CYBEREDGE GROUP

# 2022 STATE OF EXTENDED DETECTION AND RESPONSE (XDR)

A Survey of International IT Security Professionals on Their Motivations for Leveraging XDR, the Benefits of XDR, and the Rationale for Outsourcing XDR's Management

**July 2022**

A CYBEREDGE RESEARCH STUDY SPONSORED BY:

opentext™

# Table of Contents

# Introduction

The 2022 State of Extended Detection and Response (XDR) report takes a close look at the current state of this emerging technology's adoption. For our survey, we wanted to talk to the people who are involved in security technology selection and procurement decisions, including executives as well as directors and managers in IT security operations. We also wanted to hear from security analysts, incident responders, architects, engineers, and compliance auditors—the people on the front lines who work with security technologies on a day-to-day basis.

Our objective for this report is to understand the market's current understanding of and progress in adopting extended detection and response (XDR) and managed extended detection and response (MXDR) offerings.

The survey at the heart of this report was conducted in March and April of 2022. At this time, XDR is still an emerging category within the cybersecurity market. As a result, we expect industry stakeholders' perceptions of the definition and capabilities of XDR to change in the future as adoption proceeds and the market matures.

CyberEdge would like to thank our research sponsor, OpenText, who conceived this report and whose support has been essential to its success.

## Top Five Insights

This report contains dozens of actionable insights on the state of XDR adoption. Here are our top five takeaways:

1. **Enthusiasm is running high.** The current cyber threat landscape is unquestionably challenging, and security programs continue to struggle with staffing shortages and complex cybersecurity toolsets. XDR is expected to mitigate some of these difficulties by consolidating the capabilities of multiple security products into a cohesive platform. Stakeholders are eager to adopt emerging technologies that promise to reduce operational costs, improve efficiencies, and enhance security practitioners' effectiveness.
2. **When it comes to XDR's native capabilities and integrations, expectations vary.** As a new market category, XDR is relatively poorly understood. While security leaders and practitioners know that consolidating a broad array of tools' capabilities is beneficial, there's a lack of agreement about what, exactly, should be part of an XDR solution and what should instead be integrated into it.
3. **Adopters expect to see dramatic operational cost savings.** Nearly all survey participants (99.2%) expect XDR's adoption will reduce their organization's technology and personnel costs. Because the strength of this perceived benefit is so great, there's less concern about the cost of the technology itself.
4. **XDR's perceived complexity is a worry.** While more than 98% of respondents either have adopted XDR or are planning to do so in the near-term future, a majority of stakeholders are looking for a solution that will be easy to use. Furthermore, respondents prize excellent customer support, both from the XDR solution's vendor and from prospective MXDR providers. Factors that make XDR's benefits more accessible are highly valued.

### Survey Demographics

- **Responses received from 400 qualified IT security operations executives, managers, and practitioners**
- **All from organizations with 500 or more employees**
- **Representing eight countries: Australia, Brazil, Canada, India, Singapore, South Africa, the United Kingdom, and the United States**
- **Representing 17 industries**

# Introduction

5. **Outsourcing management and monitoring of XDR is increasingly attractive.** More than 94% of survey participants either rely on an MXDR provider to manage their XDR solution or are planning to do so. Given the perennial challenge of skills shortages in cybersecurity as well as the fact that MXDR can enable access to expertise, knowledge of best practices, and shared efficiencies on a 24x7x365 basis, the tendency to lean on third-party experts is only logical.

## About This Report

The findings of this report are divided into four sections:

### Section 1: Adoption

XDR is an emerging category within the security product market. It promises to consolidate the capabilities of multiple security tools and products within a single, centralized, and cohesive platform. For security programs that have long struggled to achieve comprehensive visibility across increasingly complex IT ecosystems, this is an attractive proposition. This section of the survey provides insights into the current state of XDR adoption. It looks at current XDR adoption as well as respondents' plans for acquisition. It also reveals which XDR use cases are most important to respondents, as well as what they're looking for in an XDR vendor.

### Section 2: Technology

Because XDR is an emerging market category, which capabilities XDR solutions should or should not include is not always well understood. The questions in this section focus on which security tools survey participants believe should be part of every best-of-breed XDR solution, and which security tools and capabilities should be integrated with such systems. This information can help readers compare what they're looking for in an XDR solution with their peers' expectations.

### Section 3: Benefits

What are adopters of XDR hoping to achieve through their implementation of this technology? The third section investigates the benefits that survey participants expect that an XDR solution will enable their security program to realize. Among the biggest value propositions offered by XDR are improving security operations staff efficiency, mitigating cyber risk, and reducing personnel and technology costs.

### Section 4: Managed Security Services

In the last section, we asked survey participants about their plans and reasons for outsourcing the management of an XDR solution to an MXDR provider. Access to skilled personnel is critical for maximizing the value of the detection and response capabilities that an XDR solution can provide. We asked about personnel shortages in IT security, as well as use cases for outsourcing the monitoring and management of an XDR solution. We also asked about current plans to outsource XDR's management, as well as what strengths and capabilities are most important in an MXDR vendor.

## Navigating This Report

We encourage you to read this report from cover to cover so you don't miss any valuable tidbits. That said, there are three other ways to navigate through the report if you're looking for a particular topic:

- **Table of Contents.** Each topic in the Table of Contents pertains to specific survey questions. Click on any topic to jump to its corresponding page.
- **Research Highlights.** The Research Highlights page showcases the most significant headlines of the report. Page numbers are referenced with each highlight so you can quickly learn more.
- **Navigation tabs.** The tabs at the top of each page are clickable, enabling you to conveniently jump to different sections of the report.

# Research Highlights

## Adoption

- **Widespread enthusiasm.** More than 98% of respondents either already have an XDR solution in production, are planning to implement one, or are currently evaluating solutions (page 6).
- **Multiple use cases matter.** While organizations are most interested in gaining the ability to automatically detect and respond to threats and better prioritize responses, all of the use cases we asked about were rated highly (page 7).
- **Ease of use is paramount.** More than half of respondents (51.4%) said that ease of use was what they most needed in an XDR solution (page 8).
- **Accuracy over cost.** While 45.8% of respondents said that accurate threat detection was among the most important factors for choosing an XDR solution, only 30.8% cited cost (page 8).

## Technology

- **EDR, DLP, NDR, and TIP are most important capabilities to include in XDR.** Nearly 40% of respondents believe that EDR, DLP, NDP, and TIP capabilities should be part of a cohesive, unified XDR solution (page 9).
- **NDR and TIP are the most important capabilities to integrate.** Approximately 40% of survey participants view NDR and TIP as particularly important to integrate with an XDR solution (page 10).
- **XDR definitions vary.** As a market category, XDR remains immature. As a result, there's a lack of agreement about which tools' capabilities should be included in an XDR solution, and which should be integrated (page 9 and page 10).

## Benefits

- **XDR's expected to mitigate risks.** Over 93% of respondents agree that implementing XDR will improve their organization's ability to mitigate cyber threat risks and lower costs (page 11).
- **Big cost reductions.** Nearly all survey participants (99.2%) agree that adopting XDR will enable their organizations to realize cost savings, with a mean expected cost reduction of 25% (page 12).
- **Speed and efficiency improvements ahead.** Over 98% of respondents believe that adopting XDR will improve the efficiency of their security operations staff, with reducing time-to-remediate seen as especially important (page 13).

## Managed Security Services

- **Wanted: more skill and expertise.** Over 73% of organizations lack the skilled IT security personnel that they'd need to fill all open positions in their security program (page 14).
- **MXDR's on the rise.** Not only are nearly half of organizations (46.9%) already outsourcing the management and monitoring of their XDR solution to an XDR provider, but an additional 47.5% are planning to do so (page 15).
- **More efficiency, less risk.** Most respondents are seeking an array of benefits from MXDR; reducing risks by leveraging best practices from an expert is seen as important, but so are efficiencies (page 16).
- **Effectiveness and visibility matter.** Most of all, stakeholders want an MXDR provider whose solution will enhance their visibility into threats and ability to take action (page 17).

