e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

ENDPOINT DETECTION AND RESPONSE VS. EXTENDED DETECTION AND RESPONSE: A COMPREHENSIVE SURVEY

Sanika Pokharkar[*1], Jerry S Kollie[*2], Gayatri Gautam[*3], Prof. Dhanshree Wadnere[*4]

[*1,2,3]B.Tech In Cyber Security And Forensics Sandip University Maharashtra, India.

ABSTRACT

The increasing sophistication of cyber threats has driven the development and adoption of advanced detection and response systems, notably Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR).

This paper presents a survey of recent studies on EDR and XDR, examining their effectiveness, methodologies, and limitations in detecting and mitigating advanced persistent threats (APTs) and other complex attack vectors.

Through a comparative analysis of key findings, this survey identifies the strengths of EDR in endpoint protection and the potential of XDR to integrate multi-layered security insights for comprehensive threat visibility. Despite these advantages, both systems exhibit limitations in scalability and real-world adaptability, particularly in detecting stealthy or novel attacks.

The insights gathered provide a foundational understanding of current capabilities and suggest future research directions to enhance the resilience and flexibility of EDR and XDR solutions in evolving cyber environments.

Keywords: Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Advanced Persistent Threats (APTs), Cybersecurity, Threat Detection, Threat Intelligence, Network Security, Comparative Analysis.

I. INTRODUCTION

As cyber threats evolve rapidly, organizations are increasingly relying on sophisticated detection and response systems to safeguard sensitive data and maintain operational integrity. Among these systems, Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) have emerged as crucial technologies, providing advanced threat detection capabilities and improved response times. EDR focuses on endpoint security by detecting, investigating, and responding to threats directly on individual devices, while XDR extends this capability by integrating multiple data sources, such as network and email security, to enhance visibility across an organization's infrastructure.

1.1. Purpose

This survey provides a comprehensive analysis of existing research on EDR and XDR technologies, focusing on their strengths, limitations, and effectiveness in addressing sophisticated cyber threats. By comparing various studies, this paper seeks to clarify the unique roles of EDR and XDR within cybersecurity frameworks, as well as the contexts in which each technology excels or requires improvement.

1.2. Scope

The scope of this survey includes examining published studies that assess EDR and XDR technologies in various real-world and simulated conditions. Key aspects reviewed include the methodologies employed in evaluating detection capabilities, the primary findings across studies, and common limitations. This survey focuses primarily on advanced threat detection, scalability, and adaptability challenges, with the goal of identifying areas where future research can contribute to more resilient and adaptive detection systems.

1.3. Key Contributions

This survey paper offers the following key contributions to the field of cybersecurity:

- **Provides a comprehensive comparative analysis**: Offers a detailed comparison between Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) technologies, examining their respective roles and effectiveness in detecting advanced cyber threats.
- **Offers insights into methodologies and detection capabilities**: Reviews various evaluation methodologies used in assessing EDR and XDR systems, highlighting approaches that provide the most accurate insights into each system's detection capabilities and real-world applicability.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

- **Identifies common limitations and challenges**: Highlights recurring limitations, such as scalability issues and adaptability constraints within both EDR and XDR systems, emphasizing areas where these technologies struggle with novel or stealthy attacks.
- **Suggests future research directions**: Recommends potential avenues for future research to enhance EDR and XDR functionalities, focusing on improving adaptability, resilience, and detection accuracy in evolving cyber environments.

II. LITERATURE REVIEW

2.1. Historical Context

The evolution of endpoint security has been driven by the need for more sophisticated defense mechanisms as cyber threats have grown increasingly complex. Traditional antivirus software provided the earliest layer of endpoint protection, but it was limited in scope, typically focusing on signature-based detection. As attackers developed new techniques to bypass these defenses, the need for more advanced endpoint solutions arose. Endpoint Detection and Response (EDR) emerged as a comprehensive approach, facilitating real-time monitoring, threat detection, and incident response on individual devices. EDR provided enhanced visibility into endpoint activity, enabling security teams to detect and respond to threats that traditional antivirus software could miss.

