

January 2023

XDR REPORT

To Achieve the Promise of XDR,
Look Beyond the Endpoint

Executive Summary	3
Key Findings	4
High-Level Themes	4
Introduction	5
The Benefits	6
The Strategy	7
Overcoming the Barriers	8
Conclusion	9
Methodology	9

Executive Summary

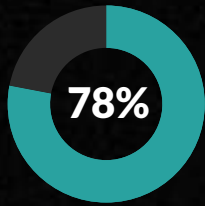
Most IT leaders (78%) agree that wider adoption of extended detection and response (XDR) strategies and solutions is a necessity in 2023. However, a deeper dive into their perspectives on XDR reveals knowledge gaps that may be keeping their organizations from reaping the full benefits of this strategy. In our survey of 950 IT decision makers across seven global markets, undertaken in partnership with Wakefield Research, less than half (47%) accurately acknowledged increased network visibility through higher-fidelity network telemetry as a foundation for XDR. Instead, many view XDR's distinction as providing consolidated solutions under a single vendor. Others view it as simply an extension of network detection and response (NDR) or a new buzzword being used to describe security information and event management (SIEM).

While nearly three-quarters of IT decision makers (72%) use an XDR strategy at their organization, our data shows that despite their direct experience with XDR, they generally lack an understanding of the value it brings to their businesses at large. Most IT decision makers (78%) recognize the value of XDR for cybersecurity practitioners, yet nearly half (46%) see the benefits as extending to few outside their department. This limited recognition of the business value of XDR in mitigating cyber risk and improving resiliency — particularly in today's expanded cloud and remote work environments could impede companies' ability to reap the full benefits of an XDR strategy and make it harder for CISOs to obtain funding to implement them. Given the business disruption cyberattacks cause and the direct financial impact, it's all the more important for organizations to ensure their XDR strategies focus on deepening network visibility and enhancing response capabilities.

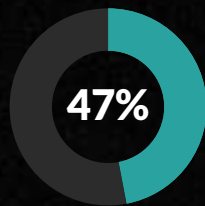
XDR Defined

XDR is a strategy for deepening threat visibility and accelerating threat detection and response by correlating endpoint data with higher-fidelity network telemetry and other data sources.

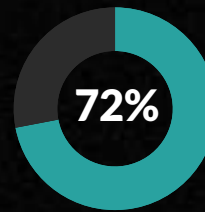
Key Findings



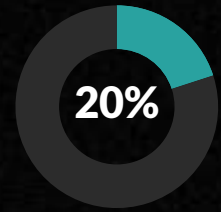
78% say wider adoption of XDR is a necessity in 2023



47% identified the accurate definition of XDR



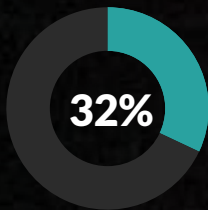
72% using an XDR strategy



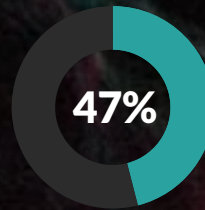
20% planning to use XDR in the next 12 months

Prevalence of XDR

XDR is...

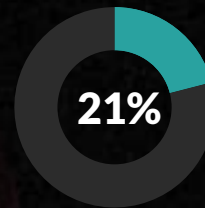


32% ...a game-changer for my organization

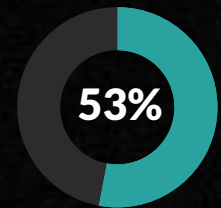


47% ...a cutting-edge strategy, but few benefit outside of IT

At companies without XDR...



21% say their board is pushing for XDR



53% say their board is curious about XDR

High-Level Themes

— Organizations have adopted XDR at a rapid pace, viewing it as a necessity. Most boards at companies without XDR are also interested.

— Vendors have been successful in shaping buyers' perceptions of the benefits of XDR, but sometimes they've shaped those perceptions too narrowly.

— The value of XDR goes beyond the benefits most commonly cited by vendors in their product messaging, as recognized by those with an XDR strategy in place.

— Despite recognizing the importance of implementing an XDR strategy, many struggle to articulate the business value of XDR, even among those at organizations where XDR is being used.

— To derive full value from an XDR strategy, organizations need to understand the wide variety of benefits it can provide and the range of technology components and data sources needed to implement it.