# Section 1: Adoption

## State of XDR Adoption

**Select the option that best describes your organization's adoption of an extended detection and response (XDR) solution.**

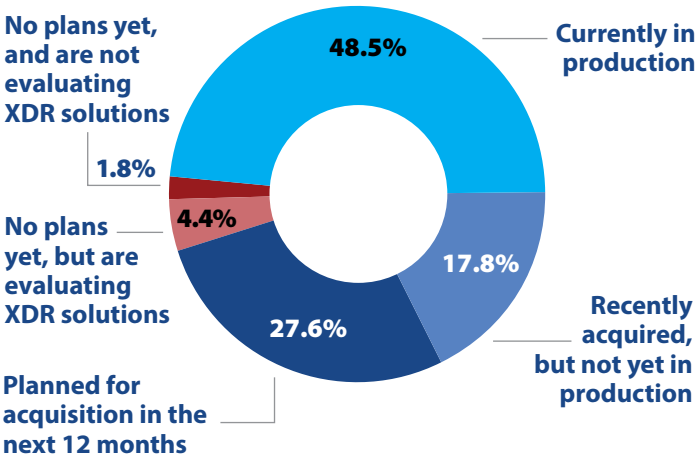


*Figure 1: Percentage of organizations with XDR solutions currently in production, as well as organizations with and without plans to acquire them.*

XDR is an emerging technology category that's received a great deal of analyst and media attention of late because it promises to improve efficiency in security operations, as well as to enhance the visibility and capabilities that even resource-constrained teams can achieve. In this survey, we asked participants if they had already adopted and implemented an XDR solution, or if they were planning to do so within the next 12 months (see Figure 1).

A large majority of respondents (more than 98%) reported that they already have an XDR solution in production, are planning to acquire one or implement one, or are currently evaluating vendors and solutions.

We were surprised to see adoption rates so high, but this finding may reflect the relative maturity of security programs within this particular audience. Nearly half (49%) of survey participants have roles in organizations with more than 5,000 employees, and a significant majority (77%) hold executive or management positions.

This well-informed and sophisticated audience clearly has no trouble understanding the benefits of this technology, or that there's an enormous market need for the cost and operational efficiencies that XDR has the potential to provide.

Among industries, the financial services sector leads the way in XDR adoption, with over 60% of respondents currently having a solution in production. Government agencies are the least likely to have already adopted XDR, with only 33% currently having a solution in place; 11% have not yet even begun evaluating XDR solutions.

**This well-informed and sophisticated audience clearly has no trouble understanding the benefits of this technology, or that there's an enormous market need for the cost and operational benefits that XDR has the potential to provide.**

# Section 1: Adoption

## XDR Use Cases

**On a scale of 1 to 5, with 5 being highest, rate the importance of each of the following XDR use cases.**

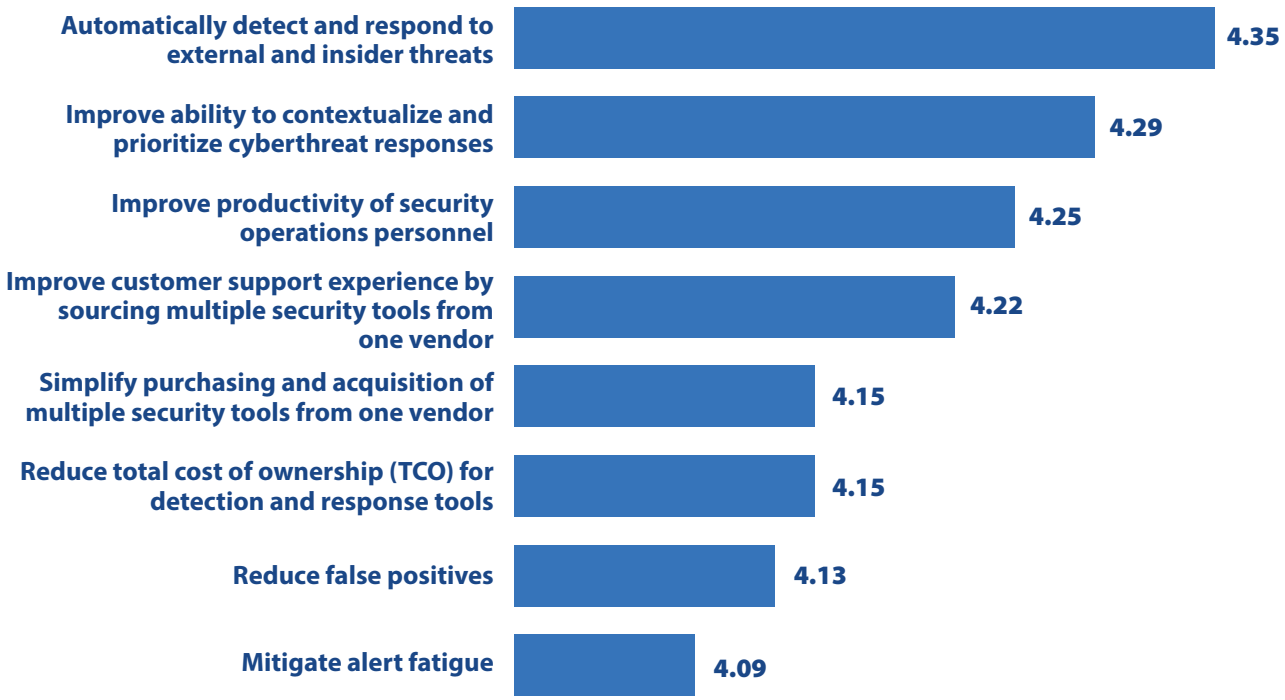


*Figure 2: Most important use cases for XDR*

We've already determined that organizations are embracing XDR. With more than 98% of organizations already having a solution in place or planning to implement or acquire one (see Figure 1), it's clear that awareness of the benefits of this emerging technology is high.

To better understand the motivations of organizations that are enthusiastically adopting XDR, we asked survey participants which XDR use cases were most important to them. As it turns out, all of them!

Every one of the use cases we asked about was rated higher than 4.0 on a five-point scale where 1 is of little importance and 5 is the highest level of importance (see Figure 2). Responses were tightly clustered, meaning that all use cases were considered to be similarly important.

The two use cases with the highest importance ratings were automatically detecting and responding to external and insider threats (4.35) and improving the ability to contextualize and prioritize cyberthreat responses (4.29). But even the use case with the lowest importance rating, mitigating alert fatigue, was still considered to be of the highest importance by 38% of respondents. In fact, all the use cases were rated as having high (4) or highest (5) importance by more than 76% of respondents.

