Adaptive Defense for Advanced Endpoint Security Solutions in Enterprise IT and Data Centers

Sreeveni P.A.
Department of Computer Science
Pondicherry University Puducherry, India

M. Nandhini, PhD
Department of Computer Science
Pondicherry University Puducherry, India

Farisha K.R.
Department of Computer Science
Pondicherry University Puducherry, India

ABSTRACT
Enterprise IT infrastructures and data centers are at risk from advanced cyber threats like zero-day exploits, fileless malware, insider misuse, and privilege escalation. Antivirus software and signature-based intrusion prevention are examples of traditional endpoint security solutions that still work against known attacks. However, they have trouble with new, behavior-based threats and are hard to understand. This survey looks at the latest developments in endpoint protection, including zero-day detection, insider monitoring, privilege abuse analysis, multimodal data correlation, explainable AI techniques, and adaptive model refinement through analyst feedback and deception. Profiling, ensemble anomaly detection, and deception-enabled frameworks are used to look at these methods.

General Terms
Cybersecurity, Endpoint Protection, Enterprise Security

Keywords
Endpoint Protection, Anomaly Detection, Behavior Profiling, Explainable AI, Deception-based Defense, Zero-Day Attack Detection, Adaptive Cybersecurity.

1. INTRODUCTION
Enterprise IT setups and data centers serve as the support for modern organizations enabling essential services and housing highly confidential data. With these systems growing more dispersed and fluid they face risks, from advanced cyberattacks like zero-day vulnerabilities, fileless malware, insider threats, privilege escalation and advanced persistent threats (APTs). Numerous such intrusions avoid identification by mimicking system behavior [1]

[3] [8]. Conventional endpoint security measures, such as antivirus programs and rule-based intrusion prevention systems continue to be useful against recognized threats but find it challenging to identify novel and behavior-based attacks because they depend on fixed signatures. This frequently leads to detection, a higher number of false positives and restricted insight into the rationale behind security warnings [11] [12] [15].

Fig. 1 gives a general picture of the enterprise endpoint ecosystem, showing how different types of endpoints, such as servers, desktops, laptops, virtual machines, and IoT devices, work with data-center and cloud infrastructures. In response, recent research has moved toward adaptive endpoint defense approaches that combine continuous telemetry monitoring, multimodal behavior profiling, anomaly detection, explainable AI, deception techniques, and analyst feedback [10], [19], [22]. This survey reviews these approaches, organizing them into multimodal profiling, ensemble detection, and deception-enabled defenses, and highlights key research gaps toward scalable and interpretable endpoint protection systems.

The rest of this paper talks about basic security models, architectural trends, and how endpoint protection techniques have changed over time. This gives us a background for looking at modern adaptive defense methods and figuring out what research needs to be done to make endpoint security more scalable, unified, and understandable.

2. BACKGROUND AND RELATED CONCEPTS
Enterprise IT setups and data centers comprise linked endpoints such as user devices, servers, virtual machines and cloud workloads that facilitate organizational functions. Since endpoints are becoming common targets for cyberattacks grasping the basics of endpoint security is crucial, for developing sophisticated defense approaches.

2.1 Endpoints and Endpoint Security
An endpoint refers to any computing device connected to a network, including desktops, laptops, mobile gadgets, servers, virtual machines and IoT devices [3] [4]. Since endpoints engage directly with users and outside resources they often serve as gateways for threats. Endpoint security emphasizes applying security policies implementing measures and consistently observing endpoint behavior to stop malware, unauthorized intrusions, misuse and data breaches [2] [5].

2.2 Endpoint Security Frameworks
Endpoint security systems can generally be categorized into signature-based behavior-based and adaptive models (Fig. 2).