Introduction

Facing the escalating threat of cyberattacks and their increased level of sophistication, IT professionals are determined to find solutions to protect and secure sensitive data and critical infrastructure. One approach that has captured the attention of many IT leaders is XDR. Since its emergence in 2018, XDR has become a fixture in the cybersecurity industry. More than 3 in 4 IT decision makers (77%) describe themselves as very or extremely familiar with it, and 72% say their company is using an XDR strategy.

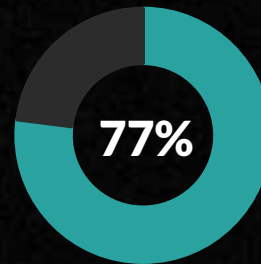
The majority of IT decision makers view XDR as a disruptive technological force and the next logical step in the future of cybersecurity. XDR incorporates network and other telemetry to build on endpoint detection and response (EDR) solutions, and ultimately, to shift detections from the endpoint to earlier in the attack cycle. More than three-quarters (78%) describe XDR as a game changer or cutting-edge security strategy.

However, it seems many IT decision makers may be having difficulty understanding the company-wide value of its implementation. While 32% describe XDR as a “game changer” for their organization, nearly half (46%) view it instead as a cutting-edge strategy that benefits few outside of their department.



Nearly half view XDR as a cutting-edge security strategy that benefits few outside their department

The breadth of this viewpoint is concerning since the purpose of XDR is to reduce organizations’ cyber risk exposure by improving visibility and detecting threats before they lead to a negative business impact.



77% of IT decision makers describe themselves as very or extremely familiar with XDR

What’s more, those IT decision makers who say XDR has limited value may have trouble making a case for an XDR strategy that resonates with critical business stakeholders to get their buy-in. This will be particularly important for the 20% of IT decision makers planning to implement an XDR strategy in the next 12 months.

First-hand experience with XDR appears to have helped some—but not all respondents—recognize its business benefits. Among those who are currently using XDR, 36% describe it as a company-wide game changer, compared to just 22% of IT decision makers without XDR. Even so, 43% of IT decision makers with XDR see it as a tool that benefits few outside of their department, in line with the 53% of IT leaders without XDR who hold this view.

The Benefits

The majority of IT decision makers at companies without an XDR strategy (58%) say they are very or extremely familiar with XDR, yet their understanding of XDR and its benefits appears to be guided primarily by vendor messaging. In contrast, those at organizations with an XDR strategy in place demonstrate a deeper understanding of its advantages. When asked to rank the top three benefits of XDR, IT decision makers at companies without an XDR strategy most commonly cited faster threat response (60%), increased detection coverage (50%), reduced time to identify threats (48%), and extended coverage of the attack surface (47%).

The list of top three benefits selected by IT decision makers with XDR was more varied and far less dominated by the benefits commonly touted in vendor messaging, having seen the benefits their organization experiences from XDR first-hand. For instance, while 42% of IT decision makers with XDR included faster response to threats among the top three benefits they cited, this is a much smaller percentage than the 60% of IT decision makers without XDR who included faster response in the top three. These IT leaders' lists included extended coverage of the attack surface (45%), improved alert prioritization (45%), reduced time to identify threats (43%), and increased detection coverage (43%).

Their rankings also commonly included tool replacement or consolidation (42%), which was cited by less than a third of IT leaders without XDR (32%). Similarly, while reduction in the number of

false positive alerts was least commonly ranked as a top three benefit by both groups, it was included by 39% of IT decision makers with XDR, compared to just over a quarter of IT decision makers without XDR (26%).