# Section 1: Adoption

## What's Needed in an XDR Vendor

**Which of the following factors are most important when evaluating XDR vendors?**

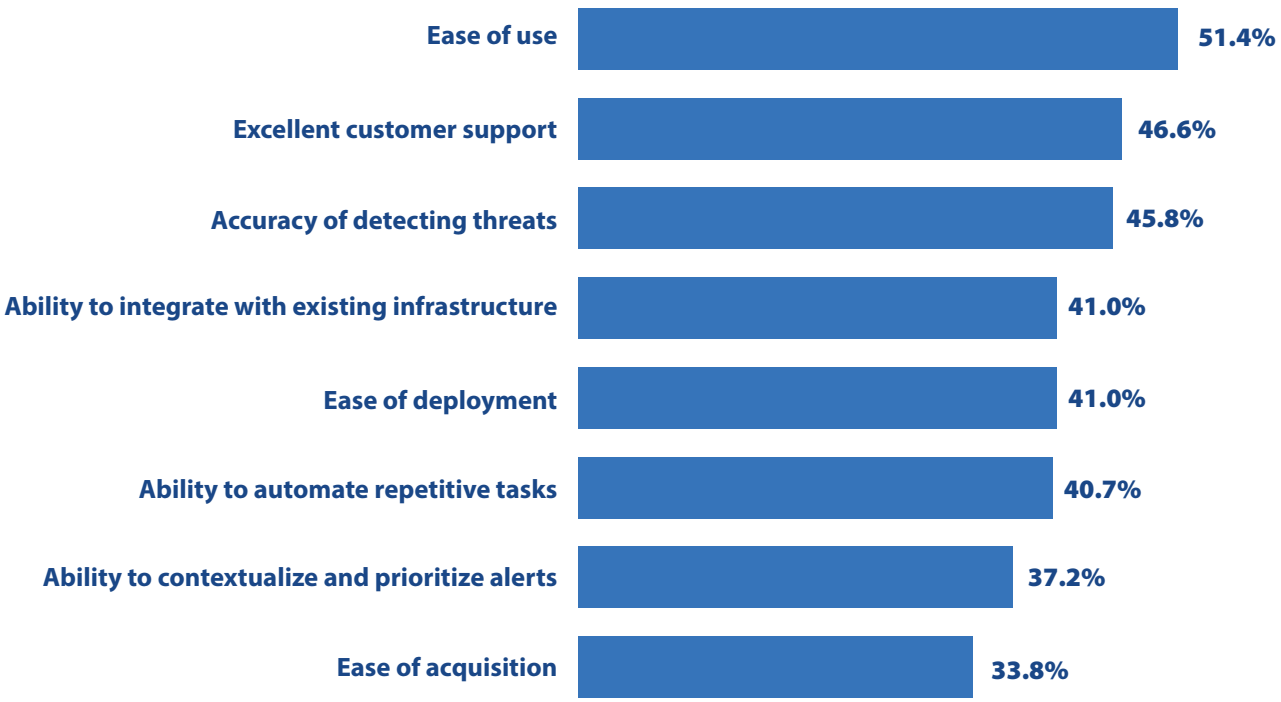


*Figure 3: Most important factors when evaluating XDR vendors.*

Many security programs are implementing or seeking out XDR solutions with hopes of enhancing their security team's productivity and strengthening detection and response capabilities. However, the number of vendors entering this fast-growing market is rapidly increasing. We were curious which factors were most important to XDR solution buyers, and what key differentiators might set best-of-breed solutions apart.

The most often-cited qualities that organizations are looking for in an XDR solution include ease of use (cited by 51.4% of respondents) and excellent customer support (cited by 46.6% of respondents) (see Figure 3). XDR's perceived complexity is apparently a concern for many potential buyers, who want to find solutions that will make security operations teams' jobs easier while enabling them to accomplish more. Also important was accuracy of detecting threats (cited by 45.8% of respondents). For 40.7% of respondents, the ability to automate repetitive tasks mattered.

Third-party validation (by analyst firms such as Gartner or Forrester) was the least important factor overall, mentioned by only 19.9% of respondents. This suggests that a vendor who is able to demonstrate a solution's accuracy, ease of use, and top-notch customer support may be able to overcome a lack of third-party validation to gain market share.

Cost was also among the least important factors, with only 30.8% of respondents indicating that they thought it was important. It's likely that many organizations expect that implementing XDR will help them to lower security operational costs overall, so much so that the cost of the solution itself isn't deemed critically important.

# Section 2: Technology

## Tools to Be Included in XDR

**Which of the following security tools should be provided by every best-of-breed XDR vendor as part of a cohesive, unified security incident detection and response solution? (Select all that apply.)**

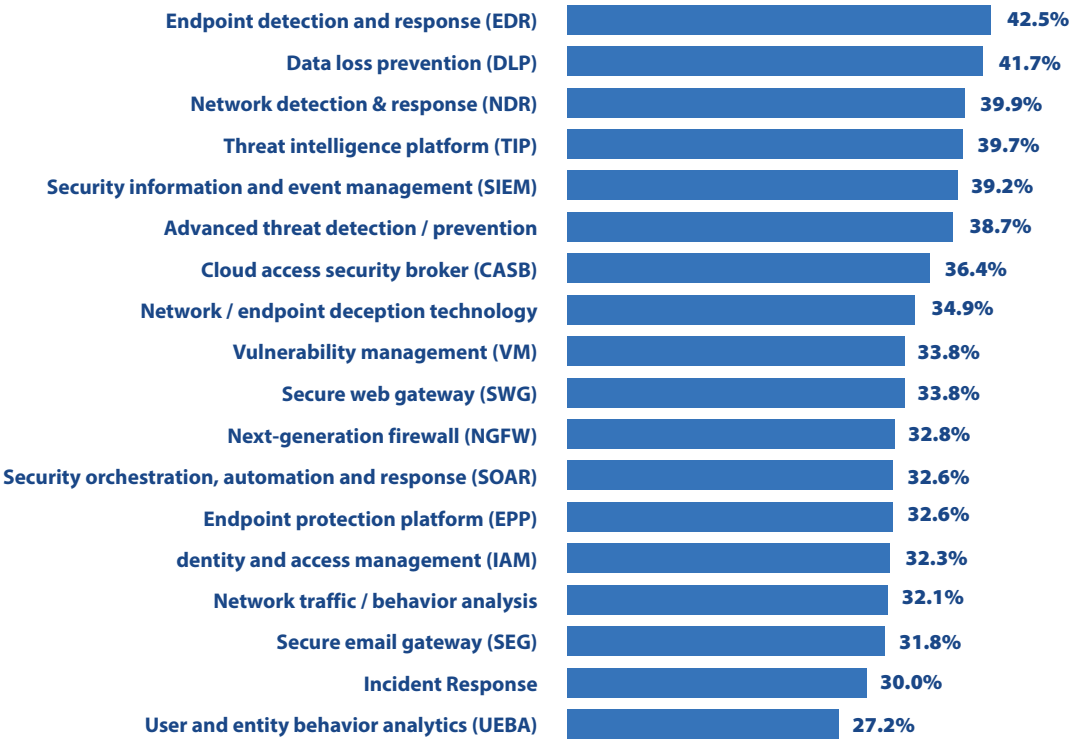


*Figure 4: Tools that should be provided as part of comprehensive XDR.*

While XDR is seeing enthusiastic adoption across a broad array of industries, what exactly should fall into this fledgling market category is often unclear to prospective buyers. We asked about the capabilities of 18 different security tools, and almost every one of them was seen as important to include in an XDR solution by approximately one-third of respondents (see Figure 4).

The most frequently cited capabilities were those of endpoint detection and response (EDR) products (mentioned by 42.5% of survey participants), data loss prevention (DLP) products (mentioned by 41.7%), and network detection and response (NDR) products (mentioned by 39.9%). But more than 33% of respondents said that as many as ten distinct capabilities were important.

We were surprised to see that security information and event management (SIEM) wasn't at or near the very top of the list. After all, XDR products have been viewed as both functionally similar to SIEM tools and as an attempt to solve some of the biggest security operations challenges that SIEM's adoption has raised. It seems that some respondents view XDR as a potential replacement for SIEM while others see SIEM capabilities as something that needs to be included within an XDR solution.

These inconsistencies likely reflect a market and industry that is still maturing. It's likely that expectations and definitions will become more uniform as the use of XDR becomes more widespread.

# Section 2: Technology

## Tools to Be Integrated with XDR

**Which of the following security tools, if not provided by the XDR vendor, are important to integrate into a comprehensive XDR solution?**

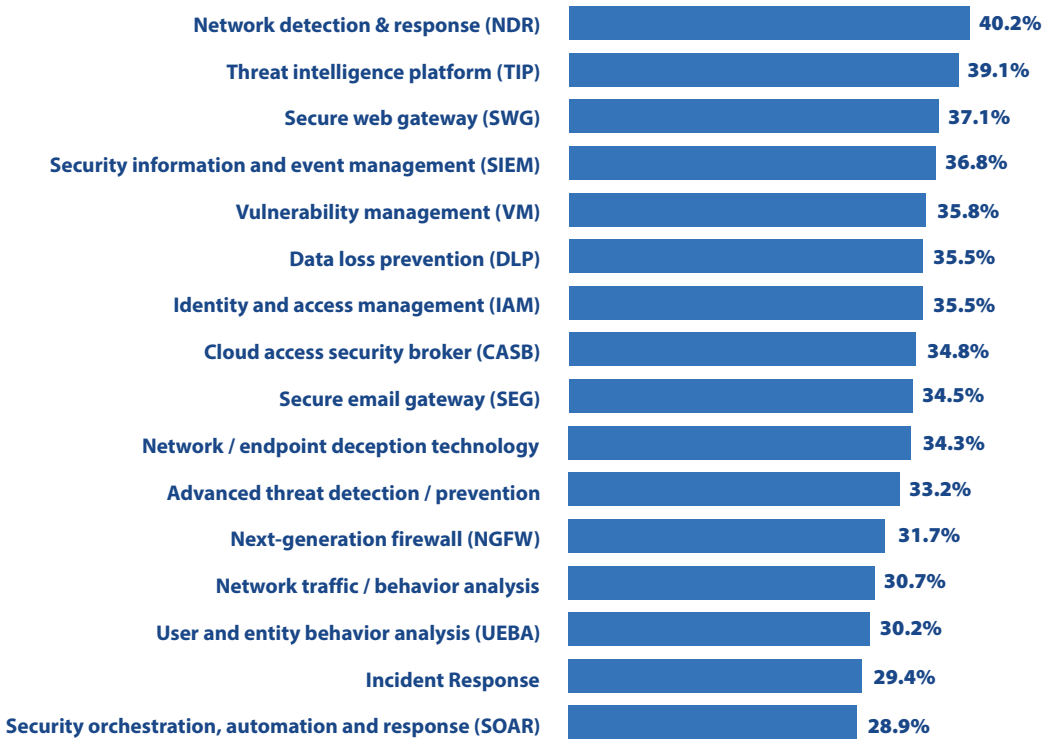


*Figure 5: Tools that should be integrated to achieve comprehensive XDR.*

As was also the case with native capabilities, survey participants viewed a broad array of integrations as desirable. More than one-third of the respondents cited at least 11 security tools' capabilities as important to integrate with XDR (see Figure 5).

