CRA | Business Intelligence

XDR Poised to Become a Force Multiplier for Threat Detection

APRIL 2022

Sponsored by

eSENTIRE exterro

XDR Poised to Become a Force Multiplier for Threat Detection

FINDINGS FROM A MARCH 2022 CYBERRISK ALLIANCE RESEARCH STUDY

BACKGROUND

Security teams are increasingly underserved by the collection of detection and response tools they've collected and patched together over time.

These siloed security solutions once served their purpose. But as attacks grow in frequency and boldness, security teams can no longer keep up. As a result, more attacks are slipping through the defensive net while practitioners drown in logs and alerts that are harder to process and act upon.

There are reasons this has happened. The pandemic shift to remote operations vastly expanded the attack surface. There are many more cloud services and endpoints to keep an eye on, not to mention the volume of data flowing in and out of the network and the behavior of users working from everywhere. There are simply more network anomalies to spot in real time than current defenses were designed to handle.

Practitioners seeking a more holistic approach to threat detection and response are now looking to eXtended threat and response (XDR), a term coined by Nir Zuk of Palo Alto Networks in 2018.

Gartner views XDR as the evolution of endpoint detection and response, cloud-native platforms that more easily scale and synthesize hordes of detection data so security teams can better track threats and respond to incidents more thoroughly and quickly.

XDR platforms may vary by vendor, but all are designed to give organizations the needed visibility to root out adversarial threats without disrupting users or invoking alert fatigue. This allows security teams more time to perform solid investigations and improve their threat response posture whether an attack comes through a network, endpoint, email, or the cloud.

"Less than one in five respondents say they are very satisifed with their ability to correlate security data aross all products and services — no wonder there's great interest in eXtended Detection and Response (XDR) platforms. Our latest XDR research results show that only 12% are currently using it, but 77% are likely to invest in XDR in the next two years. Ease of use and price will drive purchasing decisions, but buyers are split on the benefits of Open XDR vs. Closed XDR platforms." – Matt Alderman, EVP, CyberRisk Alliance

RESEARCH METHODOLOGY

The data and insights in this report are based on an online survey conducted in February and March 2022 among 300 IT and cybersecurity decision-makers and influencers. Respondents represented U.S. organizations of all sizes and industries.

Organization size breakouts:

- Small (1–99): **24%**
- Medium (100–999): **30%**
- Large (1,000–1,999): **34%**
- Enterprise (10,000 or more): **12%**

Industry breakouts:

- Manufacturing: **23%**
- Business or professional services: **11%**
- Retail or ecommerce: **11%**
- Financial services and insurance: **11%**
- High-tech/IT: **9%**
- Other (healthcare, education, transportation, government, non-profits, media, energy, and utilities): **35%**

EXECUTIVE SUMMARY

Organizations continue to grapple with the pace of threats, especially those that evade existing cybersecurity solutions or go undetected for longer than they should. Even under the best of circumstances, security operations can be stretched thin by today's demands and the siloed nature of security solutions that scatter data and slow productivity.

Among the survey's key findings:

