International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

A Survey on Endpoint Detection and Response Systems

Rekha Saraswat[1], Mo Kareem[2], Dr. Mary Jacintha M[3]

[1] Scientist E, Education & Training Department, CDAC Noida, Noida, India
[2] Project Engineer, Education & Training Department, CDAC Noida, Noida, India
[3] Scientist F, Education & Training Department, CDAC Noida, Noida, India

Abstract
Cybersecurity threats have become increasingly sophisticated and frequent, posturing significant risks to organizational data, infrastructure, and operational continuity. As enterprises increasingly depend on interconnected digital systems and endpoint devices, continuous monitoring and timely detection of cyber threats have become essential to ensure organizational security. In order to ensure the security of organizational data, the deployment of advanced security solutions is necessary to enhance endpoint visibility and enable effective detection and response to cyber threats. End Point Detection & Response (EDR) systems play an important role in monitoring or tracking end points such as workstations, laptops, servers, or even mobile phones and analysing the data associated with them with the intent or aim to identify or analyse potential cyber security threats. These systems are also capable of collective cybersecurity monitoring of the enterprise. This research work aims to analyse the efficiency of existing EDR systems in monitoring or analysing cyber incidents in real time.

Keywords: EDR, Cyber Security, Endpoint Security, Malware Detection, Cyber Security, Data Security

1. Introduction

The nature of cybersecurity risks is shifting in the modern threat environment, becoming more complex and targeting not only the organizational infrastructure but also the endpoints such as server, laptops, desktops, and mobile computing devices that it relies on. As the end point devices provide the primary gateway into the organizational networks, these devices are primary targets for the malicious actors and therefore there has been a rising need for Endpoint Detection and Response Technologies.

The proposed study will help address this gap inasmuch as it will conduct a live performance evaluation of the most popular EDR tools on a cyber simulation. This study will not only focus on theoretical evaluation, where opinions about EDR tools are sought, but will put these tools to the test for various simulated cyber-attacks and thus help generate actionable intelligence about what the individual tool can and cannot do.

The end objective is thus the provision of actionable insights that can be utilized by the cybersecurity practitioner by making them aware of the pros and cons of existing EDR technology and the manner in which they should be guided in the optimization of the detection method and the process of incident response.