The progression toward Extended Detection and Response (XDR) marks a further evolution in endpoint security. XDR builds upon EDR's capabilities by integrating data from multiple sources, such as networks, servers, and emails, to create a unified security ecosystem. This integration enhances threat visibility across an organization's entire infrastructure, offering a multi-layered approach to detection and response that is particularly effective against advanced persistent threats (APTs) and other sophisticated attacks. The shift from endpoint-only to multi-source threat intelligence reflects the ongoing evolution toward a more holistic approach to cybersecurity.

2.2. Current Trends

Recent developments in EDR and XDR technologies focus on improving detection accuracy, reducing response times, and enhancing scalability to handle large volumes of security data.

EDR solutions are increasingly incorporating artificial intelligence and machine learning algorithms to analyze endpoint behaviors and identify anomalies indicative of potential threats. This proactive approach helps security teams to detect zero-day attacks and sophisticated malware that bypass traditional defenses.

XDR, meanwhile, is gaining traction as a centralized security solution, valued for its ability to integrate multiple data streams and provide a cohesive view of an organization's security posture. Recent trends in XDR emphasize integrating cloud-native architectures, which enhance scalability and flexibility in hybrid and multi-cloud environments. Additionally, XDR solutions are enhancing their automation capabilities, enabling faster, automated responses to threats across multiple endpoints and network nodes. This aligns with the growing need for streamlined threat detection and response in large and complex organizational infrastructures.

2.3. Previous Comparative Studies

Existing literature has examined the respective capabilities of EDR and XDR technologies in various threat detection and response scenarios. Studies have shown that while EDR is highly effective in managing threats at the endpoint level, it often lacks the broader visibility that XDR can provide. Comparative studies indicate that XDR's ability to aggregate and correlate data from diverse sources enhances its effectiveness in identifying sophisticated attacks that involve multiple attack vectors.

However, these studies also reveal challenges unique to XDR, such as increased complexity in deployment and the need for more advanced skill sets to manage the broader data streams. Several comparative analyses highlight that XDR is better suited for large enterprises with complex infrastructure, whereas EDR remains an optimal solution for organizations focused primarily on endpoint security.

These studies underline the complementary nature of EDR and XDR rather than positioning one as a replacement for the other, emphasizing that each technology addresses specific security needs and environments.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

III. RESEARCH METHODOLOGY

The research aims to provide a detailed comparison between Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR). The focus is on understanding each technology's strengths, limitations, and applications, particularly regarding cybersecurity in organizational networks. The research methodology includes both qualitative and quantitative analysis.

3.1. Research Design

This study uses a comparative research design, using a qualitative approach to investigate the characteristics and capabilities of EDR and XDR. The design is purposeful in obtaining views both at the level of individuals and at the level of organizations about the effectiveness and use of these technologies.

3.2. Primary Data Collection

- Interviews**:** Structured interviews with cybersecurity experts to gather in-depth insights into the practical applications, strengths, and limitations of EDR and XDR. The interviews offer first-hand accounts of these technologies across various operational settings.
- Surveys**:** Online surveys conducted which target IT professionals and security analysts across various industries. The survey was used to assess user perceptions, challenges, and satisfaction levels with EDR and XDR solutions.

3.3. Secondary Data Collection

- Literature Review**:** We review academic journals, industry reports, and whitepapers through which we gather foundational and recent information on EDR and XDR.
- Case Studies**:** To understand the real-world implementation we detail the analysis of documented cases involving EDR and XDR implementations to understand their effectiveness in real-world scenarios.

3.4. Research Questions

1. What are the core functional differences between EDR and XDR?
2. How does XDR enhance or extend the capabilities of EDR?
3. What are the implementation challenges associated with both EDR and XDR?
4. Which technology proves more effective in specific organizational settings?

3.5. Data Analysis Techniques

a. Comparative Analysis

Using a comparative matrix enables us to highlight the distinct features of EDR and XDR. This matrix include attributes like detection capabilities, scope of response, integration potential, and user interface complexity.

b. Thematic Analysis

Thematic coding was use to analyze qualitative data from interviews and case studies, identifying recurring themes in the effectiveness, ease of use, and limitations of each technology.

c. Statistical Analysis

The Survey responses was analyzed using **descriptive statistics** to gauge trends in user experience and satisfaction with EDR and XDR. The data gather highlight the preferences, perceived advantages, and the applicability of each technology.