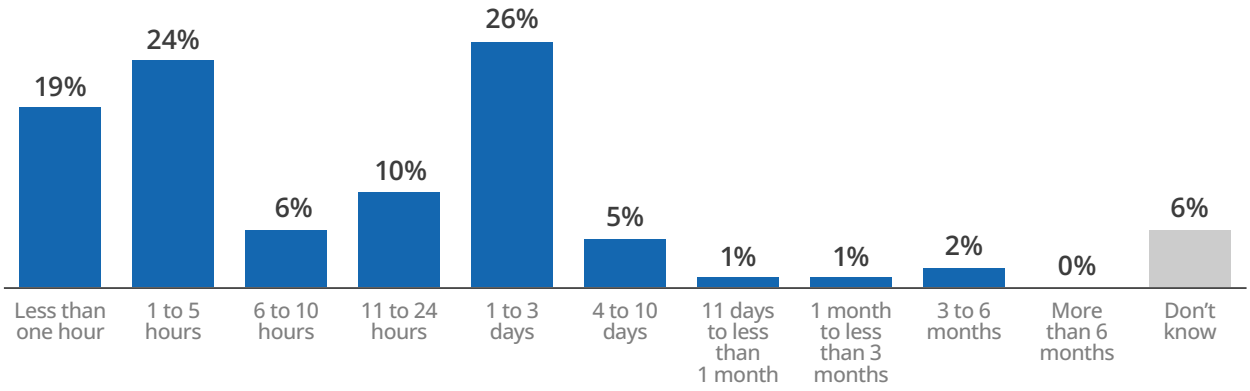
- The lack of visibility or context from existing security solutions caused 47% of respondents to miss threats at least once in the past 12 months.
- Only 17% are very satisfied with their ability to correlate security data across all products and services. Without the ability to see anomalies and/or malicious activities as they occur and across the spectrum of products and services, it's impossible to catch everything.
- Visibility into threats impacting their network was especially a problem for monitoring employee-owned endpoints, software vendors and third-party partners, with mean visibility scores of 4.6, 4.6, and 4.5 (out of 7), respectively.
- While familiarity with XDR is high (70%), current adoption of an XDR platform is relatively low — only 12% of respondents reported using this technology.

"We made the decision to implement XDR after a data breach, and I think it was the right call. Our organization is more secure than ever since we implemented XDR, and that's what we were looking for," said one satisfied XDR platform user.

ORGANIZATIONS MISSING THE RED FLAGS DUE TO LACK OF VISIBILITY AND CONTEXT

One of the persistent issues for cybersecurity teams is responding quickly to accurate threat assessments. A majority (59%) of those surveyed typically respond to an identified cyber threat within a day, while the remainder said it typically takes them days or weeks to detect and identify cyberthreats at their organization.

To the best of your knowledge, what is the average estimated time it typically takes to detect and identify real cyberthreats at your organization?



Common sense says the longer an incident goes unnoticed, the more potential for financial, legal, regulatory, and reputational damage. At the same time, today's IT infrastructures are now borderless and more porous to support modern technical and business ecosystems heavily reliant on networked, web-enabled devices, remote users, and third-party providers. As a result, protections must extend to everything from email and endpoints to on-premises datacenters and cloud workloads.

It is also no longer enough to thwart a threat. To prevent similar attacks, cybersecurity professionals need time to isolate and analyze the malware or unexpected user behavior, then adjust their products, policies, procedures, and awareness training.

In this study, almost everyone said they were capable of doing at least some of the legwork in response to a real threat — with 60% indicating their ability to contextualize real cybersecurity threats was very or extremely accurate.

When asked specifically about missed cyber threats due to lack of visibility and context, 47% believed they had been compromised at least once in the past 12 months.

Known threats ran the gamut, from careless employees to outsiders seeking to steal trade secrets and client lists. The human element — whether from turnover on the security team or an undertrained workforce falling for phishing scams — was a common theme among those with compromised defenses.

Several in the study also took their threat monitoring or endpoint detection solutions to task, admitting their current tools were no match for today's sophisticated attacks.

"Too many tools are not identifying the real threats but are identifying false threats," noted one respondent. Indeed, log management has long been an issue for teams that must weed out false positives and negatives.

Another respondent suffered a data breach last year and didn't find out until it was too late.