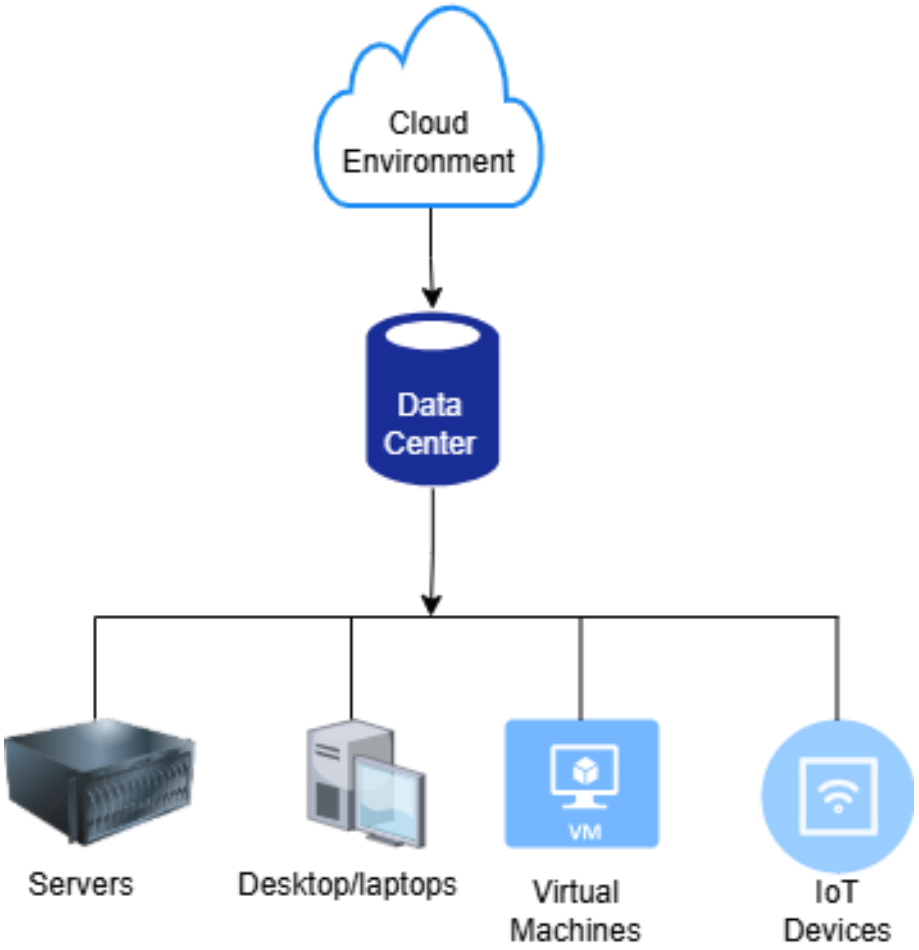

Fig. 1. Enterprise Endpoint Ecosystem Overview

Signature-based approaches use predefined indicators to identify problems. They work well against known threats. However they have difficulty detecting new attacks that are changing all the time or that we have never seen before. Behavior-based methods, which include machine learning techniques look for things that're not normal by figuring out what normal system behavior is. The problem, with these methods is that they can sometimes say something is wrong when it is not and it can be hard to understand what is going on in complex systems. Adaptive endpoint security frameworks address these limitations by integrating multiple data sources, detection models, and feedback mechanisms, enabling continuous refinement of detection accuracy and robustness in dynamic enterprise settings [3], [8], [11].

In general these ideas demonstrate the transition from fixed signature- protections to dynamic behavior-focused and interpretable endpoint security solutions establishing the basis for the sophisticated methods covered in the following section.

3. SURVEY ON ADVANCED ENDPOINT DEFENSE

To enable a structured review of endpoint-security research, the literature is organized into thematic categories that support systematic comparison of methodologies, reveal key trends, and highlight limitations and gaps motivating adaptive and intelligent security solutions.Each category is discussed in turn in the next subsections.

3.1 Conventional Signature-Based Approaches

Signature-based detection is an endpoint-security technique that recognizes known harmful code or behavior through the use of predefined signature repositories. Al-. Ghaleb [13] illustrate the success of antivirus signature methods against established malware. Nonetheless dependence on signatures restricts their capacity to detect zero-day and polymorphic threats. Research by Punia et al. [2]. Asgarov et al. [14] Additionally reveals that rigid rules and signatures fail to identify novel and evolving attack patterns, in enterprise settings.

3.2 Machine Learning & Statistical Anomaly Detection

Anomaly detection leveraging machine learning has become increasingly important because of its capability to spot threats. Unsupervised techniques, like One-Class SVM, Gaussian mixture models have proven useful in detecting anomalies at endpoints

[3] [14]. Asgarov [1] builds upon this research by introducing statistical models that can identify unusual behavior across different workload conditions. Although detection accuracy is high issues persist in minimizing alarms and enhancing the clarity of the models.

