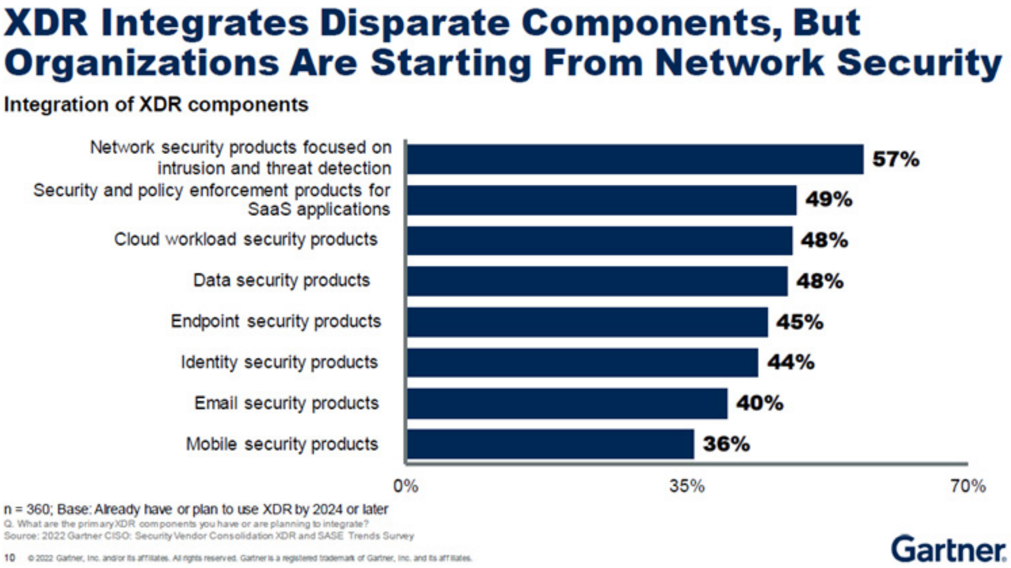
Adopting an XDR approach to security offers many benefits to organizations of all sizes and across all industries.

According to a Gartner survey 59% of the respondents claimed that XDR can improve the organization's security capabilities related to prevention, detection, or response maturity.[5] Specifically, XDR enables different security solutions to see, share, and analyze data so they can more effectively detect threats and deliver a coordinated response that covers the entire attack surface.

As a result, already overburdened security teams can reduce the complexity of operations while simultaneously enhancing their detection and response capabilities, ultimately better protecting their organization's networks and assets.

XDR: Where to Start

Interested in adopting XDR technology, but not sure where to start? There are many components to XDR. A recent Gartner study found that most organizations begin by integrating XDR components into their network security technology stack.[6]



XDR Integrates Disparate Components, But Organizations Are Starting From Network Security

Integration of XDR components

n = 360; Base: Already have or plan to use XDR by 2024 or later

Q. What are the primary XDR components you have or are planning to integrate?

Source: 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey

10 © 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

This is typically followed by endpoint security as a great tool to validate what the network (or cloud or email) security product may see.

Conclusion

Digital innovation has transformed businesses and the networks they use to run critical applications, perform online transactions, connect remote workers, and collect and process critical data. As a result, now more than ever, today's security teams are left trying to manage a vast collection of security tools from a variety of vendors and establish some sort of visibility and consistent policy orchestration and enforcement across their organization.

Network security is the most common component (57%) organizations are planning to integrate with for XDR.[7]

A new approach to security is essential, and XDR offers enterprises the benefits needed to operate successfully in this new era. The most common anchor component of XDR is network security, with the inclusion of cloud, endpoint, email, and identity security commonly rounding out the initial solution set.

[1] "Gartner Survey Shows 75% of Organizations are Pursuing Security Vendor Consolidation in 2022," Gartner, September 13, 2022.

[2] Ibid.

[3] Ibid.

[4] Craig Lawson, et al., "Market Guide for Extended Detection and Response," Gartner, November 8, 2021.

[5] "Gartner Survey Shows 75% of Organizations are Pursuing Security Vendor Consolidation in 2022," Gartner, September 13, 2022.

[6] Ibid.

[7] Ibid.

December 7, 2022 1:12 AM
1869551-0-0-EN