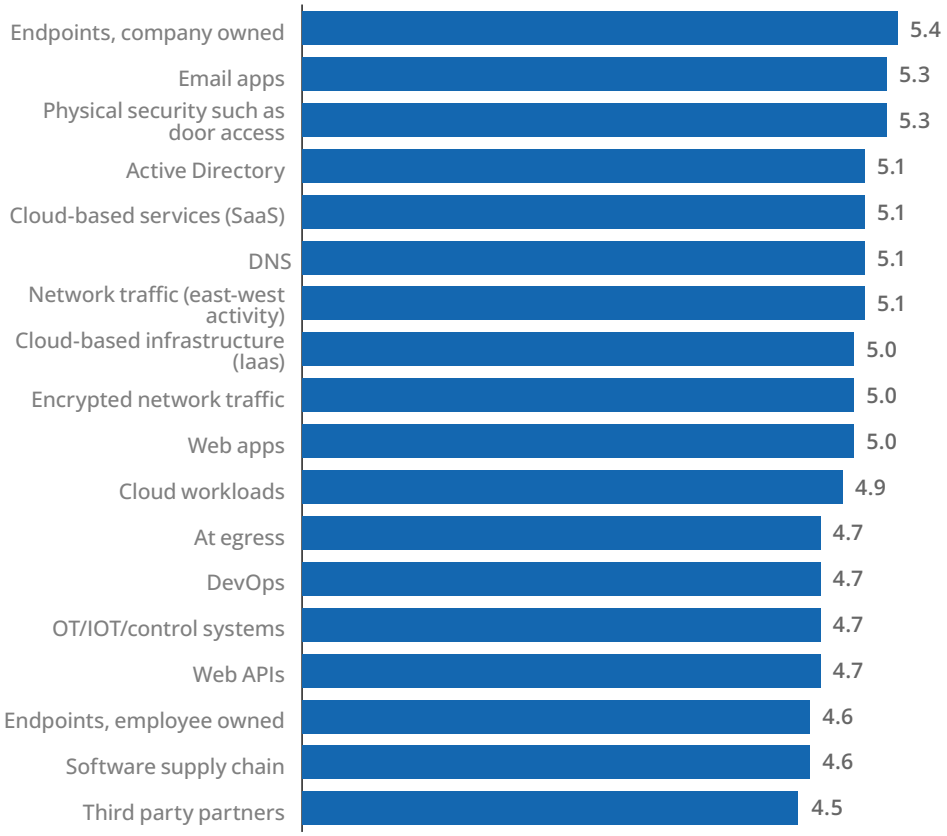
"We didn't see any red flags; everything was normal. However, we were actually under attack. Even though we discovered it in less than 10 days, that's still a lot of time when you're under attack. I know some companies don't find out that they suffered a data breach after like six months, and that's really crazy."

NEED FOR IMPROVED THREAT VISIBILITY INTO EMPLOYEE-OWNED ENDPOINTS, SOFTWARE SUPPLY CHAIN, AND THIRD-PARTY PARTNERS

One of the most touted benefits of XDR platforms is their ability to collect and correlate data from any source, including third parties. A SIEM also collects data from multiple sources, but the volume of alerts can overwhelm a team. Augmenting a SIEM with XDR allows security analysts to dig deeper into the data, so attention is paid to relevant threats by context, not just volume.

Providing access to all activity from one platform also gives security analysts better context to generate accurate reports and respond quickly when needed. But such visibility remains hard to come by. Only 17% of study participants were very satisfied with their current ability to correlate security data across all security products and services. Visibility into threats impacting their network was especially a problem for monitoring employee-owned endpoints, software vendors and third-party partners, with mean visibility scores of 4.6, 4.6, and 4.5 (out of 7), respectively.

For each of the following, please rate your organization's level of visibility into threats impacting your network. Please rate each on a scale from 1 to 7, where 1 is "No visibility" and 7 is "Very high visibility."



These trouble spots point to significant shifts in the past two years. During the pandemic, organizations that sent employees home with corporate equipment could more easily notice suspicious activity on issued devices and network traffic than those that allowed workers to use personal devices and home networks for official work. Said one participant who cited employee negligence for missing a threat: "We are so shorthanded that tasks are sometimes not carried through with the same level of care."