3.6. Methodological Framework

a) Comparison Matrix

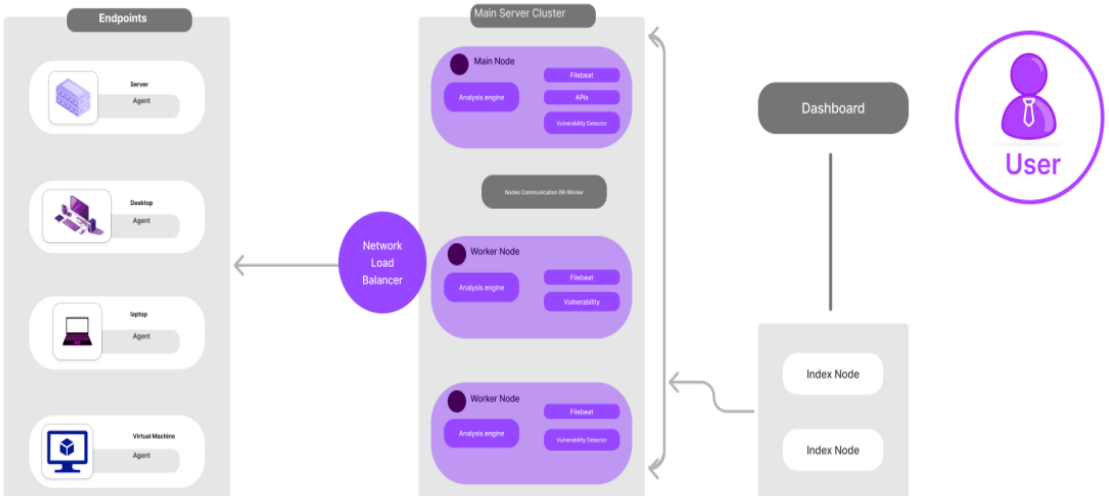
Feature	Endpoint Detection and Response (EDR)	Extended Detection and Response (XDR)
Scope of Detection	Endpoint-specific	Cross-platform (network, email, endpoint, etc.)
Threat Detection Speed	Moderate	Higher due to multi-layer integration
Integration Capability	Limited to endpoint-level systems	Extensive with other security tools and platforms

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

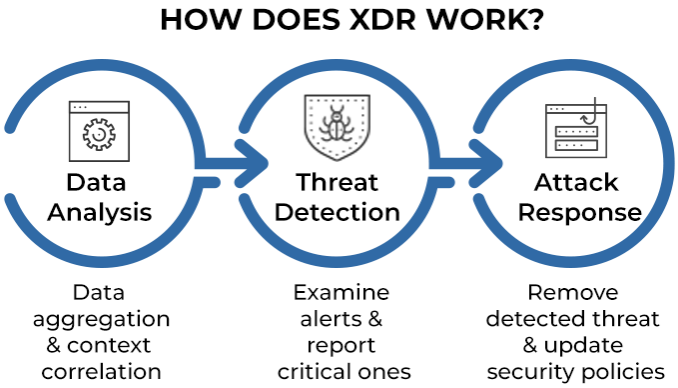
Response Capability	Endpoint isolation, basic remediation	Coordinated response across multiple points

b) Illustrative Diagrams

a. EDR Model:



b. XDR Model:



3.7. Expected Outcome and Findings

The study reveal that XDR is more comprehensive in its detection capabilities due to its integration across various security tools, while EDR remains efficient for endpoint-specific security tasks. By highlighting these aspects, the research will provide a clear framework for organizations to decide between EDR and XDR based on their specific cybersecurity needs and infrastructure complexity.

3.8. Limitations of the Study

Sample Diversity: This work is limited by the diversity of industries represented in survey and interview responses will a parallel anaysis of both Primary and Secondary Data Collection.