Network detection and response (NDR) capabilities (mentioned by 40.2% of respondents) were seen as particularly important to integrate, as were threat intelligence platform (TIP) capabilities (mentioned by 39.1%).

Several of those ranked near the top of the list of important-to-include capabilities (such as DLP, NDR, TIP, and SIEM) were also at or near the top of the list of important-to-integrate capabilities. This overlap speaks to the fact that this market is still being defined. Many prospective adopters remain unsure of which product capabilities should be part of XDR and which should be incorporated through the integration of other vendors' products.

What's clear, however, that achieving centralized visibility and infrastructure protection across as much of the security architecture as possible is desirable to most stakeholders in this industry.

# Section 3: Benefits

## XDR's Risk and Cost Impact

**Select the option that best describes your agreement with the following statement: "Once fully implemented, I expect our XDR solution to significantly improve my organization's ability to mitigate the risks of advanced cyberthreats while lowering our operational costs."**

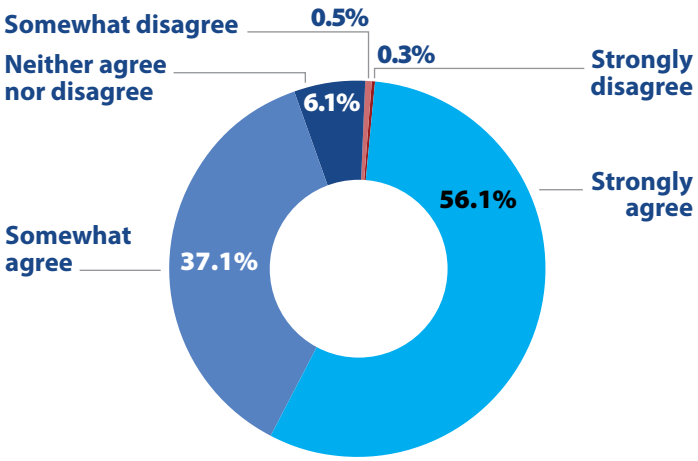


*Figure 6: Percentage of respondents who agree or disagree that XDR can improve their organization's ability to mitigate risks while lowering costs.*

We've already noted that there's widespread enthusiasm for XDR adoption among survey participants, but which specific benefits are stakeholders hoping this technology will enable their organizations will realize? To answer this question, we asked respondents if they agreed that XDR's implementation could be expected to significantly improve their organization's ability to mitigate cyber risks while lowering operational costs.

Agreement was near-universal, with more than 93% of respondents stating that they strongly or somewhat agreed with the statement (see Figure 6).

Among industries, the financial services sector led the way in enthusiasm for XDR's benefits, with over 98% of survey participants agreeing that they expect XDR to improve their organization's ability to mitigate cyber risks while reducing costs (see Figure 7). Other highly regulated industries were more guarded in their responses, with only 90% of healthcare respondents in agreement, and 81.8% of those in government.

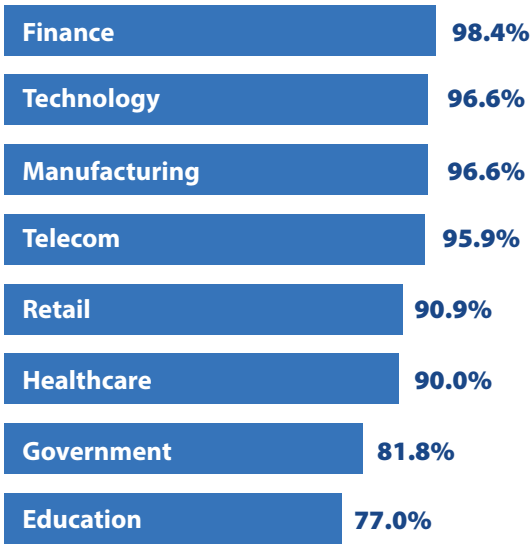


*Figure 7: Percentage of respondents who generally agree that XDR can improve risk mitigation while lowering costs, by industry.*

# Section 3: Benefits

## Cost Reduction from XDR

**Estimate the total annual cost reduction (i.e., personnel costs, technology costs) you expect your organization to achieve by consolidating multiple security tools into a cohesive, unified XDR solution.**

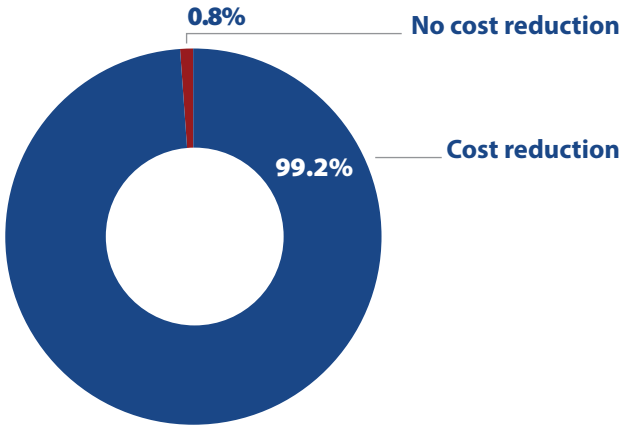


*Figure 8: Percentage of organizations expecting to see a cost reduction from XDR's adoption.*

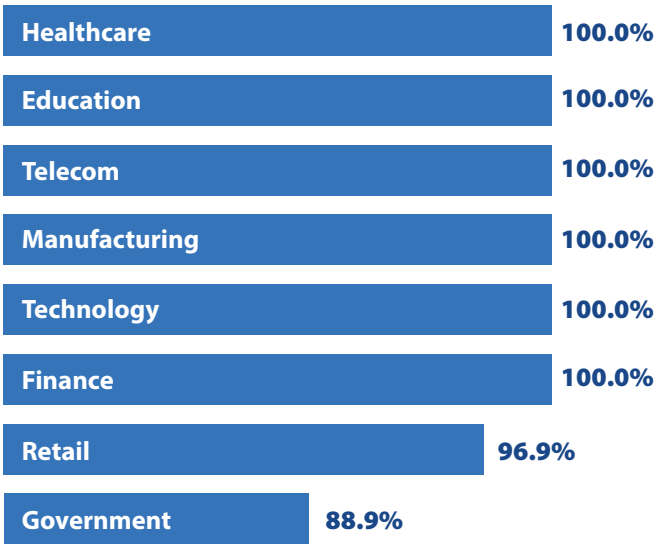


*Figure 9: Percentage of organizations expecting to see a cost reduction from XDR's adoption, by industry.*

There's great confidence among security leaders and practitioners that XDR will quickly pay for itself, and this confidence is consistent across industries and geographies. Over 99% of survey participants said that they expect to see a cost reduction from implementing XDR (see Figure 8). The global mean cost reduction that they expected to see was 25.0%.

Organizations in some highly regulated industries are anticipating particularly large cost reductions from implementing XDR. Respondents in financial services are expecting to see a mean cost reduction of 32.9%, while those in healthcare expect to see a 27.4% cost reduction (see Figure 9).

Overall, it's clear that there's near-universal agreement in the market that XDR's adoption has the potential to create efficiencies that will lower costs. With cybersecurity spending continuing to climb year after year, this is among XDR's most promising possible benefits.