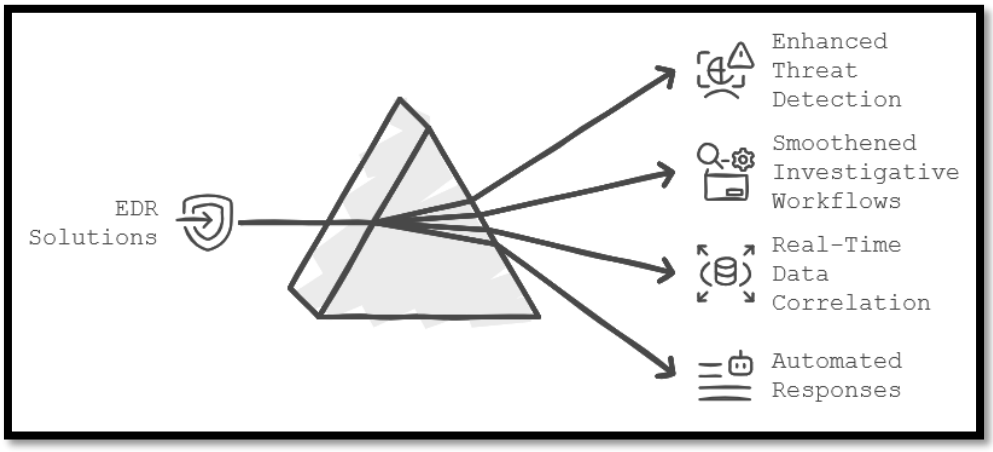

Figure 1. Architecture of EDR

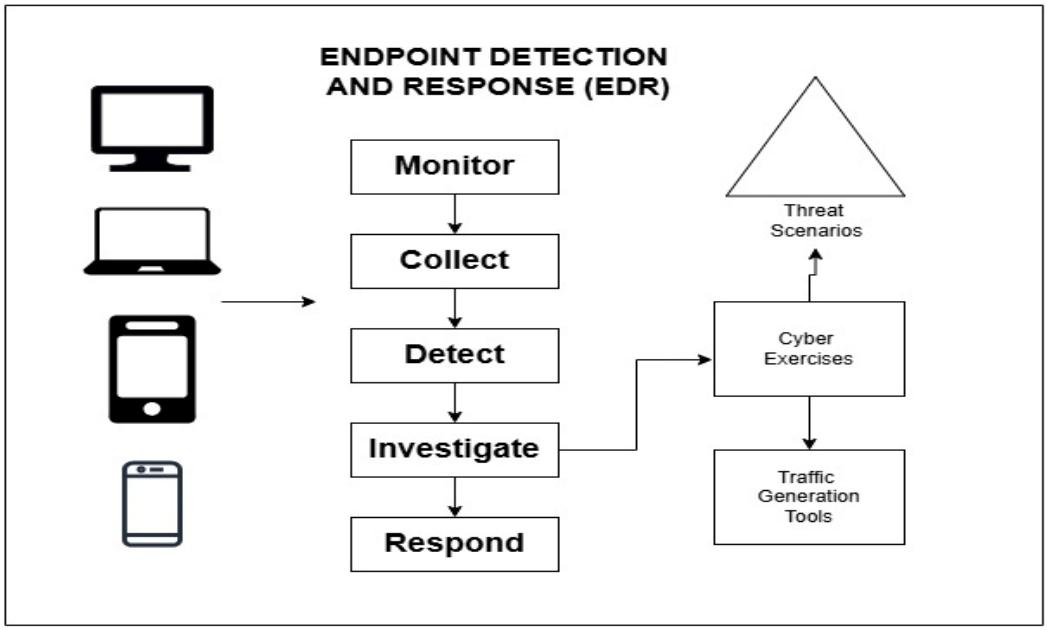

Figure 2. Functionality of EDR Systems

2. Literature Survey

The work done by **Asad Arfeen** & **Saad Ahmad** mentions that the growth in cyberattacks and inability of traditional security solutions such as firewalls, antivirus solutions, in detecting the advanced threats have driven endpoint protection methods to advance noticeably, a fact established through numerous studies. The traditional security solutions, are no longer sufficient against complex attacks that could bypass signature-based detection. To plug this security hole, researchers and cybersecurity experts have developed technologies called Endpoint Detection and Response systems. EDR solutions are able to merge endpoint visibility with network data analysis to enhance threat detection and smoothen investigative workflows, hence making EDR an important building block of modern cybersecurity ecosystems by offering real-time data correlation and automated responses. However, like all other human made solutions, current EDR solutions are not spared from limitations: though effective on the endpoint level, they are found ineffectual in the case of threats which can propagate through an environment made up of complex cloud infrastructure and mobile devices. This limitation gave birth to Extended Detection and Response, which integrates endpoint, network, email, and cloud security data onto one platform. This

literature study on the EDR system is an essential element of modern cybersecurity and works as a base for more comprehensive models, for example the XDR model, which helps to monitor and mitigate threats continuously. **[1]**

The work done by **Harpreet Kaur** and **Dharani Sanjaiy SL** highlights that, with the increasing complexity of cyber-attacks on endpoint devices, a tremendous amount of research has been conducted on Endpoint Detection and Response (EDR). While current research is centered on the integration of the use of machine learning (ML), behavior analysis, and AI, more emphasis in the earlier research had been on relatively more conventional approaches such as signature recognition and heuristic analysis in threat identification and deletion. The limitations associated with conventional security strategies and the need for proactive threat hunting and real-time visibility had also been stressed by researchers. While certain concerns exist with regard to false positives and model drift, research on the use of AI & ML in contemporary EDR solutions has also been thoroughly studied, reflecting enhanced efficiency in the area of anomaly or threat identification. The literature reveals a number of critical parameters related to contemporary EDR solutions including t**elemetry data acquisition and endpoint monitoring, integration of threat intelligence, forensic investigation support and** t**hreat hunting by behavioral indicators.**

Further developments including Extended Detection and Response (XDR) systems and image-based malware detectors are fore fronting a more converged strategy. In the broad scope of literature, innovation in EDR solutions continues to be supported in order to counter advanced cyber threats. **[2]**

The research done by **George Karantzas** and **Constantinos Patsakis** finds that testing the effectiveness of EDR solutions in real-world scenarios. This paper is also intended to understand EDR solutions and their mechanisms in malware detection and alert generation, and their use in analysis of incidents. This paper compares different EDR solutions that are presently being used in the market, on the basis of their detection and response capabilities and their performance effect. Some Key Findings from the Paper.

- **EDR Solution Effectiveness:** EDR tools detected threats that normal antivirus products failed to discover.
- **Operational Load:** Some EDR platforms significantly impacted endpoint performance, highlighting a trade-off between security and usability.
- **Alert Quality:** The study found notable differences in false positive rates between EDR vendors, stressing the importance of tuning configurations.
- **Human Factor:** Skilled analysts were essential for effective incident response, even with advanced automation in place.