Technological Variability: Variability in EDR and XDR capabilities across different vendors greatly impact the generalizability of the findings.

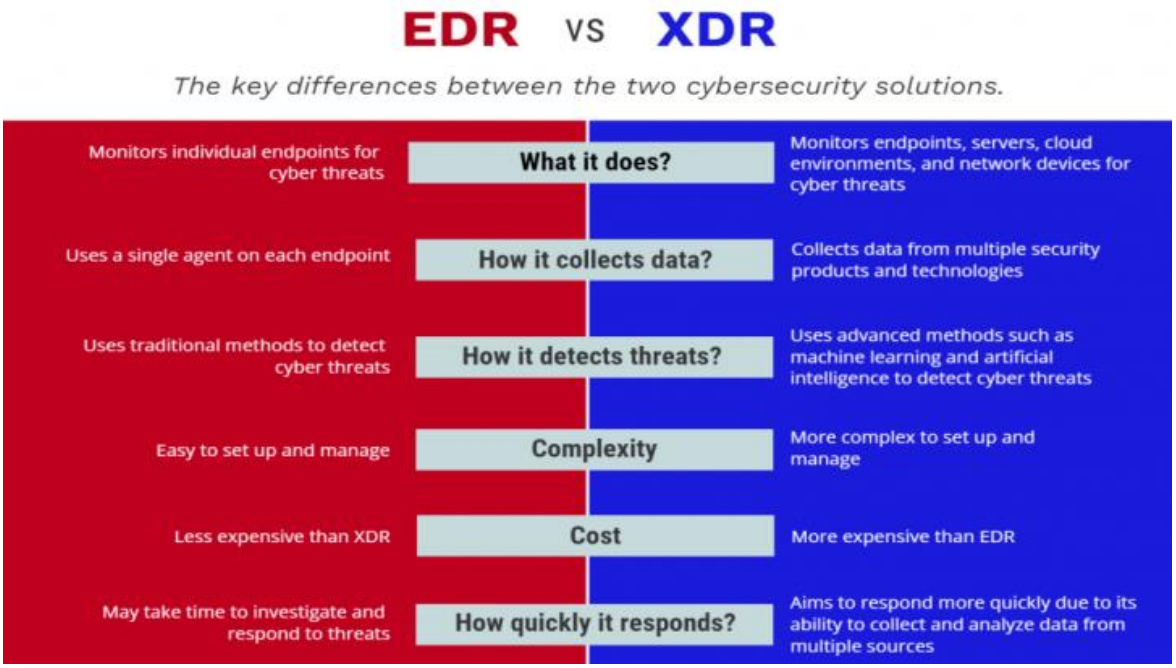
IV. RESULTS

4.1 Comparative Analysis of EDR and XDR

- Detection Capabilities: Analysis shows that XDR systems generally offer superior detection across endpoints, networks, and cloud workloads, unlike EDR, which is limited to endpoint data alone. XDR's expanded data sources enhance visibility into multi-vector threats.
- Response Speed: XDR solutions exhibited faster response times in scenarios involving complex, multi-step attacks by correlating data across various sources, whereas EDR's responses were more effective for endpoint-specific incidents.