**There's great confidence among security leaders and practitioners that XDR will quickly pay for itself... Over 99% of survey respondents said that they expect to see a cost reduction from implementing XDR.**

# Section 3: Benefits

## Efficiency Improvements from XDR

**Which of the following security operations staff efficiency improvements, commonly realized by organizations that embrace XDR, do you believe would have the greatest impact on your organization?**

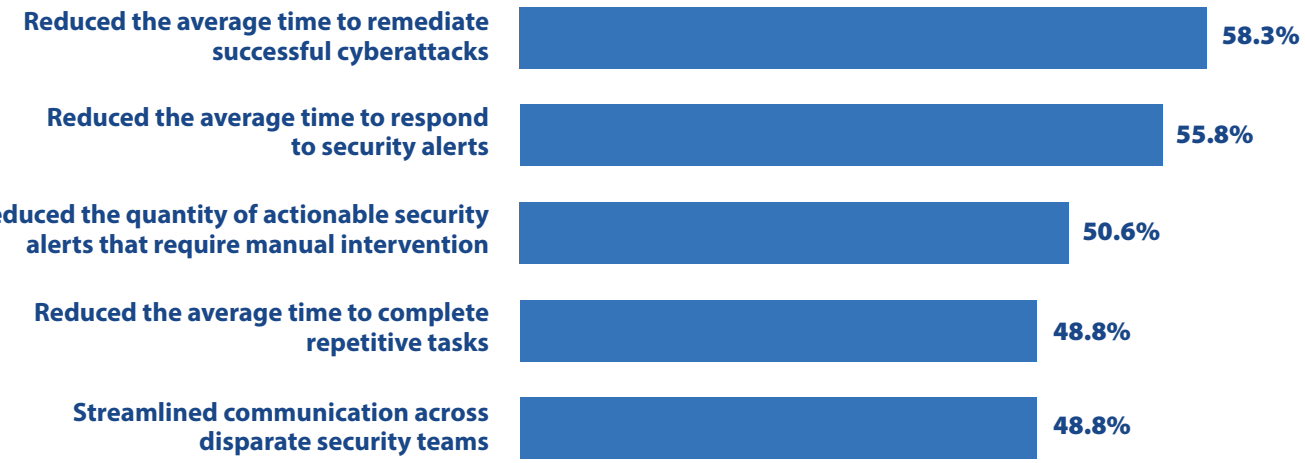


*Figure 10: Security operations staff efficiency improvements to be realized from implementing XDR.*

We took a closer look to see which security operations staff efficiency improvements, commonly realized by organizations embracing XDR, were perceived as most impactful by survey participants. All of the efficiency improvements we asked about were perceived as important by a majority or near-majority of respondents (see Figure 10). Even the improvement that was ranked as important least often, streamlining communication across disparate security teams, was still considered important by 46.8% of respondents.

Given the enthusiasm for XDR's adoption, it's unsurprising that more than 98% of respondents believe that XDR will improve security operations staff efficiency. Beyond this general agreement, reducing the average time to remediate successful cyberattacks was ranked among the most impactful efficiency improvements by 58.3% of respondents, while 55.7% ranked reducing the average time to respond to security alerts as most impactful.

Of course, when it comes to reducing the impact of a security incident, time is of the essence, so it's only to be expected that speeding remediation and response would be important to security professionals. However, given the extent of the challenges that today's security operations teams face, it's logical that all efficiency improvements to be gained from adopting XDR would be of significant value.

# Section 4: Managed Security Services

## Staffing Shortages

**Is your organization currently experiencing a shortage of skilled IT security personnel?**

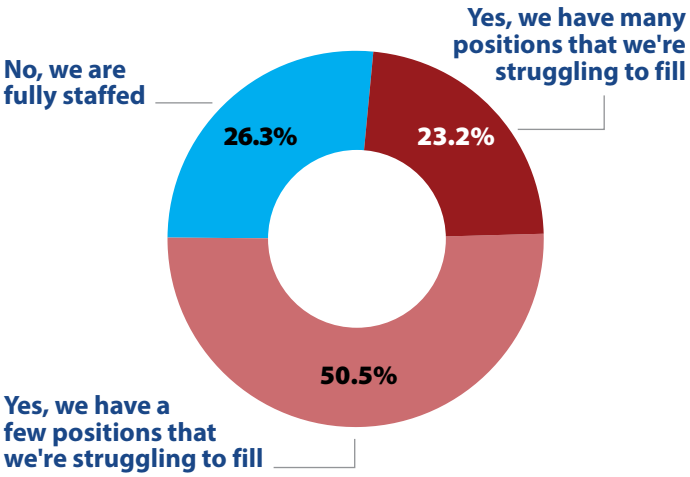


*Figure 11: Percentage of organizations experiencing IT security personnel shortages.*

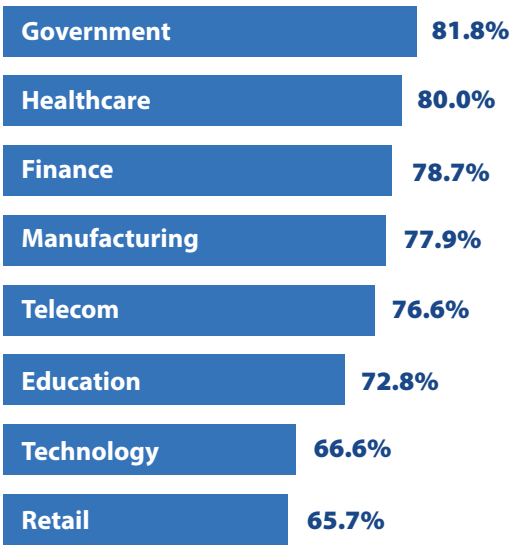


*Figure 12: Percentage of organizations experiencing IT security personnel shortages, by industry.*

We're all aware that the scarcity of talent is a perennial problem in the cybersecurity industry. We wanted to see how broadly this issue was reflected in the survey participant population, so we asked how many respondents were currently experiencing shortages of skilled IT security personnel. More than 73% of respondents are in organizations that are currently struggling to fill at least some positions (see Figure 11).

Staffing shortages are particularly acute in highly regulated industries like financial services, where 78.7% of organizations have unfilled IT security positions, healthcare, where 80% of organizations have unfilled positions, and government, where 81.8% of organizations have unfilled positions (see Figure 12). Severe staffing shortages—in which organizations have many positions that they're struggling to fill—are particularly prevalent in the U.S., impacting 37.5% of respondents there.

If anything, we were surprised to see that 26.3% of survey participants say that their security program was fully staffed. Even so, the need for efficiency improvements that can be gained from implementing technologies like XDR is readily apparent elsewhere in this survey.

**Staffing shortages are particularly acute in highly regulated industries like financial services… healthcare… and government.**

# Section 4: Managed Security Services

## Outsourcing Plans for XDR

**Do you currently outsource monitoring and management of your XDR solution to a managed extended detection and response (MXDR) provider?**

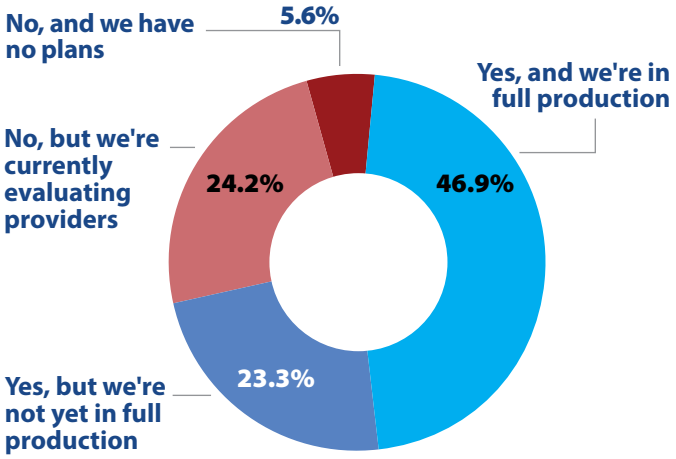


*Figure 13: Current or planned outsourcing of the monitoring and management of an XDR solution.*

Organizations are embracing managed extended detection and response (MXDR) with great gusto. In fact, they're showing nearly as much enthusiasm for MXDR as they're displaying for XDR overall. More than 94% of respondents either have currently outsourced the monitoring and management of their XDR solution to an MXDR provider, are planning to do so, or are evaluating prospective providers.

