June 30, 2025 Vol. 8 No. 2 E-ISSN 3027-0480 P- ISSN 3027-2750
Harvard International Journal of
ENGINEERING RESEARCH AND TECHNOLOGY (HIJERT)
www.harvardpublications.com

TRADITIONAL VS NEXT GENERATION ANTIVIRUS: EVALUATING THEIR ROLE IN MODERN CYBER SECURITY

OGHENETEGA AVWOKWURUAYE; EJINKONYE IFEOMA O.; & ALIYU MUSTAPHA UMAR
Department of Cybersecurity, Admiralty University of Nigeria, Delta State
Corresponding Author:
avwokuraye-cyber@adun.edu.ng

DOI: https://doi.org/10.70382/hijert.v8i5.010

Abstract

The rapid evolution of malware has raised questions about the adequacy of traditional antivirus software, which primarily relies on signature-based detection. While effective against known threats, this approach is insufficient for addressing emerging risks such as ransomware, zero-day exploits, and advanced persistent threats (APTs). This study investigates the comparative effectiveness of traditional antivirus solutions and next-generation antivirus (NGAV) systems. Using a review of scholarly literature, industry reports, and case studies, the paper evaluates how

Keywords: Antivirus, Cybersecurity, NGAV, Ransomware, Machine Learning, Zero-Day Exploits.

INTRODUCTION

In an era where digital threats are evolving at an unprecedented pace, the significance of robust cybersecurity measures has never been more paramount. With cyberattacks becoming increasingly sophisticated, the tools we rely on to safeguard our digital environments must also advance. Antivirus software, a cornerstone of cybersecurity for decades, is undergoing a transformative shift from traditional models to next-generation solutions. While traditional antivirus software primarily focuses on known malware signatures, next-generation antivirus (NGAV) employs advanced technologies such as artificial intelligence and machine learning to detect and mitigate both known and unknown threats in real-time. Despite the extensive discussion of these developments in industry reports and white papers, there remains a

artificial intelligence, behavioral analytics, and global threat intelligence contribute to NGAV's resilience against modern attacks. Findings indicate that NGAV significantly outperforms traditional antivirus in detecting and mitigating advanced threats. The study contributes to the cybersecurity discourse by recommending a hybrid defense framework that leverages the strengths of both approaches to deliver cost-effective and comprehensive endpoint protection.

notable gap in academic literature: few studies provide a systematic, research-driven comparison of traditional antivirus and NGAV approaches, particularly with respect to their effectiveness in real-world attack scenarios, organizational adoption challenges, and long-term implications for cybersecurity strategy. Existing scholarship often treats antivirus solutions as a monolithic category, overlooking the nuanced differences in detection methods, performance trade-offs, and resource requirements.

This paper seeks to bridge that gap by offering a structured analysis of traditional and next-generation antivirus technologies within an academic framework. By integrating insights from both industry practice and scholarly research, it examines the strengths, limitations, and contextual applications of each approach. In doing so, the study contributes to a deeper understanding of how antivirus solutions evolve alongside emerging cyber threats, providing a foundation for further research and informed decision-making in cybersecurity strategy.

LITERATURE REVIEW

Detection Effectiveness

Traditional antivirus (AV) solutions rely primarily on signature-based detection, matching files against databases of known threats. This approach is effective for well-documented malware but struggles with zero-day exploits and rapidly mutating attacks (Symantec, 2021). McAfee (2020) similarly notes that signature updates cannot keep pace with the speed of new malware variants, leaving systems vulnerable during the gap between emergence and recognition.

Next-generation antivirus (NGAV) addresses these shortcomings by using artificial intelligence (AI), machine learning (ML), and behavior-based detection to identify threats in real time. Gartner (2022) highlights that NGAV's ability to recognize anomalous behaviors improves detection of unknown threats. However, Gartner's findings are based on vendor data and analyst assessments, which raises concerns about market-driven bias. Independent, peer-reviewed evaluations remain limited, leaving an academic gap in objective comparative analysis.

False Positives and Accuracy

A recurring limitation of traditional AV is its high rate of false positives, where legitimate files are mistakenly flagged as malicious (McAfee, 2020). This not only disrupts workflows but also erodes user confidence in the tool. NGAV claims to reduce false positives by

focusing on behavioral patterns, but evidence is mixed. While Gartner (2022) suggests greater precision, CISA (2021) warns that automated response features in NGAV can exacerbate the impact of false positives by triggering unnecessary quarantines or remediation processes. These conflicting perspectives reveal a lack of consensus on NGAV's accuracy, pointing to the need for rigorous, independent testing in diverse computing environments.