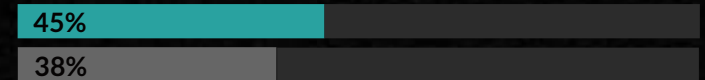
Benefits of XDR

■ IT decision makers with XDR ■ IT decision makers without XDR

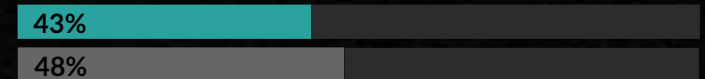
Extended coverage of the attack surface



Improved alert prioritization



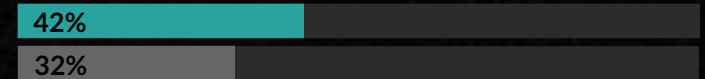
Reduced time to identify threats



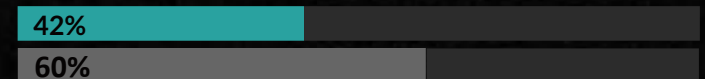
Increased detection coverage



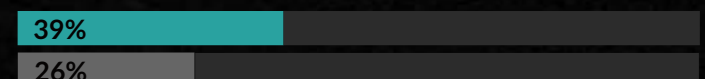
Tool replacement or consolidation



Faster response to threats



Reduced false positives



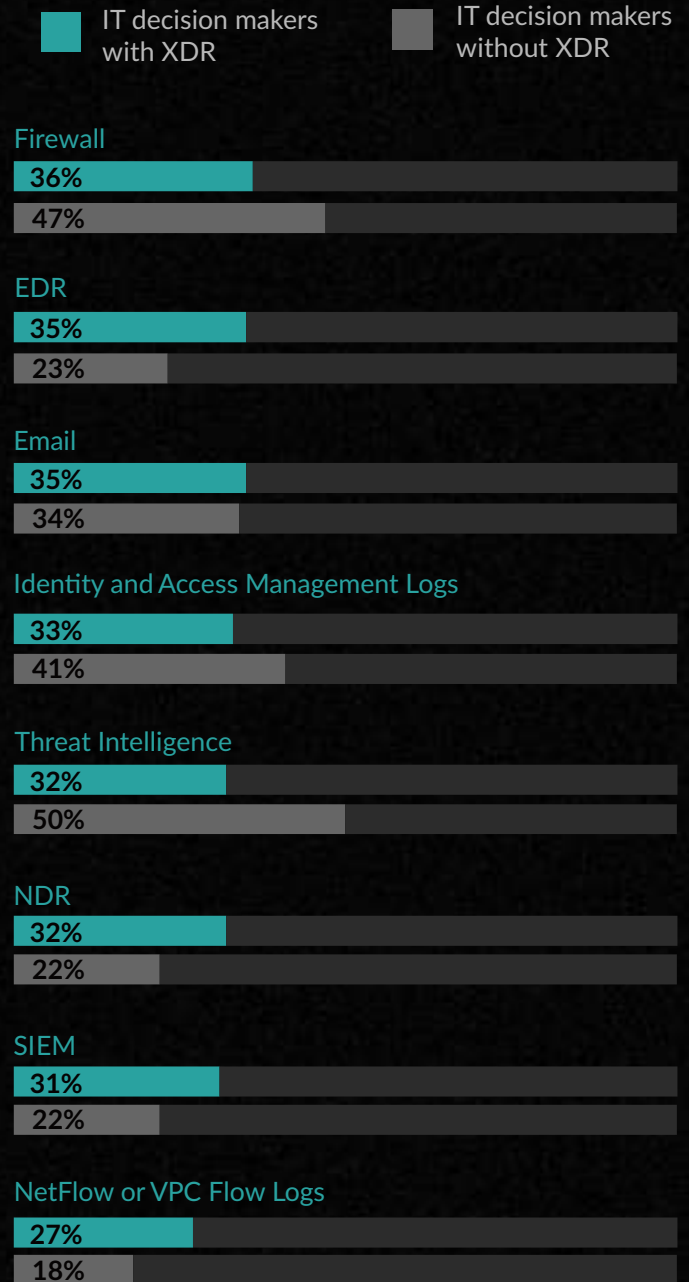
The Strategy

XDR combines the capabilities of several cybersecurity tools to provide a more comprehensive and proactive approach to detecting and responding to threats. While IT decision makers at companies using an XDR strategy recognize a broad range of components and data sources as critical to a successful XDR implementation, those without XDR demonstrate a narrower understanding. IT leaders without XDR showed a strongly defined list of top three components in an XDR strategy—threat intelligence (50%), firewall (47%), and identity and access management logs (41%).

In contrast, IT leaders at companies using XDR demonstrate a broader understanding of the necessary components, with no single one rising to the top. Firewall (36%) was the most commonly included among IT decision makers with XDR, followed by EDR (35%) and email (35%). Yet less than a quarter of IT decision makers without an XDR strategy (23%) included EDR as a top three component.

XDR strategies incorporate several kinds of detection and response tools, including NDR and SIEM. While both NDR and SIEM were among the components least commonly viewed as critical across those with and without XDR, they were included even less frequently by IT decision makers without XDR. Nearly a third of IT decision makers with XDR included NDR (32%) and SIEM (31%) as top three components, compared to less than a quarter of IT decision makers without XDR who view NDR (22%) and SIEM (22%) as critical.