As it was found from the previous works in the area of cybersecurity, common methods of cybersecurity protection, such as an antivirus, firewalls, and intrusion detection systems, cannot be effectual in the matter of APT attack security. In this way, the breach of the mentioned defects led to the birth of the EDR solution for security protection. As presented from previous research work, EDR helps in gaining telemetry analysis, facilitating forensic analysis, and conducting proactive hunting missions of threats. Automation and machine learning have also been applied to enhance accuracy levels and swift up response actions.

However, research work also reveals challenges in operational processes posed by extremely high alert levels, chances of falsities, and the need for experienced analysts to interpret complex results. **[3].**

The research done by **Fagbohunmi Grifin Siji** and **Okafor Patrick Uche** mentions that insider threat detection and response in endpoint security encompass designing new algorithms, such as GP algorithms, mathematical models, machine learning, user behavior analytics, and decoy files, mainly to detect insider threats. Other studies have proposed virtualization techniques and models for classification to detects such insider threats. Few discussed the type of threats and mitigation tools. Key gaps identified:

- Many solutions require specialized, expensive software, which small and medium organizations can seldom afford.
- Some approaches do not give explanation regarding the application scenarios or capture the emerging insider threats.
- Previous surveys described tools but did not compare the relative performance.

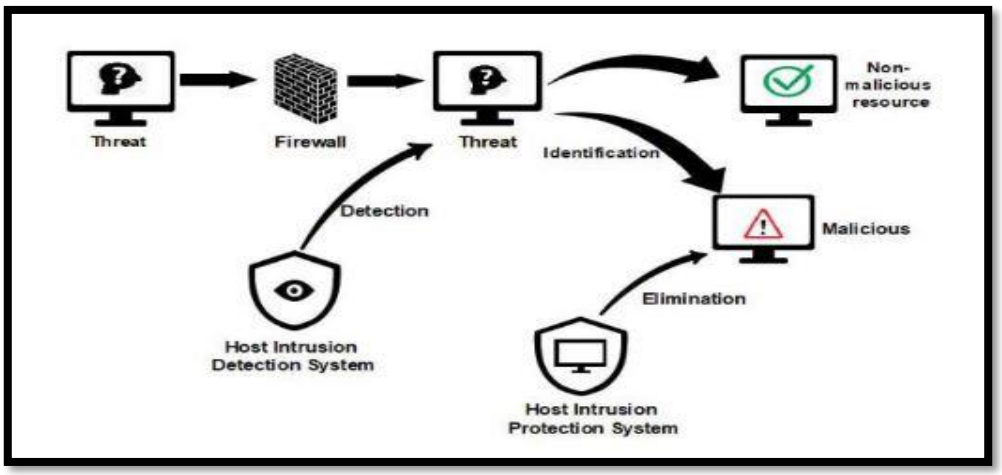

Figure 3. Procedure on threat detection by EPP [4]

This paper therefore presents an advanced model in assessing the benefits and shortcomings of EPP and EDR. This gap gave rise to the current study that compares Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) to determine their advantages, disadvantages, and suitability for different organizational needs. **[4]**

The research done by **Shripad Sunil Chaudhari** and **Sagar Santosh Pradhan** mentions that the history of endpoint security explains how traditional firewall and antivirus software utilize signature-based detection methods, which are only effective against known threats and incapable of encountering more complex threats such as file-less malware attacks and zero-day vulnerabilities. According to researchers Anselmi et al. (2018) and Smith (2017), this limitation led to the development of Endpoint Detection and Response (EDR) and behavior-based detections. There are three main tasks in the area of threat detection, incident investigation, and response EDR tasks, according to Gartner (2019). Researches (Bhatia & Kumar, 2020) mentioned that the use of EDR technology improves the effectiveness of the security process by minimizing the Mean Times to Detect (MTTD) and Respond (MTTR) to the attack. An

important consideration in EDR technology is the application of Machine Learning and Artificial Intelligence to the system; the models are trained to monitor unusual system calls and Advance Persistent Threats, according to Rani et al. (2021) and Krishnamurthy & Patel (2020). However, the challenges in EDR include false positives, the process being resource-consuming in small companies, privacy concerns regarding the data life cycle management, and the capacity to work well within other available systems, including SIEM systems.