Organizations in the telecommunications and government sectors are particularly likely to outsource monitoring and management of their XDR solution, with none of the survey participants in these sectors reporting that they don't already do so or have plans to.

Earlier in the survey (see Figure 1), we asked about organizations' adoption or planned adoption of XDR solutions. As you may recall, 48.5% of respondents said that they currently had an XDR solution in production. Above (see Figure 13), you'll see that a majority of these solutions (48.5% of respondents) are being managed.

Similarly, 27.6% of survey participants indicated that they were planning to acquire an XDR solution within the next 12 months (see Figure 1). And 47.5% of respondents are either evaluating MXDR providers or are partway through the process of implementing an MXDR solution (see Figure 13). While these categories cannot be perfectly mapped onto one another, it's clear that the majority of new installs in survey participants' organizations will be managed.

**As you may recall, 48.5% of respondents said that they currently had an XDR solution in production. Above, you'll see that a majority of these solutions are being managed.**

# Section 4: Managed Security Services

## Reasons for Outsourcing

**On a scale of 1 to 5, with 5 being highest, rate the importance of each of the following use cases for outsourcing monitoring and management of an XDR solution to an MXDR provider.**

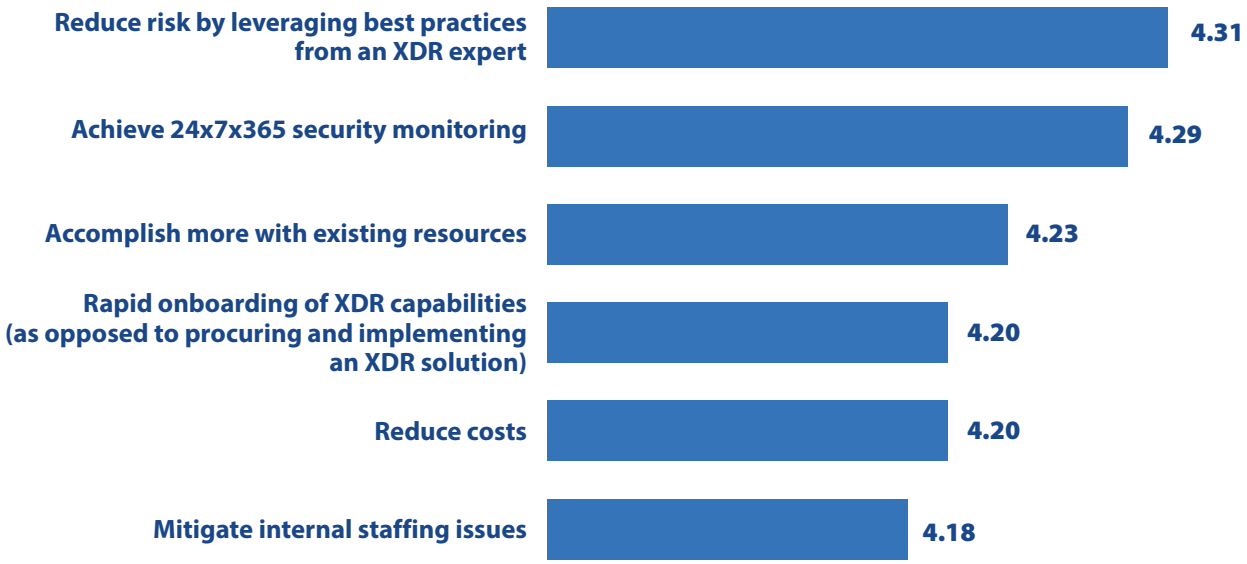


*Figure 14: Most important use cases for outsourcing monitoring and management of an XDR solution.*

We presented survey participants with a list of six common use cases for outsourcing the monitoring and management of an XDR solution to an MXDR provider, asking them to rate each use case in terms of its importance on a five-point scale.

All of the use cases for outsourcing XDR's management were rated similarly (higher than 4.0 and lower than 4.5) on the five-point scale (see Figure 14). And all are viewed by survey participants as important.

The most important reason for outsourcing the management of XDR was reducing risk by leveraging best practices from an XDR expert. This was listed as being of the highest importance (5/5) by 85% of respondents. But even the use case with the lowest importance rating, mitigating internal staffing issues, was still considered important (4/5) or of the highest importance (5/5) by more than 80% of survey participants.

These results make clear that despite the fact that XDR is still an emerging market category, the value of outsourcing to an MXDR provider is already well understood.

# Section 4: Managed Security Services

## MXDR Provider Capabilities

**Which of the following factors are most important when evaluating MXDR providers to monitor and manage an XDR solution?**

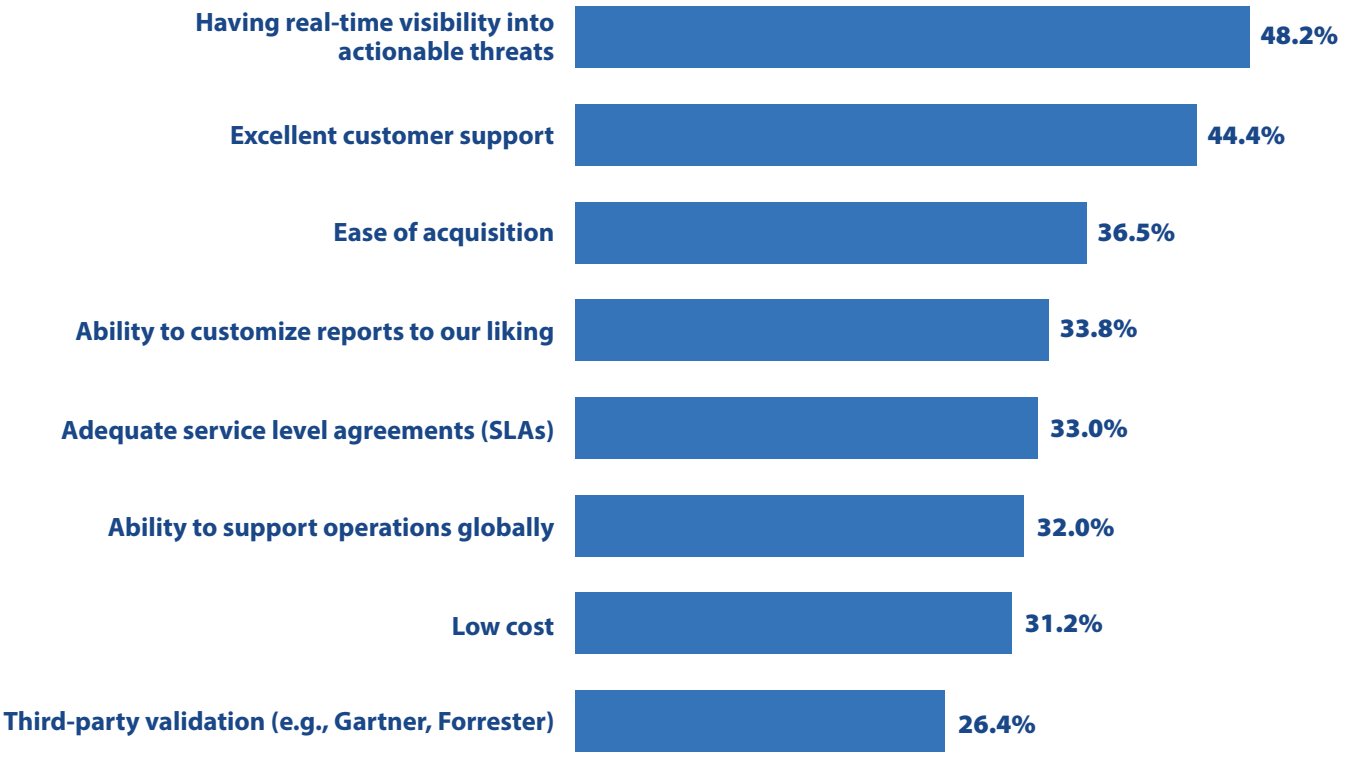


*Figure 15: Most important factors when evaluating MXDR providers.*

We asked survey participants which factors were most important to them when evaluating prospective MXDR providers. Over 48% of respondents indicated that having real-time visibility into actionable threats was among their most important considerations when outsourcing, making this the top-ranked choice.

Similar to what we saw in the responses to our question about XDR solution capabilities (see Figure 3), low cost and third-party validation were less important to survey participants than a solution's accuracy or customer support (see Figure 15).