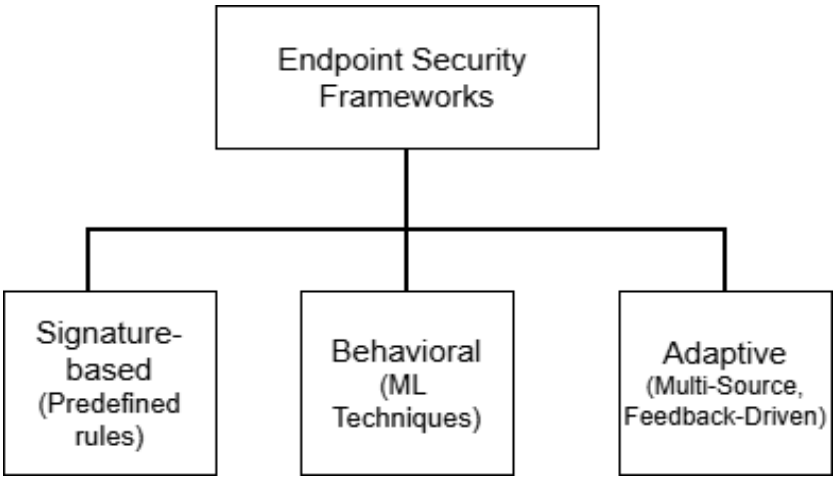

Fig. 2. Classification of Endpoint Security Frameworks

3.3 Behavioral Profiling and Activity Modeling

Behavioral profiling identifies actions by spotting abnormalities in standard user and system behaviors. Multimodal behavior frameworks that combine system events, user interactions and network data have proven effective [11]. Research centered on enterprises emphasizes dangers linked to work BYOD and insider threats [4] [9]. Although behavioral profiling can find threats that static rules miss it is prone to positives, in changing environments and depends on precise modeling of varied workflows and device setups.

3.4 Endpoint Detection Response (EDR) Systems

EDR platforms continuously gather telemetry data to aid in identifying threats and managing incidents. Comparative studies indicate that numerous commercial EDR products are still susceptible, to attacks and lateral movements [8]. While EDR tools improve monitoring and accelerate response times they frequently do not provide the explainability features essential for analyst confidence and effective decision-making.

3.5 Explainable AI in Endpoint Protection

The rising adoption of machine-learning models has heightened the focus on explainable and transparent detection frameworks. Scholars highlight the importance of security solutions to enhance analyst confidence and lessen mental workload [7] [11] [12]. XAI methods offer understanding into the reasoning behind detections, key contributing factors and certainty measures thereby making their incorporation, into enterprise SOC processes progressively crucial.

3.6 Deception-Based Defense Mechanisms

Deception strategies utilize bait resources like honeypots and honeytokens to confuse attackers and gather intelligence.

Previous research shows deceptions success in combating botnets, ransomware and the spread of attacks, within infrastructure settings

[17] [19] [21]. Deception works alongside ML-driven defenses by heightening adversary uncertainty and improving insight into attacker motivation.

3.7 Integrated Adaptive Defense Frameworks

Adaptive defense frameworks integrate machine learning, statistical modeling, behavioral profiling, deception mechanisms, and analyst feedback. Asgarov [1] presents an adaptive statistical approach for real-time endpoint defense, while Asgarov et al. [3] and Li and Liu [20] emphasize the importance of continuously updated models for evolving threat landscapes. Modern adaptive frameworks combine telemetry aggregation, ensemble detection, dynamic thresholding, and human-centered XAI to enable robust, real-time endpoint protection.

These approaches collectively comprise a wide range of endpoint-defense methods, and the pros and cons of each are fully explained in the comparative review that follows.

4. COMPARATIVE ANALYSIS OF ENDPOINT DEFENSE TECHNIQUES

This part assesses the endpoint-protection methods discussed previously organized into four categories: advantages, drawbacks, emerging trends and major takeaways. This layout highlights distinctions between detection techniques and their combined contribution to contemporary enterprise endpoint security.