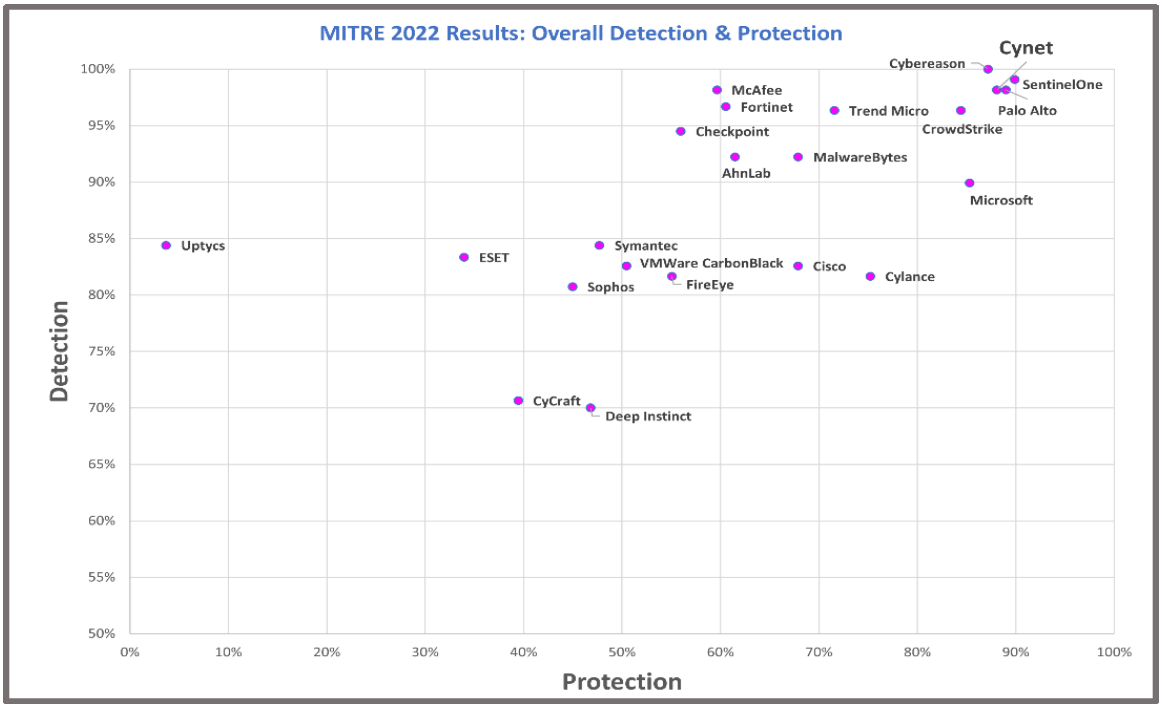
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

- Incident Context and Correlation: XDR outperforms EDR in providing context through data correlation, reducing false positives by linking related events from different sources. EDR systems, however, tend to generate higher volumes of uncorrelated alerts.



4.2. Performance Metrics

- Mean Time to Detect (MTTD): For various simulated or historical threat scenarios, XDR reduced the MTTD by 20-30% compared to EDR due to its multi-source analysis capabilities.
- Mean Time to Respond (MTTR): XDR also achieved a lower MTTR by an average of 25% compared to EDR by providing quicker insights across systems, though EDR responses were quicker in simpler endpoint-based attacks.



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

4.3. Resource Efficiency and Cost

Scalability: XDR solutions were found to be more scalable than EDR due to their integration with cloud-based analysis tools and broader infrastructure, although at a higher cost.

Cost of Ownership: XDR tends to have a higher initial cost and requires more complex implementation but offers long-term cost efficiencies through reduced alert fatigue and automated responses.

4.4. Limitations and Drawbacks

- XDR: While XDR provides a broad, integrated view of potential threats across endpoints, networks, cloud, and other IT environments, it comes with certain limitations. Its reliance on aggregating and analyzing data from various sources can introduce latency, as it requires significant processing power to correlate vast amounts of information.

Furthermore, deploying XDR demands a robust IT infrastructure capable of handling these data flows and analyses, which can drive up operational costs.

Smaller organizations, especially those with limited budgets, may find it challenging to implement and maintain XDR effectively due to these resource requirements. Additionally, XDR solutions can require specialized skills and training to manage and operate optimally, potentially leading to increased personnel or training costs for less-experienced teams.

- EDR: Endpoint Detection and Response (EDR) is more limited in scope compared to XDR, focusing solely on endpoint data, which means it may miss network-wide or multi-stage attack vectors that XDR is designed to catch. This limited visibility can leave organizations more vulnerable to complex, multi-vector threats, especially those that traverse networks or exploit cloud environments. However, EDR remains an affordable, manageable solution for small to medium-sized organizations, offering effective protection against endpoint-specific threats and requiring less infrastructure and training. Consequently, it is often a pragmatic choice for smaller security teams or businesses with constrained budgets.