Resource Consumption and Performance

Performance trade-offs also differentiate traditional AV and NGAV. Traditional solutions often consume significant system resources due to constant scanning and large signature updates (Symantec, 2021). NGAV attempts to offset this by using cloud-based analytics, which can reduce local processing demands (Gartner, 2022). Yet, reliance on cloud infrastructure introduces new challenges, such as bandwidth strain and latency issues, particularly in low-connectivity regions. Few academic studies provide empirical benchmarking of these trade-offs in real-world enterprise contexts, leaving organizations to rely primarily on vendor claims.

Incident Response and Organizational Integration

Traditional AV tools generally provide limited incident response, alerting administrators to threats but offering minimal automated containment (CISA, 2021). NGAV enhances this by incorporating continuous monitoring and automated response, which can reduce malware dwell time and improve organizational resilience. However, automation also introduces the risk of over-reliance on AI-driven decision-making, raising questions about accountability and the role of human oversight in critical incidents. While industry reports highlight these capabilities, detailed academic case studies on NGAV adoption, integration challenges, and long-term effectiveness are scarce.

Critical Gaps in Literature

Overall, the literature reflects an overreliance on industry-driven sources (e.g., Gartner, McAfee, Symantec, CISA), which may embed commercial or policy biases. There is also a lack of independent, peer-reviewed benchmarking directly comparing traditional AV and NGAV performance. Furthermore, the underexplored dimensions of organizational adoptions Such as cost, compliance, and user trust suggest that current research is overly detection-focused. Addressing these gaps requires a shift from descriptive reporting toward empirical, academic studies that evaluate both technical effectiveness and broader organizational implications.

METHODOLOGY

This study adopts a mixed-methods research design, combining a systematic literature review with empirical data from surveys and case studies. This approach allows for a balanced understanding of antivirus software effectiveness, drawing on both existing scholarly/industry knowledge and firsthand practitioner insights.

Systematic Literature Review

Databases and Keywords: Relevant sources were collected from IEEE Xplore, ScienceDirect, and Google Scholar, using the keywords: "traditional antivirus," "next-generation antivirus," "cybersecurity," "malware detection," and "effectiveness."

Timeframe: Studies published between 2018 and 2023 were prioritized to ensure contemporary relevance.

Inclusion Criteria: Studies were included if they:

i. Compared traditional antivirus with NGAV technologies.
ii. Reported effectiveness against modern cyber threats such as ransomware, phishing, and advanced persistent threats (APTs).
iii. Provided empirical data, performance metrics, or case studies illustrating antivirus performance.

Data Extraction and Synthesis: From each study, information was extracted regarding:

i. Types of antivirus solutions analyzed.
ii. Metrics used (e.g., detection rates, false positives, performance overhead).
iii. Contextual factors (e.g., organizational size, threat landscape).

Findings were thematically organized into four categories: detection effectiveness, false positives and accuracy, resource consumption, and incident response.

Surveys

Target Population: The survey targeted IT professionals, cybersecurity analysts, and decision-makers with practical experience using antivirus solutions.

Sample Size and Recruitment: A total of 25 respondents participated, recruited via professional networks such as LinkedIn, cybersecurity forums, and organizational contacts.

Survey Instrument: A structured questionnaire was designed, containing both closed-ended (Likert-scale) and open-ended questions. The survey focused on:

i. Current use of traditional vs. NGAV solutions.
ii. Perceived effectiveness of antivirus tools against specific threats (e.g., ransomware, phishing).
iii. Implementation and management challenges, including cost, usability, and system performance.

Data Analysis: Closed-ended responses were analyzed using descriptive statistics (frequencies, percentages, and cross-tabulations) in SPSS. Open-ended responses were thematically coded to capture recurring perceptions and insights.

Case Studies

Selection Criteria: Three organizations were studied, representing small (healthcare clinic), medium (educational institution), and large-scale (financial services) environments. Each had experience with both traditional antivirus and NGAV solutions.

Data Collection: Semi-structured interviews were conducted with IT security personnel (one per organization), supplemented by internal security incident reports. The data focused on malware incidents, detection times, system performance, and user feedback before and after NGAV adoption.

Analysis: A comparative approach was used to identify patterns in detection success rates, incident response times, and operational efficiency across traditional and NGAV deployments.

Ethical Considerations

All participants provided informed consent prior to participation. Survey responses were anonymized to ensure confidentiality, and interviewees were assigned pseudonyms. Participants were informed of their right to withdraw at any time without consequence. Case study organizations were reported in generalized terms to protect organizational identity.

FINDINGS AND RESULTS

The evaluation of 25 participants—comprising IT professionals, cybersecurity analysts, and decision-makers across various industries—produced clear evidence of the relative strengths and weaknesses of traditional antivirus (AV) and next-generation antivirus (NGAV) solutions. These results were triangulated with findings from recent peer-reviewed studies to enhance validity.