Another important area of this current literature is the combination of machine learning (ML) and AI. These engines, trained on "Normal vs. Abnormal" and corpora containing "Normal vs. Abnormal," are able to discover subtle anomalies that are overlooked by signature engines and significantly improve the detection of zero-day and fileless malware. This literature also refers to adaptive approaches that "learn from new patterns of attacks and adapt themselves according to the evolving nature of attackers." **[5]**

The work done by **Mohammed Mujtaba** and **Aseel A. Omair** recommends the use of Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) solutions in contemporary cybersecurity. Endpoint monitoring, behaviour analysis, anomaly identification, and response are primarily covered under EDR, while XDR does the same by combining multiple sources such as endpoints, networks, emails, clouds, and servers. AI/ML analytics, endpoint software, and continuous data flow are employed by these solutions to detect anomalies and respond quickly. Existing studies mentioned in the paper indicate that such tools improve visibility, detection efficacy, and response effectiveness, especially when dealing with fileless malware, insider attacks, and Advanced Persistent Threats (APTs) attacks. Importance is also accorded, according to the literature, to their integration with SIEM and threat intelligence platforms, dependency on KPI metrics such as mean time to detect and respond, and objectives of continuous monitoring that are reviewed. Best practices emphasize defining security strategies, risk assessments, and EDR/XDR integration with compliance obligations. **[6]**

The work done by **Zainuddin Bin Yusof** mentions that modern threats have evolved to bypass traditional antivirus tools. In such a scenario, EDR solutions will bridge this gap by offering continuous monitoring, behavioral analysis, machine learning-based detection, automated response, and forensic support. They are designed to integrate with SIEM and threat intelligence for quicker detection and enhanced incident response. But EDR involves resource-intensiveness, false positives, and skilled staff, hence the challenge of integration. The paper derives the idea that future improvement should rest on AI/ML for enhancing accuracy, reducing false alerts, and combating threats in an evolved manner. **[7]**

The work done by **Harmionee Kaur** and **Richa Tiwari** mentions that Endpoint security in particular has seen the advent of a huge number of Internet of Things devices and also Bring Your Own Devices environments that have enlarged the surface of attacks.

It also analyses the currently available machine learning algorithms-based intrusion detection systems like DIDS, USTAT, STL, MINDS, Haystack, NetSTAT, DT-SVM, GA-IDS.

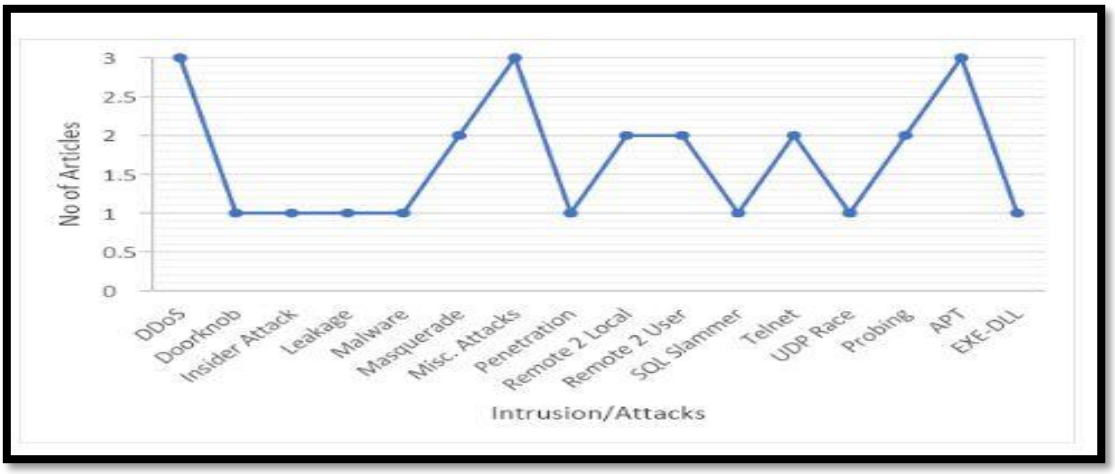

Figure 4. IoT threat compared to the number of publications in this study that offer corresponding solutions. [8]

The paper highlights that the EDR solutions based on ML are capable of combating threats such as malware, ransomware, port scanning, authentication attacks, and APT, which are difficult for conventional solutions to effectively counter. At the same time, the paper highlights the issues arising from intelligent malware and human security elements and explains that the AI/ML-based solutions are capable of increasing accuracy and automation rates**. [8]**

The work done by **Sanika Pokharkar** and **Jerry S. Kolie** mentions that Endpoint Detection and Response (EDR) and more recently Extended Detection and Response (XDR) represent the next step in security solutions from traditional antivirus. As traditional antivirus software relied solely on signature-based detection, it was prone to sophisticated and crafty attacks. Today, businesses gain better visibility into their endpoints due to real-time endpoint visibility, threats, and response offered by EDR solutions, but EDR solutions are endpoint-focused solutions, which are somewhat narrow in scope.
The findings indicate that XDR complements the functionality of EDR by enabling the integration of information coming from various sources such as networks, servers, cloud, and emails to provide a comprehensive multi-layered defensive platform. The recent trends in research work emphasize the application of AI/ML technologies in the realm of EDR & XDR solutions to make anomaly detection, scalability, and response times more efficient.