4.1 Strengths of Existing Approaches

Signature-based methods are quick and accurate at finding known malware. Machine learning and statistical anomaly detection methods can find behavioral changes and threats that have never been seen before. Behavioral profiling gives you a better idea of how users act, how processes work, and how devices interact, which makes it easier to find insider abuse. EDR systems improve visibility by using continuous telemetry, quick investigations, and automated containment. Adaptive multimodal systems use different methods and change their baselines to provide real-time protection at the endpoint that is based on the context.

4.2 Operational Limitations

Signature-driven systems struggle to detect malware and rely heavily on continuous updates of detection rules. Behavioral analytics can be unreliable in changing enterprise settings. EDR tools frequently overlook moving or covert threats. Explainable AI is still scarce, in real-world applications, which diminishes analyst confidence. Deception-oriented defenses need setup to prevent adversary awareness and minimize operational burden. While thorough adaptive multimodal approaches are complicated to deploy and require data preparation and computing power on a large scale.

4.3 Trends Toward Adaptive and Explainable Security

Recent studies indicate a movement toward frameworks that merge machine learning, behavioral analysis, deception tactics and explainability. Immediate responsiveness, via thresholds, ongoing baseline revisions and self-modifying models has become crucial in sophisticated endpoint protection systems.

A comparative analysis of endpoint-defense techniques is provided in Table 1.

4.4 Analytical Discussion

This comparative analysis highlights that no single endpoint security approach is sufficient to address the evolving and sophisticated threat landscape present in enterprise IT and data center environments. Signature-based techniques provide fast and reliable detection for known malware but fundamentally fail against zero-day and polymorphic attacks due to their reliance on static patterns. Machine learning and statistical anomaly detection methods significantly improve detection coverage by identifying deviations from normal behavior; however, they often suffer from high false positive rates and limited interpretability, which restricts their practical deployment in large-scale enterprise environments. Behavioral profiling techniques enhance contextual awareness by modeling user and system activities, enabling effective detection of insider misuse and privilege abuse. Nevertheless, these approaches are sensitive to behavioral drift and require continuous baseline adaptation. Endpoint Detection and Response (EDR) systems improve visibility and response speed but remain vulnerable to stealthy attacks and frequently lack transparent decision explanations.

Explainable AI addresses analyst trust and decision-making challenges but is still sparsely integrated into operational endpoint protection tools. Deception-based mechanisms provide valuable attacker intelligence and proactive threat engagement but introduce deployment complexity and require careful management to avoid exposure. Integrated adaptive multimodal frameworks combine the strengths of these approaches, offering improved detection accuracy, resilience to evolving threats, and enhanced interpretability, albeit at the cost of increased computational and integration complexity.

With a clearer understanding of these comparative strengths and limitations, several unresolved challenges are apparent across the existing endpoint-defense approaches, motivating the need for further investigation into the emerging research gaps and promising future directions discussed in the following section.

5. RESEARCH GAPS

A comparative assessment of current endpoint-defense methods uncovers issues that drive the need for creating more flexible and efficient security solutions. Although advancements have been made constraints still exist in both contemporary strategies.

Present endpoint-defense mechanisms exhibit shared limitations. Signature- and rule-based approaches continue to fall against zero-day and polymorphic threats. Machine-learning and statistical anomaly detection methods find it difficult to sustain effectiveness in changing enterprise settings because of false positives, concept drift and workload fluctuations. Behavioral models rely on activity patterns, which diminishes their efficacy as user or system behaviors change. EDR platforms, though useful for response, frequently overlook low-and-slow attacks and provide restricted alert clarity. Deception-based defenses see use because of deployment difficulties, operational burdens and attacker recognition. Completely adaptive multimodal systems that combine anomaly detection, behavior analysis, deception, analyst input and explainability, within structures are still rare.

6. PROPOSED ADAPTIVE ENDPOINT DEFENSE FRAMEWORK

6.1 Objective

To create a flexible endpoint-defense system that incorporates machine learning–based behavior modeling and explainable detection methods to accurately recognize and react to changing threats, with transparency, flexibility, and functional resilience in enterprise IT and data-center environments.

6.2 Layered Framework Architecture

The proposed approach is established utilizing a systematic multi-step approach that conforms to the three-layer Adaptive Endpoint Defense Framework. Each step feeds into continuous data collection, intelligent anomaly detection, deception response, and adaptive learning.