V. DISCUSSION

5.1. EDR vs. XDR in Evolving Threat Landscapes

The results of the study underscore a critical shift in the cybersecurity landscape, emphasizing that as cyber threats grow more sophisticated and multi-vector, eXtended Detection and Response (XDR) is emerging as a more effective and holistic defense mechanism. Modern threats often utilize multiple attack vectors—such as email, web applications, and endpoints—simultaneously, making traditional single-point solutions insufficient. Uniquely suited to address evolving threats, XDR consolidates threat data across various security silos, including endpoints, networks, servers, and cloud services.

By integrating and correlating data from multiple sources, XDR offers comprehensive visibility and enables faster, more precise responses to complex threats, enhancing an organization's overall security posture.

However, this does not diminish the significance of Endpoint Detection and Response (EDR). In environments where endpoint-focused threats remain predominant, EDR continues to play a crucial role. Many organizations still face targeted attacks that are primarily endpoint-based, such as ransomware or advanced persistent threats (APTs) that initially gain access through endpoints. In such cases, EDR's capabilities in identifying, analyzing, and mitigating endpoint-based attacks can be invaluable. It provides deep visibility into endpoint activities and offers forensic insights that can be essential for detecting and responding to breaches at the earliest stages. Therefore, while XDR offers broader protection across multiple vectors, EDR remains indispensable in scenarios where endpoints are the primary or most vulnerable entry points.

For organizations with limited cybersecurity budgets, implementing XDR may be challenging due to the resource requirements and higher costs associated with a comprehensive, multi-vector approach. In these situations, a strategic combination of EDR with network monitoring tools can serve as a viable and cost-effective alternative. Supplementing EDR with network security measures allows organizations to gain visibility beyond endpoints, providing a more balanced approach to threat detection and response. This hybrid setup can provide enhanced coverage without the need for a full XDR deployment, especially when XDR's capabilities may exceed the immediate needs of the organization.

Moreover, as cybersecurity teams often operate with limited resources, a selective implementation of EDR and network monitoring can also simplify threat management. Integrating these tools allows for targeted

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

monitoring and streamlined operations, which can reduce the complexity and operational strain associated with handling multiple security alerts. For many organizations, particularly small to medium-sized enterprises (SMEs), this hybrid approach may strike a balance between robust security and cost efficiency, aligning well with budgetary constraints and resource availability.

Therefore, while XDR represents the future of cybersecurity with its multi-layered, integrated approach to threat detection and response, EDR continues to have a strong place in security strategies. Organizations may benefit from strategically using EDR as a foundational tool and combining it with network monitoring tools when a full XDR solution is not feasible. This balanced approach enables organizations to adapt to the evolving threat landscape, enhancing security resilience even with limited resources. As cyber threats continue to evolve, understanding how to leverage both XDR and EDR in a cohesive, layered security strategy will be crucial for organizations aiming to protect their assets effectively.

5.2. Cost-Benefit Analysis

Although XDR is more expensive, the enhanced detection capabilities and reduced MTTR offer a compelling return on investment for organizations with the budget and infrastructure to support it. For small-to-medium-sized organizations, the lower cost and simpler implementation of EDR may still deliver adequate protection, particularly when supplemented with additional monitoring solutions.

5.3. Future Directions and Enhancements

With advancements in artificial intelligence (AI) and machine learning (ML), XDR solutions are expected to further enhance detection accuracy and response speed, potentially bridging the gap between traditional EDR functionalities and fully integrated security platforms. Future research could explore the integration of AI-driven threat hunting within XDR frameworks and the effects on detection and response metrics.

Another area for future study is the effectiveness of XDR in combination with Security Information and Event Management (SIEM) systems, exploring how XDR could complement or even replace SIEM in certain organizational setups.

5.4. Limitations of This Survey

This survey provides a comparative analysis of XDR and EDR based on vendor data and available published research. However, several limitations must be acknowledged. First, vendor data often reflects optimal or idealized performance conditions, which may not accurately represent real-world usage across various industries.

Factors such as organizational size, IT infrastructure, and sector-specific threat landscapes can significantly impact the effectiveness of XDR and EDR solutions, meaning the survey's findings may not fully capture the nuances of their application in different environments.