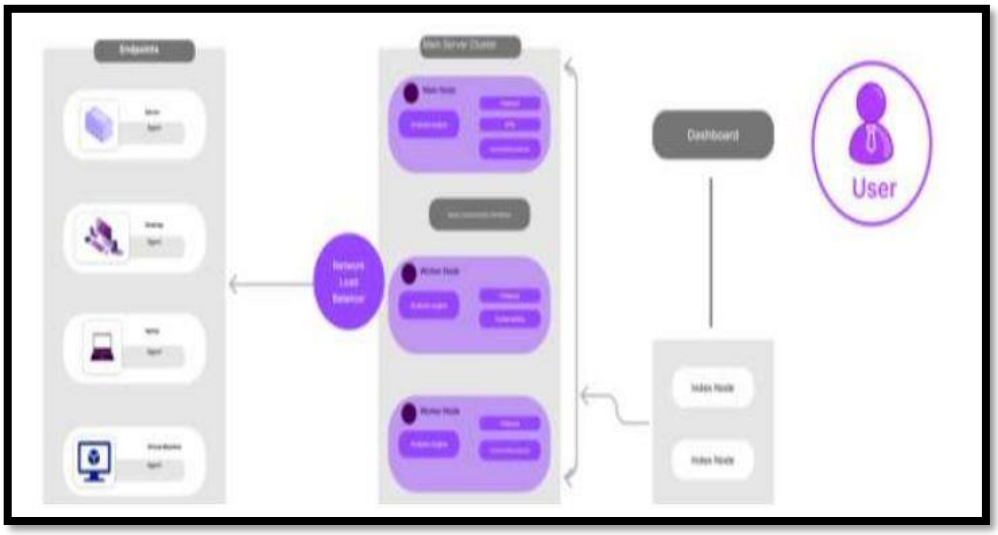

Figure 5. EDR Model (How Does EDR Work). [9]

However, XDR is more complex to deploy, resource-intensive, and costly, making it better suited for larger enterprises, while EDR remains a practical choice for smaller organizations. **[9].**

Zegar Pradipta Putra and **Ruki Harwahyu** mention in their research work that most traditional antivirus software relies on signature-based detection, which makes it ineffective against APTs. In contrast, commercial EDR solutions are more efficient but are often expensive and closed-source. Previous work considered both the cases of commercial and open-source EDR are like Google Rapid Response and OSquery and discussed enhancements such as Tactical Graph Provenance that reduces false positives.

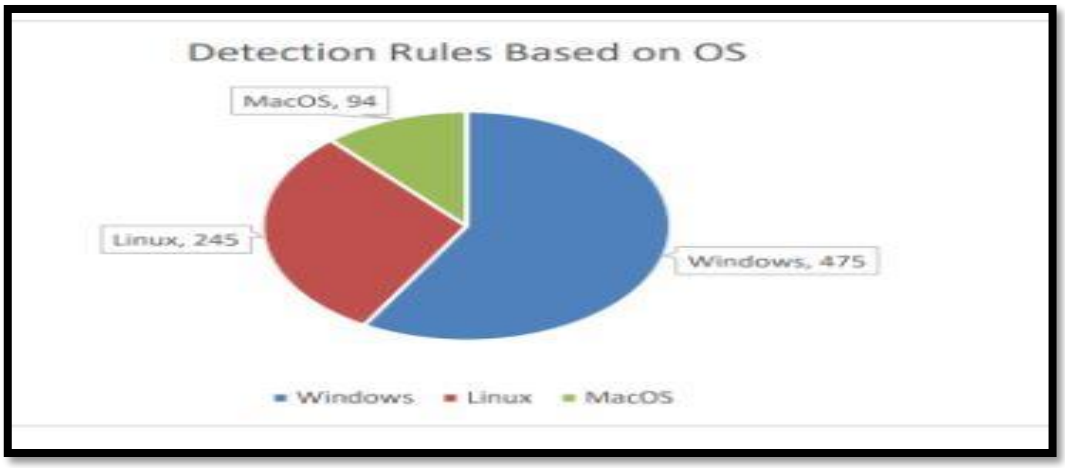

Figure 6. Detection Rules Based on OS. [10]

Threat hunting with the Elastic Stack was also done by some researchers, but more as a SIEM than as a dedicated EDR. Given this, the paper identifies this gap and focuses on evaluating Elastic Security as an open-source EDR. It tests its effectiveness against simulated APT scenarios in order to measure its efficiency, strengths, and limitations in terms of detection. **[10]**

3. Comparative Analysis

The above stated research works propose a number of effective and distinct endpoint detection and response solutions that complement each other appropriately. Yet, every proposed method has its pros and cons. The below stated table analyses that research works based on their pros and cons.