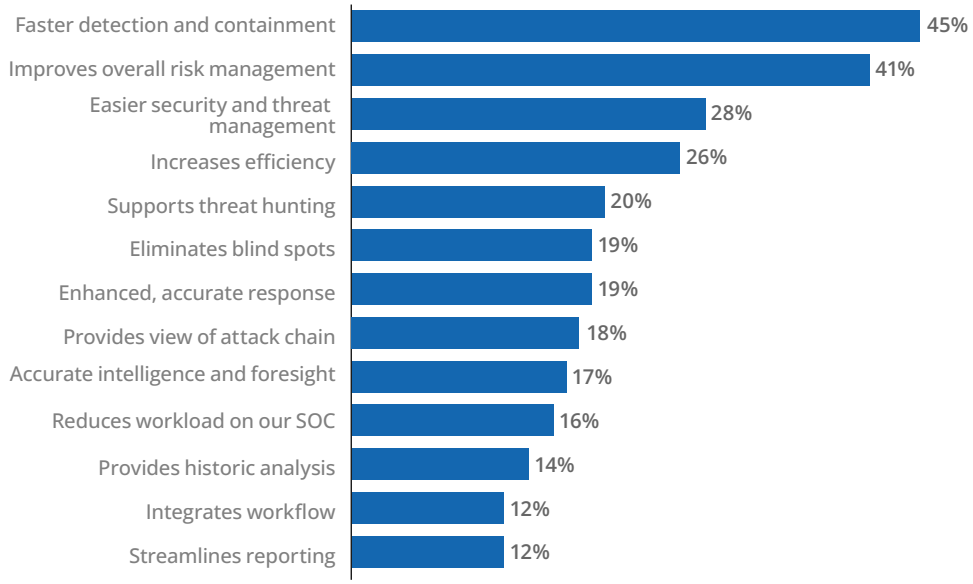
Another trouble spot is the increased data breaches arising from third parties, especially for organizations using more of them to fill workforce gaps. In a recent CRA Business Intelligence study, a majority of respondents (60%) reported a third-party partner was to blame for an IT security incident experienced by their organization in the past two years, with 45% of the victims incurring between $100,000 and $1 million in damages. (Source: CRA Business Intelligence Third-Party Risk Study, December 2021).

FASTER DETECTION AND IMPROVED RISK DETECTION ATTRACTING XDR USERS

XDR, a SaaS-based security threat detection and incident response tool, natively integrates multiple security products into a cohesive security operations system that unifies all licensed components. In essence, XDR technology is built to:

- ***Identify*** hidden and/or highly sophisticated threats across an organization's IT security ecosystem
- ***Improve*** detection and response times
- ***Investigate*** threats efficiently with a centralized user interface

What do you consider to be the top benefits of an eXtended Detection and Response (XDR) platform? Select 3 choices.



While familiarity with XDR is high (70%), current adoption of an XDR platform is relatively low — only 12% of respondents reported using this technology. Those using or familiar with XDR view the top benefits as faster detection (45%) and overall risk management improvement (41%) while streamlined reporting and integrating workflows were perceived as much lower-order benefits.