Most Important Components in XDR Strategy



The overall low proportion of respondents who view NDR as a key component suggests a gap in their understanding of the importance of this critical element. NDR is essential to XDR because, among other things, it provides organizations with visibility into threats hiding in encrypted network traffic and into cloud workloads and unmanaged devices that EDR solutions aren't designed to provide.

It also provides SOC analysts with telemetry that's absolutely critical to incident response. The lack of awareness around NDR likely stems from the fact that XDR vendors' backgrounds are in EDR, so they don't typically have a strong network security focus.

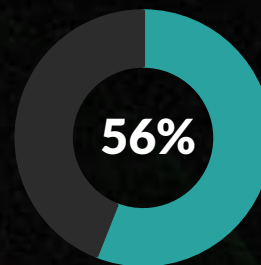
Overcoming the Barriers

At organizations that don't currently have an XDR strategy, an overwhelming 90% of IT decision makers report barriers in their way. Yet many of these obstacles may be easier to overcome than anticipated, especially when armed with an accurate understanding of XDR. Nearly a quarter of IT decision makers not using XDR (23%) say they simply don't know enough about it.

A second hurdle to implementing XDR is the perception, cited by 24% of respondents, that it would require an organization to overhaul or replace components of its current network security strategy and solutions. In fact, however,

industry-leading XDR solutions are built with native integrations so that organizations don't have to switch their network security tooling, an approach favored by 41% of IT leaders.

A third hurdle, cited by 22% of respondents, is that their leadership doesn't see the value in it. Yet a majority of IT decision makers without XDR (53%) say their boards are curious about XDR and 21% say their boards are not only interested in XDR but pushing for it.



of IT decision makers without XDR cite not having enough staff to oversee implementation or a lack of in-house expertise as roadblocks

In this challenging business environment, many IT decision makers are also concerned about potential staffing-related requirements for implementing XDR. More than half of IT decision makers without XDR (56%) cite not having enough staff to oversee implementation or a lack of in-house expertise as roadblocks. In these instances, having an external partner may be invaluable to support the implementation.

Conclusion

XDR isn't a new strategy in the cybersecurity world, but it may be that many are just beginning to understand its true capabilities and value. Confusion about XDR and how best to implement it persists, even as companies recognize the critical need for this advanced solution to help them stay ahead of cyber threats and safeguard their businesses. Momentum to implement XDR strategies is growing as companies' attack surfaces expand, yet it is crucial that IT leaders fully understand what components make the biggest difference in an XDR strategy and how a strong XDR strategy can benefit their organization's broader risk management and business resiliency strategies. In particular, many IT decision makers overlook the importance of NDR in the design of an effective XDR strategy. If they don't account for NDR as part of their XDR strategy, they risk missing out on an essential source of visibility and telemetry required to detect, respond and contain threats faster, in the earliest and least harmful stages.

While experience with XDR provides a greater understanding of its benefits, its successful implementation is being impeded by buyer perceptions that have been shaped by narrowly focused vendor messaging. Organizations looking to fully secure their environments should ensure their XDR strategy includes the necessary components to provide the greatest level of network visibility and protection.

To realize the game-changing benefits and value of XDR for their businesses, IT decision makers may be best served by keeping an open mind and considering not just the impact on their immediate security teams but on their enterprise's broader business resiliency and cyber risk mitigation goals.

Methodology

The ExtraHop XDR Survey was conducted by Wakefield Research among 950 IT decision makers with a minimum seniority of director in the following markets: US, UK, France, Germany, Australia/New Zealand, Japan, ASEAN (Singapore, Malaysia, Indonesia) between November 29th and December 4th 2022, using an email invitation and an online survey. Quotas were set for 200 respondents in the US, 50 respondents in Malaysia, and 100 respondents in each of the remaining markets.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 3.2 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

HOW XDR GETS REAL

Stop Advanced Threats with
CrowdStrike & ExtraHop

ON-DEMAND WEBINAR

CROWDSTRIKE


ExtraHop

See how CrowdStrike and
ExtraHop are powering true
XDR for their customers:
Watch our on-demand webinar

WATCH NOW

ABOUT EXTRAHOP

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

 ExtraHop

info@extrahop.com

www.extrahop.com