S. N.	Paper Title	Author	Strengths	Weaknesses
1	Endpoint Detection & Response: A Malware Identification Solution	A. Arfeen, S. Ahmed, M. A. Khan and S. F. A. Jafri,	The paper reviews EDR systems in depth, discusses their alignment with established security frameworks, and focuses on real-time monitoring, threat detection, and automation. It sets out quite well the benefits of EDR in relation to increased visibility and speedier reaction times.	It lacks experimental validation and lacks real implementation and practical examples and case studies. It also lacks discussion on practical difficulties and costs involved in implementing the system.
2	Evolution of Endpoint Detection and Response (EDR) in Cyber Security	Kaur, H., SL, D.S., Paul, T., Thakur, R.K., Reddy, K.V.K., Mahato, J. and Naveen, K.,	EDR solutions have numerous advantages, such as real-time monitoring, sophisticated threat analysis done using AI, machine learning, and hunting, along with forensic analysis capabilities. EDR solutions help contain and mitigate cyber threats very effectively.	EDR also has several weaknesses that include high false positives, a limited context of understanding for ML based techniques, a threat of attacks by adversaries, and a high need for computational resources.
3	An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors	Karantzas, G. and Patsakis, C.,	EDR solutions specialize in real-time monitoring, sophisticated detection by behavioral analysis and machine learning algorithms, forensic examination assistance, proactive threat hunting, and threat intelligence to improve their accuracy	However, their drawbacks include their high alert volume, high resource consumption, reliance on highly skilled analysts, high production of false positives, and integration difficulties with other security solutions.
4	An improved model for comparing different endpoint	Siji, F.G. and Uche, O.P.	This paper highlights the threats posed by insiders and a comparison between EPP and EDR. The application of machine learning and a monitoring process by EDR ensures it is a strong tool in dealing with novel threats. The	However, EPP faces several limitations like signature-based detection mechanisms, resource intensiveness, and concerns associated with the use of cloud services.

	detection and response tools for mitigating insider threat		model and simulations presented in this paper also aid in determining efficiency, accuracy, and loss, which assist organizations in selecting the most superior method depending on organizational needs	EDR is considered more sophisticated than EPP. However, this product still faces issues like FPs. The deployment of EDR is resource-intensive.
5	ENDPOINT DETECTION AND RESPONSE (EDR)	S. S. Chaudhari, S. S. Pradhan, H. S. Pudake, A. K. Shinde, and L. Varma	The paper shows how typical signature-based security is improved by the Endpoint Detection and Response solutions, which apply behaviour-based detection to identify advanced threats like fileless malware, zero-day attacks, and advanced persistent threats. Core functionalities of EDR solutions include threat detection, incident response, and automated response, all of which support real-time security.	Moreover, EDR solutions are also resource-intensive, meaning they are less suitable for small and medium-sized enterprises. Also, privacy issues are a concern, given the nature of the data collected and stored by the EDR solution. The above-mentioned drawbacks indicate a demand for scalable, privacy-preserving, and cost-effective solutions for the EDR tool.
6	Enhance Cyber Security with EDR and XDR Solutions	Mohammed Mujtaba, Aseel A Omair, Rawan A Zowaid, & Zaki S Ahmed.	Real-time monitoring, behavioural analytics, and automated response are all provided by EDR and XDR, which enhance advanced threat identification and shorten response times. By combining data from endpoints, networks, cloud, and email, XDR increases visibility.	They are expensive to implement, generate false positives, and need trained personnel. Integration is difficult, and ongoing data collecting raises privacy issues.
7	Effectiveness of EDR Solutions in Combating Modern Cyber Threats	Zainuddin Bin Yusof	EDR products enable endpoint continuous monitoring, behavior-based analysis, automated remediation, and forensics. This results in faster detection and response on endpoints associated with ransomware, APT attacks, or fileless malware. This solution enables seamless integration with SIEM and threat intelligence.	A case management-based EDR is resource-intensive and highly prone to false positives, and manual management requires specialized personnel. Compatibility and scalability might pose concerns for smaller firms.