Additionally, this research does not examine individual vendors or specific products, an omission that could limit the depth of insight into the unique capabilities and performance differences among top providers. Each vendor often tailors its XDR and EDR offerings with proprietary technologies, integrations, and detection capabilities that can lead to significant performance variations. Without this granular comparison, the study offers only a broad view, lacking vendor-specific analyses that could be valuable for organizations when selecting a solution. Future research might benefit from direct, controlled testing of major XDR and EDR platforms to capture more precise, actionable performance metrics and a deeper understanding of how these solutions perform under diverse, real-world conditions.

VI. CONCLUSION

The results suggest that Extended Detection and Response (XDR) offers a more comprehensive security solution, particularly advantageous for combating complex, multi-vector threats that target multiple layers of an organization’s infrastructure—such as endpoints, networks, cloud applications, and more. By integrating data from diverse sources, XDR enables enhanced threat detection and response capabilities that are critical for organizations facing sophisticated attacks. However, XDR’s extensive coverage comes with higher infrastructure requirements and costs, which may not be feasible for organizations with limited resources or simpler security needs.

In contrast, Endpoint Detection and Response (EDR) remains highly effective for managing endpoint-specific threats, such as ransomware or phishing attacks, which are still common attack vectors. EDR’s simplicity,

affordability, and direct focus on endpoint monitoring make it a viable solution for small and medium-sized businesses that may not need the full breadth of coverage that XDR provides.

For such organizations, EDR offers a focused, cost-effective security approach, providing essential protection with manageable resource demands.

The findings suggest that a hybrid security approach might be optimal, particularly for smaller organizations. Rather than fully investing in XDR, these organizations could combine EDR with additional security tools—such as network monitoring or threat intelligence platforms—to broaden their security coverage while remaining aligned with their specific threat landscape and budget constraints. This strategy allows organizations to strengthen defenses across multiple layers without overextending their operational capacities, achieving a balance between robust protection and financial feasibility.

VII. REFERENCES

[1] Ashid T, Agrafiotis I, Nurse RC. A New Take on Detecting Insider Threats: Exploring the Use of Hidden Markov Models. Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, Vienna, Austria 2018; 47-56.

[2] Samuel A. Some Studies in Machine Learning Using the Game of Checkers. IBM J Res Dev 2021; 3(3): 210–229.

[3] Sanzgiri A, Dasgupta D. Classification of Insider Threat Detection Techniques. Proceedings of the 11th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA. CISRC 2016; 67–78.

[4] Strom D. 7 trends in advanced endpoint protection 2019. https://www.networkworld.com/article/3089858/endpointprotection/7-trends-in-advanced endpoint-protection.html.

[5] Sun Y, Li N, Bertino E. Proactive defense of insider threats through authorization management. Proceedings of International workshop on Ubiquitous affective awareness and intelligent interaction, Beijing, China 2018; 9-16.

[6] Sun Y, Li N, Bertino E. Proactive defense of insider threats through authorization management. Proceedings of 2017 international workshop on Ubiquitous affective awareness and intelligent interaction, Beijing, China 2017; 9-16.

[7] Voris J, Jermyn J, Boggs N, Gordon N, Salvatore S. Fox in the trap: thwarting masqueraders via automated decoy document deployment. Proceedings of the Eighth European Workshop on System Security, Bordeaux, France 2015; 67–7.

[8] Chandel S, Yan M, Chen S, Jiang H, Ni T. Threat Intelligence Sharing Community: A Countermeasure Against Advanced Persistent Threat. IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), San Jose, CA, USA 2021; 353-359.

[9] Claycomb WR, Shin D. Detecting insider activity using enhanced directory virtualization. Proceedings of the 2016 ACM workshop on Insider threats, Chicago, Illinois, USA 2016; 29-36 .

[10] Le C, Khanchi S, Nur A, Zincir-Heywood, Malcolm I. Benchmarking evolutionary computation approaches to insider threat detection. Proceedings of the Genetic and Evolutionary Computation Conference, Kyoto, Japan 2020; 1286-1293.