Nonetheless, most of the factors were ranked as important by approximately one-third of respondents, but none were considered important by more than half. While ease of acquisition was considered important by 36.3% of respondents, low cost was considered important by 31.2%. All in all, this suggests that opinions about what matters most in MXDR are divided. Still, it seems that factors supporting the solution's overall efficacy are paramount.

**Over 48% of respondents indicated that having real-time visibility into actionable threats was among their most important consideration when outsourcing.**

# Conclusion

One thing is readily apparent from our survey: respondents believe that XDR's adoption has the potential to bring significant benefits. Let's summarize some of the most noteworthy ones:

- Reducing operational costs in cybersecurity
- Leveraging automation across the entire security incident lifecycle
- Improving threat detection and response capabilities
- Improving the ability to contextualize and prioritize cyberthreat responses
- Enhancing and centralizing visibility
- Enabling security operations teams to reduce time-to-respond and time-to-remediate for successful attacks

Nonetheless, XDR remains immature as a market category. Survey respondents weren't in agreement about what capabilities should be included in XDR, or which of this technology's use cases were most important to them. A few additional observations:

- Organizations are looking for endpoint detection and response (EDR), network detection and response (NDR), and threat intelligence platform (TIP) capabilities from their XDR ecosystem, particularly when desired native capabilities and integrations are combined.
- Organizations exhibit high levels of confidence that XDR can lower security operational costs and improve efficiencies.
- Most organizations are more concerned about a prospective solution's accuracy and ease of use than about its immediate costs.
- Outsourcing management of XDR to MXDR providers is gaining ground within this market, with a majority of respondents either already outsourcing this function or planning to do so in the future.

So, what can we learn from these insights? To us, the main takeaway is the need for greater clarity among prospective buyers about which critical security functions XDR comprises. Stakeholders should think carefully about which benefits implementing XDR will help their security program to realize, and what strategies will enable them to achieve the fastest time to value as well as the greatest risk reduction. Because XDR can be complicated to implement and manage, outsourcing these functions to an MXDR provider often makes good sense.

Consider the following suggestions as you think about whether an XDR strategy is right for your organization, and if so, how to achieve success with XDR.

### Focus on integrating the most necessary components.

The problem that ever-growing event and alert volumes pose in security operations has long been clear. XDR promises to improve this situation by integrating detection and response capabilities across the entirety of the incident lifecycle and enabling greater use of automation. However, not all vendors are integrating all products and components necessary to deliver comprehensive visibility and orchestration. Many vendors focus primarily on their own products, but without full integration of the right components, you can end up with a set of loosely connected point solutions instead of a comprehensive XDR platform that truly improves your capabilities. The tools that are most important to integrate into comprehensive XDR include the following:

- Endpoint detection and response (EDR)
- Network detection and response (NDR)
- Threat intelligence platform (TIP)
- Security information and event management (SIEM)
- Advanced threat detection and prevention

# Conclusion

### Leverage the expertise of an MXDR provider.

Our survey found that many organizations are engaging MXDR providers to manage their XDR implementations. In fact, a clear majority of new installs among our survey participants will be externally managed. In the face of current staffing shortages in IT security, stakeholders have ample reasons for outsourcing. These include access to expertise, knowledge of best practices, and around-the-clock staffing. Using MXDR may be especially helpful for smaller organizations and less mature security programs, but nearly any organization that's unfamiliar with the complexities involved in implementing and operating an XDR platform can benefit from expert assistance.

Organizations are currently outsourcing XDR's monitoring and management to MXDR providers because doing so enables:

- Access to expertise and best practices
- 24x7x365 security monitoring
- Efficiencies that make it possible to accomplish more with existing resources
- Risk reduction
- Cost consolidation

### Balancing efficiency with efficacy is key.

XDR is an emerging market category, which means there are no universally agreed-upon definitions for what an XDR platform should include. Today's best-available solutions can ingest logs from a broad array of sources, including endpoints, firewalls, Internet of Things (IoT) sensors, and proxies. They're not limited to the telemetries from a single security vendor's product portfolio. And, detections should be correlated with comprehensive and current threat intelligence so that each event's scope and impact can be understood within the context of real-world attack tactics, techniques and procedures (TTP). XDR should also leverage machine learning (ML) and artificial intelligence (AI) to enhance detection accuracy and reduce noise and false positive rates.

Even with ML and AI technologies built into many XDR solutions today, not all offer the range and depth of automation capabilities that are needed to generate true efficiencies. And many organizations will need ongoing and advanced support in order to make full use of these capabilities even when they're available. XDR has great promise to introduce much-needed efficiencies into security operations, but realizing their full value also requires ongoing access to resources and expertise.

# Appendix 1: Demographics

This report is based on survey responses from 400 qualified participants from eight countries (see Figure 16). Each respondent was required to have a role as a leader or practitioner in IT security (see Figure 17). One-third (33%) of respondents held executive positions such as Chief Information Officer (CIO), Chief Information Security Officer (CISO), or VP of IT security operations. More than two-thirds (77%) held management or executive positions.

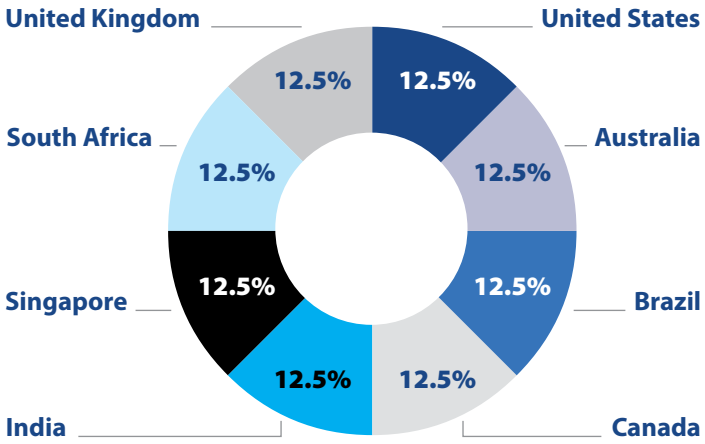


*Figure 16: Survey respondents by country.*

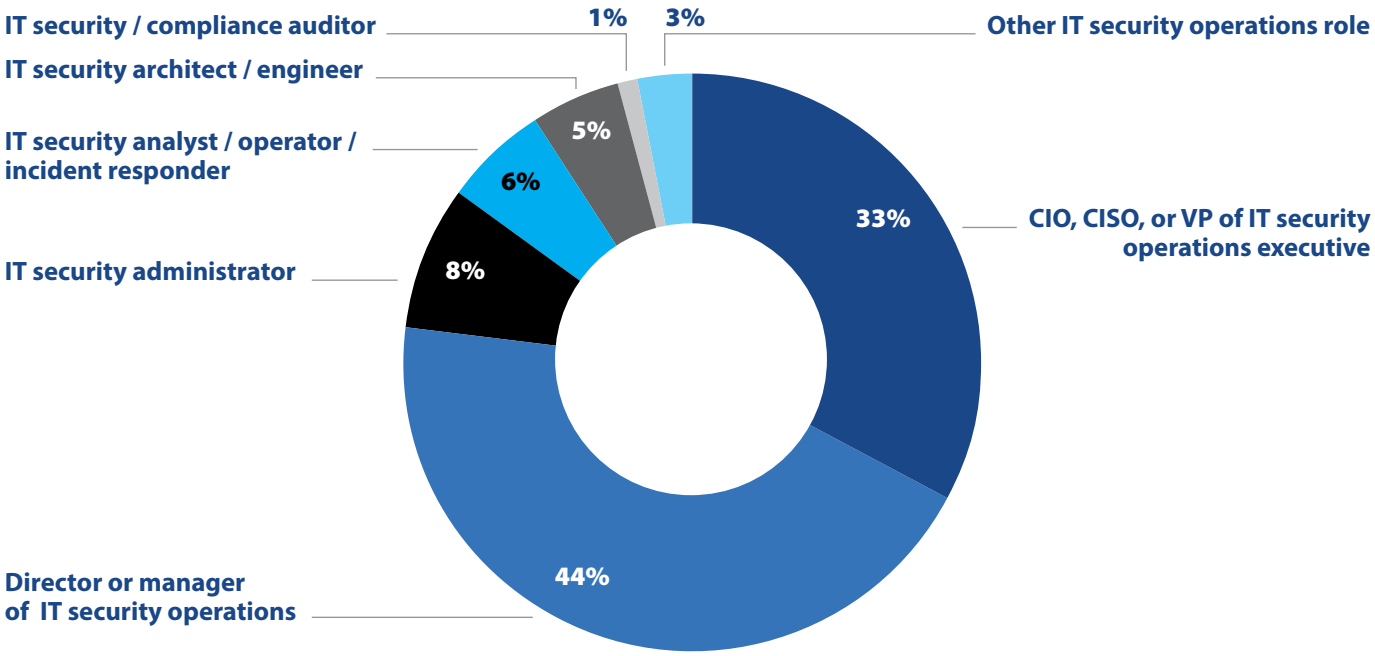


*Figure 17: Survey respondents by IT security operations role.*

# Appendix 1: Demographics

All participants in this survey were working for organizations with 500 or more employees (see Figure 18). They spanned 17 industries (plus "Other") with no single industry composing more than 16% of the total participants. For selected questions, additional analysis was conducted based on the industries with larger numbers of respondents (see Figure 19). Those eight industries—government, telecommunications, retail, finance, manufacturing, education, and healthcare—had almost three-fourths of all participants.