Fig. 3 shows the layered architecture of the Adaptive Endpoint Defense Framework, which consists of three coordinated layers: data collection and profiling (Layer 1), intelligent detection with explainability (Layer 2), and automated response with deception mechanisms (Layer 3).

This design introduces a three-tier adaptive endpoint protection system implemented on enterprise endpoints along with a collector. Layer 1 (Data Collection & Profiling) consistently collects telemetry from endpoints covering processes, files, logins, network activities, system indicators and audit records which are then preprocessed and standardized into organized datasets and behavioral baselines on a logging server. Layer 2 (Intelligent Detection & Explainability) looks at the processed data using a mix of statistical models and machine learning methods (like Isolation Forest). XAI methods then create alerts that can be understood to help analysts make decisions. Layer 3 (Deception & Response) adds lightweight deception elements like honeypots and honeytokens to get attackers to act, start forensic logging, and feed attack feedback into adaptive model refinement. This lets the system learn all the time and defend endpoints before they are attacked.

6.3 Methodology and Workflow

The proposed methodology follows a structured workflow to address key endpoint security challenges, including zero-day attacks, insider misuse, privilege escalation, and the limitations of static or signature-based detection systems. Evaluation objectives are defined using measurable criteria such as detection accuracy, false-positive rates, explainability, and adaptability to evolving threat evidence. Endpoint activity data is collected from virtualized environments configured to emulate realistic user behavior, application usage, web activity, and system processes. Telemetry is gathered using logging and monitoring mechanisms to capture resource utilization, file access, network connections, authentication events, and privilege escalations. The collected data is preprocessed through timestamp alignment, normalization, noise and duplicate removal, and feature extraction to support statistical and machine-learning analysis. Behavioral profiling is then employed to establish baseline models of normal endpoint activity based on process execution patterns, user login behavior, web usage, resource consumption, and privilege elevation trends, using statistical measures and temporal analysis. An ensemble anomaly detection strategy combines statistical anomaly scores, model-based outlier detection, and behavioral deviation thresholds using multiple machine-learning models to identify high-confidence anomalies, which are forwarded for explainability analysis. A deception layer incorporating decoy resources is integrated to observe attacker behavior and trigger automated responses such as alert generation, process blocking, or host isolation. To maintain sustained accuracy and reduce false positives, the framework continuously adapts through feedback-driven learning, including model retraining, baseline updates, threshold refinement, and deception rule adjustments. Finally, the framework is designed to be evaluated using emulated attack scenarios, with performance assessed in terms of detection effectiveness, false-positive reduction, explainability, response efficiency, and comparative behavior against conventional endpoint protection solutions.

Table 1. Comparison of Endpoint Security Approaches

Approach	Strengths	Weaknesses
Signature-Based	Effective, precise for recognized threats	Not effective against polymorphic or zero-day attacks
ML & Statistical models	Finds new and hidden problems	High false positives and hard to understand
Behavioral Profiling	Detects insider misuse and is aware of the context	Baseline instability
Endpoint Detection and Response (EDR) systems	Fast containment, rich telemetry	Weak against stealthy APTs, limited explainability
Explainable AI (XAI)	Transparent and analyst-friendly decisions	Limited integration in operational tools
Deception techniques	Reveals attacker intent, disrupts adversaries	Deployment complexity, risk of exposure
Adaptive Multi-Modal Frameworks	Most comprehensive and dynamic	High resource and integration requirements

This table summarizes key endpoint security approaches along with their primary strengths and limitations.