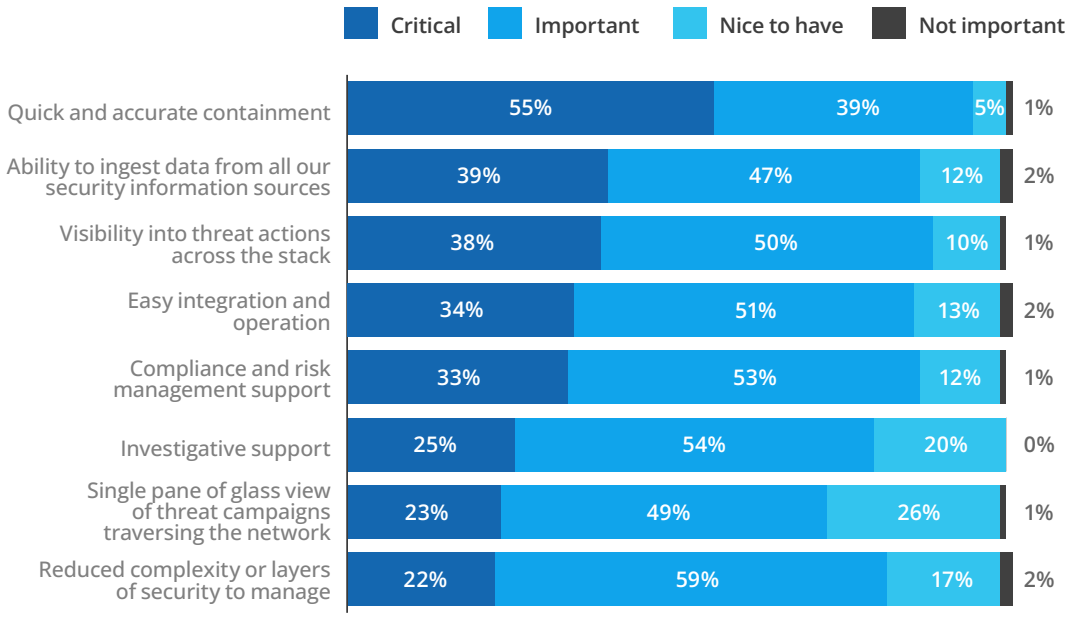
Nearly half (46%) of XDR users reported they are very satisfied with their XDR platforms (two-thirds of respondents reported their organization has

one or two XDR platforms). XDR users commented that they benefit from faster discovery rates, more accurate reporting, and ease of use.

"It runs smoothly with other software we are using and catches almost every threat and issue. It is easy to deploy, easy to update, can make changes as needed quickly, and our employees are able to get up to speed quickly" was one among many describing the benefits of XDR.

While XDR technology has yet to become widespread, a large majority (77%) of current users and others familiar with XDR report they are somewhat or very likely to invest in XDR technology in the next two years. Among those not yet deploying XDR, 55% believe the quick and accurate containment ability of XDR would be a critical capability for their organization, which addresses the common challenge of reducing the time it takes to hunt down a legitimate threat. Another 39% of future XDR adopters said the ability to ingest data from all security information sources is critical.

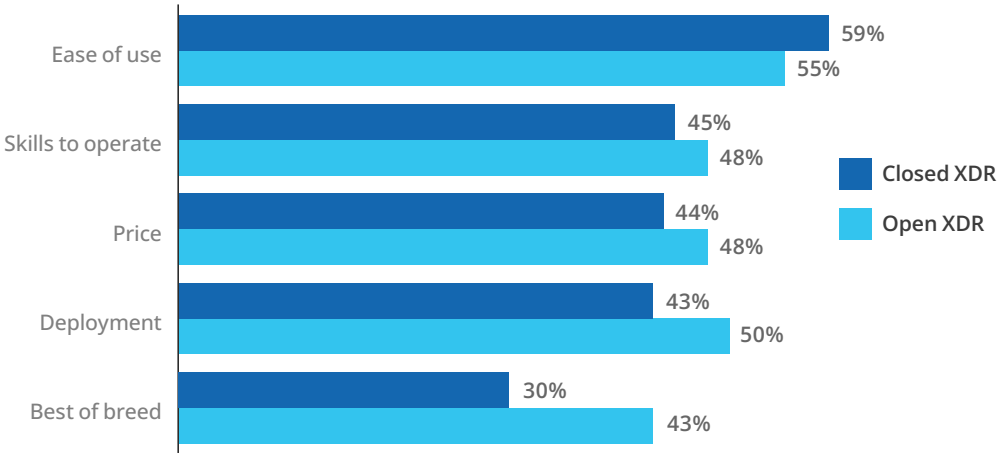
How would you rate the importance of each of the following XDR platform features/capabilities to your organization?



Note: Totals may not sum to 100% due to rounding.