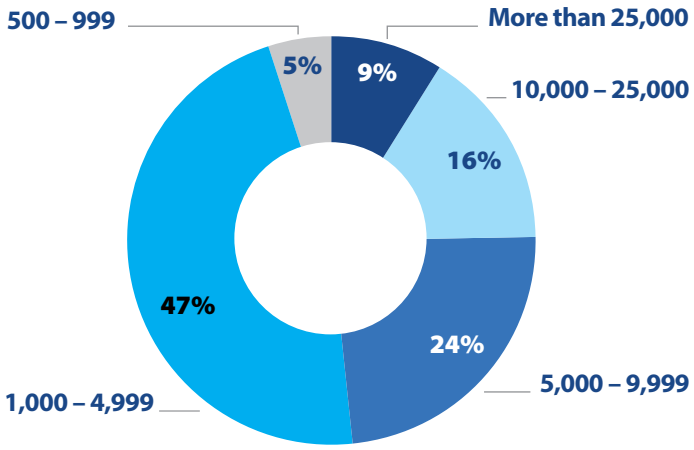


*Figure 18: Survey respondents by organization employee count.*

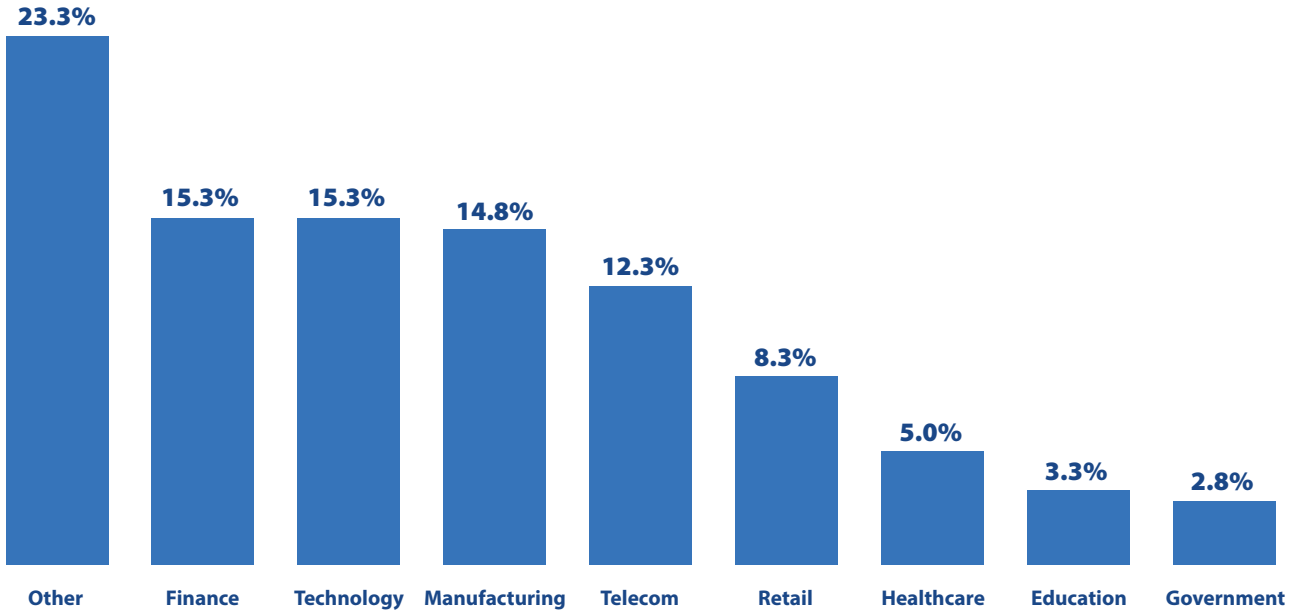


*Figure 19: Survey respondents by industry.*

# Appendix 2: Research Methodology

CyberEdge developed a 15-question web-based survey instrument in partnership with OpenText. The survey was promoted via email to 400 IT security professionals in the United States, Australia, Brazil, Canada, India, Singapore, South Africa and the United Kingdom in March and April 2022. The global survey margin of error for this research study (at a standard 95% confidence level) is 5%. All results pertaining to individual countries and industries should be viewed as "anecdotal" as their sample sizes are much smaller. CyberEdge recommends making actionable decisions based on global data only.

All respondents must meet two filter criteria: (1) they must have an IT security role, and (2) they must be employed by a commercial or government organization with a minimum of 500 global employees.

At CyberEdge, survey data quality is paramount. CyberEdge goes through extraordinary lengths to ensure its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the "right" people are being surveyed by (politely) rejecting respondents that don't meet the respondent filter criteria of the survey (e.g., job role, job seniority, company size, industry)
- Ensuring that disqualified respondents (who do not meet respondent filter requirements) cannot restart the survey (from the same IP address) in an attempt to obtain the survey incentive
- Constructing survey questions in a way to eliminate survey bias and minimize the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the survey questions
- Ensuring that survey respondents view the survey in their native language (e.g., English, German, French, Spanish, Japanese, Chinese)
- Randomizing survey responses when possible to prevent order bias
- Adding "Don't know" (or comparable) responses when possible so respondents aren't forced to guess at questions they don't know the answer to
- Eliminating responses from "speeders" who complete the survey in a fraction of the median completion time
- Eliminating responses from "cheaters" who apply consistent patterns to their responses (e.g., A,A,A,A and A,B,C,D,A,B,C,D)
- Ensuring the online survey is fully tested and easy-to-use on computers, tablets, and smartphones

CyberEdge would like to thank OpenText for making this survey report possible. We'd particularly like to thank Raj Munusamy, Anthony Di Bello, and Alexis Robbins for sharing their experience and expertise in extended detection and response with us.

## Appendix 3: About Our Sponsor

OpenText, The Information Company, enables organizations to gain insight through market-leading information management solutions, on-premises or in the cloud. The OpenText Information Management portfolio offers solutions to master modern work, digitize supply chains, deliver communication-centric experiences, and be cyber resilient.

OpenText Security helps organizations address information protection, cybersecurity, and digital investigation needs with industry-leading solutions. From endpoint detection and response to network security, OpenText provides customers with multi-layered security protection for their most important data. With the highest standards of security and compliance protocol, OpenText security solutions also offer proactive tools for digital forensics, threat intelligence and information assurance. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX), visit opentext.com.

## Appendix 4: About CyberEdge Group

Founded in 2012, CyberEdge is the largest research, marketing, and publishing firm to serve the IT security vendor community. Today, approximately one in six established IT security vendors (with $10 million or more in annual revenue) is a CyberEdge client.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading, CISO Magazine, and others.

CyberEdge has cultivated its reputation for delivering the highest-quality survey reports, analyst reports, white papers, and custom books and eBooks in the IT security industry. To learn more about how we help our IT security vendor clients succeed, connect to our website at www.cyber-edge.com.


## CYBEREDGE GROUP, LLC

1997 ANNAPOLIS EXCHANGE PKWY.
SUITE 300
ANNAPOLIS, MD 21401

800.327.8711

WWW.CYBER-EDGE.COM

INFO@CYBER-EDGE.COM