8	Endpoint Detection and Response using Machine Learning	Harmionee Kaur	APT attacks, ransomware, malware, and port scanning are some examples among many that can be detected by machine learning-based EDR systems more accurately compared to traditional methods. This is due to the real-time analytics and adaptability that they offer.	While machines are generally good at recognizing static malware, 'these systems can have difficulty dealing with evolving intelligent malware and attacks, and they are often computationally intensive and suffer from the problem of 'false positives'. Human error, such as configuration and a lack of skills, also detracts from their utility.
9	ENDPOINT DETECTION AND RESPONSE VS. EXTENDED DETECTION AND RESPONSE: A COMPREHENSIVE SURVEY	S. Pokharkar, J. S. Kolie, and G. Gautam,	EDR, with the help of behavioural analysis, rapid incident response, and real-time monitoring, provides strong endpoint-level security. XDR, integrating data from endpoints, networks, cloud, and emails, offers greater visibility, faster detection, lower false positives, and better safeguards against multi-vector attacks than EDR.	EDR is confined to the context of endpoints and cannot handle inter-domain attacks effectively. Although XDR is more elaborate, it is difficult to implement and expensive. It will be difficult for smaller firms to implement it effectively.

10	Performance Evaluation Elastic Security as Open Source EDR for Advanced Persistent Threat Cyberattack	Z. P. Putra, R. Harwahyu, and E. Hebert,	Compared to closed-source commercial technologies, Elastic Security is more affordable, adaptable, and flexible as an open-source EDR.It supports real-time monitoring, integrates with the Elastic Stack, and shows promising results in detecting APT techniques through simulated cyberattack scenarios	The platform still suffers from challenges like increased rates of false positives, very few features tailored specifically to EDR solutions as opposed to commercial solutions, and reliance on expert personnel for setup and optimization. Possibly, the platform's ability to counter highly advanced attacks will not be on par with commercial-grade solutions for enterprises.

The EDR signifies endpoint monitoring and response in real time, and this is the same for the entire set of studies. The above table explains how various researchers tackled the problem of EDR in their own unique ways, methodologically and technically, through the likes of real-time telemetry analysis, AI/ML analytics, forensic analysis, insider threat analysis, SIEM, and finally, XDR. The above table, therefore, signifies the various approaches and the range of methodologies in the literature, and what they are all trying to achieve: enhancing endpoint security.

4. Popular EDR Solution

Commercial EDR solutions are enterprise-level solutions intended for large-scale setups. They provide sophisticated threat protection, automation response, ransomware rollback functionality, and easy integration with enterprise systems. Key benefits include cloud-native designs, analytics powered by AI/ML algorithms, and support from vendors with periodic updates. Although they are highly efficient and very easy to use, they are quite expensive and need certified training. Open-source EDR solutions come with flexible options, which are pretty economical for companies that can handle them with advanced security experts. These include Velociraptor or GRR, among others, which are focused on forensics, response, and flexibility as a result of community-driven code developments. While they do allow for excellent visibility and control, they lack automation capabilities, manually need to be set up, and have a larger learning curve.

1. Commercial EDR Tools

CrowdStrike Falcon: - Cloud-native AI-powered EDR widely used in enterprises. Offers fast detection with low endpoint impact and strong cloud intelligence. Its performance is good on large-scale environments, though subscription costs are very high.

Microsoft Defender for Endpoint: - part of the integrated Microsoft 365 security ecosystem, natively integrated with Windows 10/11. Provides very good protection for Windows endpoints, thanks to native integration and real-time monitoring. Performance is strong in Microsoft environments but weaker for Linux/macOS.

SentinelOne Singularity: - Autonomous AI-based threat detection and response, including rollback. Best for automated ransomware threat response and rollback. Has very good detection accuracy, although resource-intensive for deep scans.

Tool Name	Key Features	Pros	Cons
CrowdStrike Falcon	Cloud-native, AI-based detection, threat intelligence, real-time response	Lightweight agent, great UI, top-tier detection	Expensive
Microsoft Defender for Endpoint	Integrated with Windows, threat analytics, behavioral monitoring	Deep OS integration, strong detection	Less powerful on non-Windows OS
SentinelOne	Autonomous detection, rollback capability, machine learning	Fast response, low false positives	Higher learning curve
Trend Micro Apex One	Exploit protection, machine learning, behavior monitoring	Broad OS support, centralized dashboard	May require tuning
VMware Carbon Black	Behavioral EDR, cloud-native analytics	Strong visibility, policy-based control	Complexity in deployment
Sophos Intercept X	Deep learning, anti-ransomware, exploit prevention	Simple UI, effective for SMBs	Limited integrations

2. Open Source EDR Solution

Wazuh: - Open-source solution with security monitoring capabilities, including EDR, SIEM, and Compliance. Offers robust monitoring and log analysis with manual tuning needed. Performance is stable but not particularly fast compared to commercial EDR Solutions.

Velociraptor: - An open-source tool adapted particularly for DFIR. Very efficient in forensic analysis and in-depth querying. Dependent on the skill level of the analyst. Not the best tool for automated real-time detection.