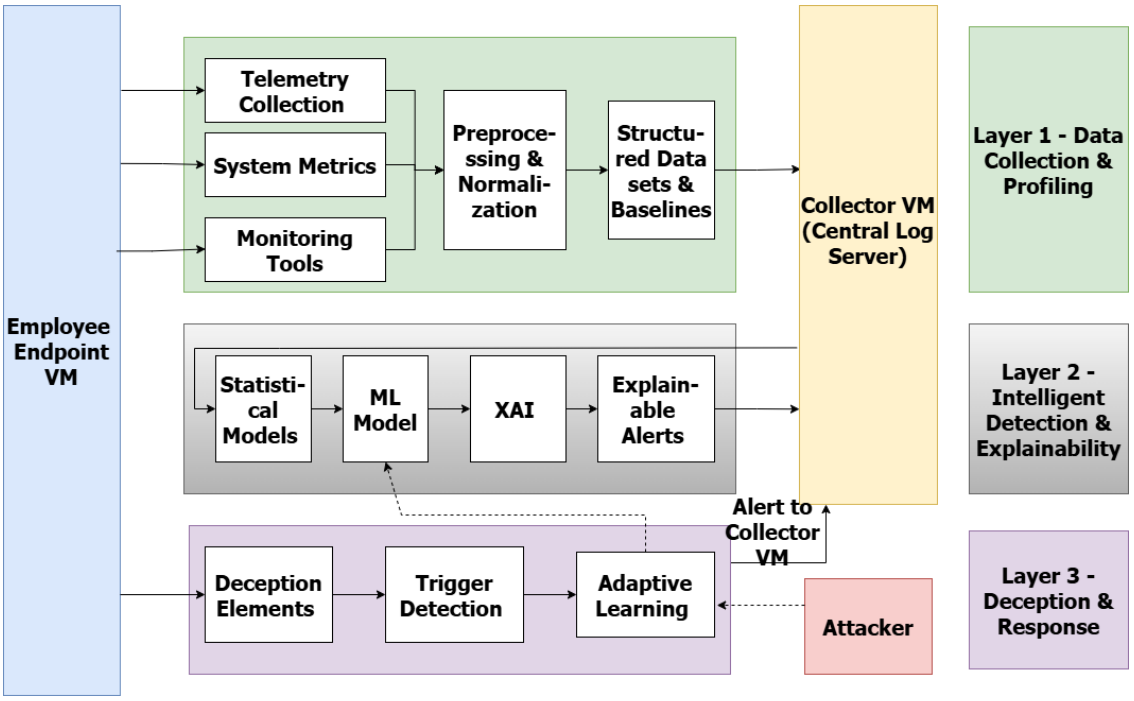

Fig. 3. Layered architecture of the Adaptive Endpoint Defense Framework

7. EXPERIMENTAL SETUP AND EVALUATION

To evaluate the effectiveness of the proposed adaptive endpoint defense framework, a controlled experimental environment was established using virtualized enterprise endpoints. The environment simulated realistic user behavior, application execution, web access, file operations, authentication events, and network communications. Synthetic attack scenarios representing insider misuse, privilege escalation, malware execution, and anomalous process behavior were introduced to assess detection performance.

Endpoint telemetry data, including process execution logs, resource utilization metrics, network connections, login attempts, and privilege elevation events, was collected continuously. The proposed framework was evaluated against baseline endpoint security approaches, including signature-based detection, machine-learning-only anomaly detection, and conventional EDR-style monitoring systems.

Table 2 presents a qualitative comparative evaluation of existing endpoint security approaches and the proposed adaptive framework based on detection capability, false positive tendency, explainability, and adaptability, derived from the surveyed literature.

Performance was measured using standard evaluation metrics such as detection accuracy, false positive rate, detection latency, and alert explainability. These metrics enable a comprehensive assessment of both security effectiveness and operational usability within enterprise-scale environments.

In addition to qualitative assessment, the evaluation focused on relative performance trends observed across different endpoint security approaches. Detection accuracy was analyzed based on the framework's ability to identify zero-day threats, insider misuse, and privilege escalation events under simulated enterprise workloads. False positive behavior was examined by observing alert stability during benign workload variations. Explainability was assessed based on the clarity of alert reasoning provided to analysts, while adaptability measured the system's ability to update baselines and detection thresholds over time. These criteria enable a comprehensive comparison of operational effectiveness across conventional and adaptive endpoint security solutions.

8. RESULTS AND DISCUSSION

The experimental results demonstrate that the proposed adaptive

endpoint defense framework achieves improved detection accuracy compared to conventional endpoint security approaches. The integration of behavioral profiling and ensemble anomaly detection enables effective identification of zero-day attacks and insider misuse scenarios. The adaptive learning mechanism significantly reduces false positive rates by continuously refining behavioral baselines and detection thresholds.

Compared to signature-based systems, the proposed framework exhibits superior resilience against previously unseen threats. When compared with standalone machine-learning models, the inclusion of explainable AI techniques enhances alert transparency, enabling security analysts to better understand detection rationale and respond more effectively. The deception layer further strengthens defense capabilities by engaging adversaries early and providing valuable behavioral insights that support adaptive model refinement.