For those likely to invest in XDR technology in the near future, ease of use is, by far, the most important perceived benefit to their organization, whether planning to integrate the technology with their existing security tools or establishing a single-vendor, XDR-ready infrastructure. Respondents also indicated other near-term investments in solutions for unifying detection and response and improving visibility across security products/services respondents were most likely to be endpoint detection and response (EDR), network detection and response (NDR), security information event management (SIEM), and threat intelligence.

In considering an XDR technology investment, which of the following do you think are the top benefits of an open XDR infrastructure (which integrates with existing security tools) vs. a closed (single vendor) XDR-ready infrastructure? Please select all that apply for each.



WHICH FORENSICS TOOLS DO YOU USE IN INVESTIGATIONS?

Respondents were asked if they had investigated an incident and which tools they used. Here's what some said:

"Our web server was hijacked. Being federal, the FBI cloned our system and investigated using the current tools at the time. We also used log analyzers to determine when and where the incursion occurred."

–IT specialist for a government organization

"We used our SIEM and Azure 365/Microsoft Security Center to do a lot of the investigation."

–Cybersecurity specialist, enterprise in the education sector

"When we conduct cyberattack investigations, we hire third-party IT specialists who pick and choose the necessary tools."

–Director of security operations for a small energy firm

"I have been involved in investigation of a recent cyber-attack. Tools we used included Kali Linux and Metasploit."

–Senior VP for a professional services enterprise

"I was involved with a DDOS attack a few years ago. We mainly relied on manual log reviews, network analysis and our third-party DDOS prevention provider to assist with the investigation."

–Application support team lead for an enterprise-level insurance company

CONCLUSION

One reason threats get through despite ample cybersecurity solutions is a workforce gap, both internally and globally. Though talent pipelines are finally filling with qualified professionals with diverse backgrounds, a 2.7 million cybersecurity workforce shortage remains, according to (ISC)[2], which has been tracking global workforce supply vs. demand for more than a decade. That gap was more than three million the prior year.

The ability of XDR to flag threat indicators early and shut down advanced threats before they can breach networks is one way to counter bad actors with limited human resources. Not only does it serve as a fail-safe to threat hunting, but it buys cybersecurity analysts more time to thoroughly investigate how to prevent future attacks — whether by hardening protections around specific targets or better educating employees on the latest phishing techniques. And it does this using the deeper data XDR collects and crunches from specific sources.

XDR doesn't supplant many of the cybersecurity tools already up and running; it supports them by corralling the data everything else generates, running that information through deeper analytics and then locating and isolating the threats that surface — or would otherwise remain hidden within millions of security alerts generated daily.

IT security and business risk decision-makers appreciate XDR's ability to better detect and contain threats and improve overall risk management. They also like the easier security and threat management and increased efficiencies that make life a little easier for everyone hunting threats.

As one respondent described XDR: "You've read all about the devastating impact that breaches cause, and you know this is a very bad situation. There is no time to waste, you need to act as soon as possible to do as much damage control as you can."

Organizations may have been hesitant to invest in XDR and fully integrate platforms with other solutions to maximize benefits. But those who have purchased these platforms indicate they are satisfied with their ease of use, improved visibility, and data contextualization.

The study suggests XDR is on track to become mainstream in the coming years, becoming a much-needed force multiplier for those professionals tired of being told to do more with less.

ABOUT CYBERRISK ALLIANCE

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, Identiverse, ChannelE2E and MSSP Alert. More information is available at ***http://cyberriskalliance.com/***.

ABOUT eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow *@eSentire*.

ABOUT EXTERRO

Exterro empowers forensic and legal teams to proactively and defensibly manage their Legal Governance, Risk and Compliance (Legal GRC) requirements. Exterro recently acquired AccessData to become the only comprehensive software platform that automates the complex interconnections of Digital Forensic Investigations, E-Discovery, Data Privacy, and Cybersecurity Compliance. Thousands of forensic and legal teams around the world in corporations, law firms, government, and law enforcement agencies trust our integrated Legal GRC platform to manage their risks and drive successful outcomes at a lower cost. For more information, visit *www.exterro.com*.