GRR Rapid Response (Google): - An incident response architecture designed for remote live forensics. Suited for very large-scale investigations as well as remote data acquisition, but difficult to scale up. Needs specialist skills in configuration.

Tool Name	Key Features	Pros	Cons
Wazuh	Security analytics, threat detection, compliance, file integrity checking	Free, ELK integration, community support	Steeper setup, no native rollback
OSSEC	Host intrusion detection, log analysis, real-time alerting	Lightweight, scalable, open-source	Limited real-time EDR features
Velociraptor	DFIR (Digital Forensics and Incident Response), endpoint monitoring	Advanced query engine, active dev	Requires technical expertise
GRR Rapid Response	Google created remote live forensics and incident response.	Great for forensic investigations	Harder to scale
TheHive+ Cortex	SOC integration, case management, threat intel enrichment	Good for investigations, scalable	Not a full EDR, more SOAR/SIEM
KAPE (by SANS)	Triage and evidence collection tool	Great for IR teams, portable	Not a real-time EDR

5. Conclusion and Future Work

To conclude, this research ends by focusing on the extremely crucial role played by Endpoint Detection & Response (EDR) products in securing business endpoints that are increasingly threatened by cyber-attacks these days. From this analysis, this paper shows that EDR solutions are capable of detecting, investigating, and responding to malicious activities in a given environment by testing it on a simulated cyber drill exercise environment. The findings from this analysis clearly identify the strengths and limitations that exist in the available EDR solutions, which offer a useful guideline on which businesses can act upon in order to increase their endpoint defenses against cyber-attacks and ensure that EDR solutions remain a critical component of a business's cybersecurity framework and can help them concentrate their efforts on their implementation for maximum efficiency.

Future work would include the enhancement of the efficacy of EDR solution tools by implementing Artificial Intelligence (AI) concepts and Machine Learning algorithms. AI-based EDR solution tools would have the potential to perform end-point analysis and correlation at a very large scale to detect threats quickly and accurately. Additionally, the future work would implement concepts pertaining to the use of AI recommendation tools, which would enable the generation of specific suggestions relevant to improving the end-point security of the organization by implementing anticipatory threat protection mechanisms and automated response strategies. This futuristic approach would not only enable organizations to be better protected by smarter and more dynamic EDR solution tools to tackle the existing threat environment but would also have the potential to safeguard against upcoming threats.

References

1. A. Arfeen, S. Ahmed, M. A. Khan and S. F. A. Jafri, "Endpoint Detection & Response: A Malware Identification Solution," 2021 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2021, pp. 1-8, doi: 10.1109/ICCWS53234.2021.9703010.
2. Kaur, H., SL, D.S., Paul, T., Thakur, R.K., Reddy, K.V.K., Mahato, J. and Naveen, K., 2024. Evolution of endpoint detection and response (edr) in cyber security: A comprehensive review. In E3S Web of Conferences (Vol. 556, p. 01006). EDP Sciences.
3. Karantzas, G. and Patsakis, C., 2021. An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), pp.387-421.
4. Siji, F.G. and Uche, O.P., 2023. An improved model for comparing different endpoint detection and response tools for mitigating insider threat. Indian J. Eng, 20(53), pp.1-13.
5. S. S. Chaudhari, S. S. Pradhan, H. S. Pudake, A. K. Shinde, and L. Varma, “Endpoint Detection and Response (EDR),” International Research Journal of Modernization in Engineering, Technology and Science, vol. 6, no. 10, pp. 3898–3902, Oct. 2024.
6. Mohammed Mujtaba, Aseel A Omair, Rawan A Zowaid, & Zaki S Ahmed. (2023). Enhance Cyber Security with EDR and XDR Solutions. International Journal of Computer Science and Information Technology Research, 11(3), 128–132.
7. Zainuddin Bin Yusof, “Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats”, JACSTIC, vol. 8, no. 12, pp. 1–9, Dec. 2024.
8. Harmionee Kaur and Richa Tiwari “Endpoint detection and response using machine learning” 2021 J. Phys.: Conf. Ser. 2062 012013DOI 10.1088/1742-6596/2062/1/012013.
9. S. Pokharkar, J. S. Kolie, and G. Gautam, "Endpoint Detection and Response vs. Extended Detection and Response: A Comprehensive Survey," International Research Journal of Modernization in Engineering Technology and Science, vol. 6, no. 11, Nov. 2024, pp.
10. Z. P. Putra, R. Harwahyu, and E. Hebert, “Performance Evaluation Elastic Security as Open-Source Endpoint Detection and Response for Advanced Persistent Threat Cyberattack”, IJECBE, vol. 2, no. 2, pp. 243–260, Jun. 2024.