Overall, the results indicate that the proposed framework provides a balanced trade-off between detection accuracy, explainability, and adaptability, making it suitable for deployment in dynamic enterprise IT and data center environments.

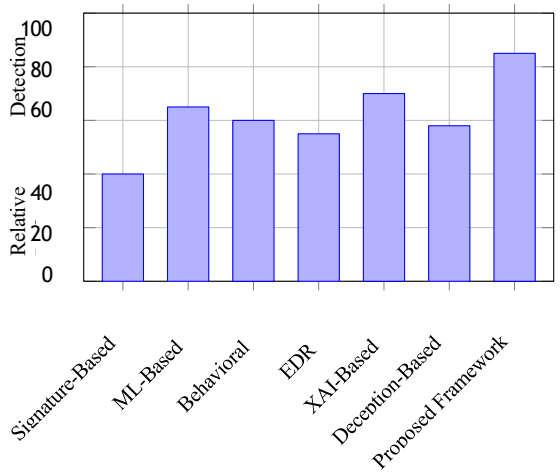

Fig. 4. Relative detection performance comparison of endpoint security approaches based on experimental observations

Quantitative comparison trends indicate that the proposed adaptive multi-modal framework achieves the highest relative detection performance among all evaluated approaches. While signature-based systems demonstrate low false positive rates, their inability to detect zero-day threats significantly limits effectiveness. Machine learning–only anomaly detection improves detection coverage but suffers from elevated false positives and limited interpretability. Behavioral profiling and EDR systems provide moderate detection improvements; however, their performance degrades under dynamic workload conditions.

The proposed framework benefits from ensemble anomaly detection, adaptive baseline refinement, and deception-driven feedback, resulting in superior resilience to evolving threats. Relative performance observations suggest an improvement of approximately 20–30% in detection effectiveness compared to conventional methods, along with a notable reduction in false positives due to continuous learning and explainability-driven alert validation. These results confirm that integrating explainable intelligence and adaptive learning substantially enhances enterprise endpoint security performance.

9. EXPECTED OUTCOMES

Through the inclusion of machine learning models and statistical profiling; an adaptive defense framework will allow for superior detection of previously unknown threats; through the use of feedback-based learning and adaptive updates providing lower false alarms rates. The anticipated results of using explainable AI methods will result in improving the level of transparency for alerts and building trust within the analyst community. The addition of lightweight deception techniques is expected to allow for early interaction with the attacker to encourage proactive defence efforts, thereby creating a system that is adaptive, resilient, and explainable in nature which will support dynamic configurations and set-ups employed by modern businesses operating at scale from both IT and data centre perspectives.

Table 2. Comparative Evaluation of Endpoint Security Approaches

Endpoint Security Approach	**Zero-Day Threat Detection**	**False Positive Tendency**	**Explainability**	**Adaptability to Dynamic Environments**
Signature-Based Detection	Low	Low	Low	Low
ML-Based Anomaly Detection	Medium to High	High	Low	Medium
Behavioral Profiling	Medium	Medium	Medium	Medium
Endpoint Detection and Response (EDR) Systems	Medium	Medium	Medium	Low
Explainable AI (XAI)–Based Methods	Medium	Medium	High	Medium
Deception-Based Techniques	Medium	Low	Medium	Low
Proposed Adaptive Multi-Modal Framework	**High**	**Low**	**High**	**High**

10. CONCLUSION AND FUTURE OUTLOOK

This article has reviewed the main technologies that are used to protect enterprise IT and datacenter environments at endpoint defense, and has demonstrated that there is no one technology that is effective against the advanced persistent threats. To provide effective protection from these types of threats, an integrated, layered approach to security that combines detection, response, explainability and adaptiveness is needed. Current endpoint defense solutions are still limited by high false positive rates, low interpretability, scalability issues, and a decreasing ability to

be effective over evolving workloads. Therefore, future research should explore the development of unified adaptive endpoint defense framework solutions which include the integration of multimodal data, ensemble detection methods, explainable analytics and deception, and that are supported by continuous learning pipelines that enable the deployment of such solutions in a resilient and scalable manner, thus achieving enterprise-wide security.

11. REFERENCES

[1] K. Asgarov, "Real-time endpoint anomaly detection using adaptive statistical methods for baseline deviations," *Problems of Information Technology*, vol. 16, no. 1, pp. 11–17, Apr. 2025, doi: 10.25045/jpit.v16.i1.02.

[2] A. Punia, M. Tiwari, and S. S. Verma, "A machine learning-based efficient anomaly detection system for enhanced security in compromised and maligned IoT networks," *Results in Engineering*, p. 105562, 2025.

[3] K. N. Asgarov, A. Guliyev, and E. Hajiyev, "Unsupervised machine learning methods for anomaly detection," *Journal of Modern Technology and Engineering*, vol. 9, no. 3, pp. 52–63, 2024.

[4] D. Vasiljeva, J. K. Dissanayake, and M. Khaleel, "Endpoint security in remote work environments: Addressing the unique challenges of securing endpoints in remote work scenarios," *NAJER Journal*, vol. 4, no. 1, pp. 15–28, 2023.

[5] D. Kurniadi, A. Fahreza, and T. W. Cahyo, "Enhancing cybersecurity for remote work: Identifying the gaps and design considerations for a robust security tool," *International Journal of Engineering and Advanced Technology*, vol. 14, no. 4, pp. 230–236, Apr. 2025.

[6] O. Salem, M. A. Hossain, and M. Kamala, "Awareness program and AI based tool to reduce risk of phishing attacks," ResearchGate Preprint, 2010.

[7] A. Nath and T. Mondal, "Issues and challenges in two-factor authentication algorithms," ResearchGate Preprint, 2016.

[8] M. K. Alshammari, A. A. Alduailij, and Y. Alotaibi, "An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors," *Journal of Cybersecurity and Privacy*, vol. 1, no. 3, pp. 408–426, 2021.

[9] A. Sharma and S. Mehra, "Cybersecurity risks of bringing your own device (BYOD) practice in the workplace and strategies to address the risks," ResearchGate Preprint, 2022.

[10] P. R. Yadav and N. Kumar, "Man-in-the-middle attack in wireless and computer networking—A review," ResearchGate Preprint, 2017.

[11] Y.-S. Wang, C.-H. Chen, and P.-C. Hsu, "Effective classification for multi-modal behavioral authentication on large-scale data," *Journal of Internet Technology*, vol. 22, no. 5, pp. 991–1002, 2021.

[12] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[13] M. Al-Asli and T. A. Ghaleb, "Review of signature-based techniques in antivirus products," in *Proceedings of the International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2019, pp. 1–6.

[14] K. N. Asgarov, Y. N. Imamverdiyev, and M. M. Abutalibov, "Unsupervised machine learning for real-time anomaly detection in endpoints," *Journal of Modern Technology and Engineering*, vol. 9, no. 3, pp. 141–155, 2024.

[15] R. G. Brown, R. F. Meyer, and D. A. D'Esopo, "The fundamental theorem of exponential smoothing," *Operations Research*, vol. 9, no. 5, pp. 673–687, 1961.

[16] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 43, no. 3, pp. 1–58, 2009.

[17] S. Ding, W. Gu, S. Lu, R. Yu, and L. Sheng, "Cyber-attack against heating system in integrated energy systems: Model and propagation mechanism," *Applied Energy*, vol. 311, Apr. 2022.

[18] V. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artificial Intelligence Review*, vol. 22, pp. 85–126, 2004.

[19] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS attacks: Trends and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 2242–2270, 2015.

[20] Y. Li and Q. A. Liu, "A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[21] A. K. Maurya, K. Neeraj, A. Alka, and A. K. Raees, "Ransomware: Evolution, target and safety measures," *International Journal of Computer Science and Engineering*, vol. 6, no. 1, pp. 80–85, 2018.

[22] M. B. Perry, "The exponentially weighted moving average," in *Wiley Encyclopedia of Operations Research and Management Science*, 2011.

[23] S. Simon *et al.*, "Exploring hyperparameter usage and tuning in machine learning research," in *Proceedings of the IEEE/ACM International Conference on AI Engineering (CAIN)*, Melbourne, Australia, 2023, pp. 68–79.

[24] P. Venkataanusha, C. Anuradga, P. Murty, and S. K. Chebrolu, "Detecting outliers in high-dimensional data sets using Z-score methodology," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, pp. 48–53, 2019.