Effectiveness of Traditional Antivirus

Participants reported that traditional antivirus solutions were effective at detecting well-established threats but were frequently bypassed by newer, polymorphic variants. Quantitatively, detection rates averaged 68%, with nearly 30% of novel malware samples missed. False positives occurred in 18% of cases, leading to alert fatigue. These findings are consistent with (Azeem, Riaz, & Shahzad, 2023), who demonstrated that reliance on signature databases leaves organizations vulnerable to zero-day exploits. Furthermore, 32% of participants noted performance slowdowns, echoing the concerns documented in (Albshaier, 2024) regarding the resource-heavy nature of traditional AV.

Effectiveness of Next-Generation Antivirus

NGAV systems achieved significantly higher performance across key metrics. Participants recorded an average 92% detection rate, with false positives reduced to 7%. Response times to incidents were 40% faster compared to traditional AV, as NGAV's

integrated behavioral analysis and automated response capabilities allowed quicker containment. These results align with (Han, Lin, Porter, & Polychronakis, 2020), who found that behavior-driven NGAV can identify ransomware activity pre-encryption. Similarly, (Kritika, Dhanya, & Sanjay, 2024) confirmed that machine learning–enhanced NGAV tools outperform signature-based systems against ransomware and phishing threats.

User Experience and Adoption Challenges

Despite its advantages, NGAV adoption presented challenges. 40% of participants expressed concerns about higher licensing costs and increased system resource consumption. Additionally, 12% of respondents experienced false negatives, where NGAV failed to identify stealthy attacks later confirmed as malicious. These issues are consistent with findings by (Arabo, Dijoux, Poulain, & Chevalier, 2020), who noted that low-and-slow advanced persistent threats (APTs) can sometimes evade behavioral detection. (Popryho, 2023) also warned of privacy risks stemming from NGAV's reliance on cloud-based intelligence, an issue reflected in participant feedback on organizational data security.

Comparative Analysis

Comparative Performance of Traditional Antivirus and Next-Generation Antivirus (NGAV) Based on Survey Results (n = 25).

Traditional Antivirus vs Next Gen Antivirus

Table 1: Comparative Analysis of Traditional AV vs NGAV

FEATURE/ METRIC	TRADITIONAL ANTIVIRUS	NEXT GEN ANTIVIRUS
Detection Rate	68% (missed ~30% of new/polymorphic threats)	92% (effective against zero-days & APTs)
False Positives	18% (frequent alert fatigue)	7% (significantly reduced)
Response Time	Slower, often requiring manual intervention	Faster, automated containment & remediation
Resource Consumption	Noticeable device slowdown (reported by 32%)	Higher demand but optimized for enterprise use
Cost	Lower licensing and maintenance costs	Higher upfront and subscription costs (40% cited as concern)
Scalability	More suitable for small businesses or individual users	Better suited for medium to large enterprises; resource-intensive
Privacy Concerns	Minimal, as data stays largely local	Cloud-based intelligence raises privacy/security concerns (raised by 28% of participants)

Several participants suggested a hybrid deployment model, where traditional AV provides baseline protection against known threats while NGAV handles behavioral and zero-day detection. This recommendation aligns with academic arguments for multi-layered security frameworks (Azeem et al., 2023).

DISCUSSION

The findings of this study underscore a widening performance gap between traditional antivirus (AV) and next-generation antivirus (NGAV) technologies. The survey of 25 cybersecurity professionals, reinforced by peer-reviewed evidence, confirms that while traditional AV retains value in detecting well-documented threats, its reliance on signature-based detection significantly undermines its relevance in today's dynamic threat landscape. With an average detection rate of 68% and nearly one in five alerts being false positives (see Table 1), traditional AV often contributes to "alert fatigue"—a challenge also highlighted in prior research (Azeem, Riaz, & Shahzad, 2023). These results demonstrate that organizations relying solely on traditional AV face substantial risks in handling zero-day exploits, polymorphic malware, and advanced persistent threats (APTs).

Conversely, NGAV demonstrated superior performance, with participants reporting a 92% average detection rate, lower false positives (7%), and faster response times enabled by behavioral analysis and machine learning (Table 1). These findings are consistent with (Han, Lin, Porter, & Polychronakis, 2020) and (Kritika, Dhanya, and Sanjay, 2024), both of whom emphasize the capacity of NGAV to proactively mitigate ransomware and phishing attacks before they escalate. The empirical results from this study lend practical weight to these academic claims, showing that in real-world organizational contexts, NGAV markedly reduces dwell time and improves response efficiency.

However, the discussion must extend beyond detection and response effectiveness. While NGAV systems clearly outperform traditional AV in threat handling, several challenges temper their adoption. Nearly 40% of participants cited higher licensing costs as a barrier, while others noted increased system resource demands (Table 1). This aligns with Albshaier (2024), who argues that although NGAV provides advanced protection, it is not always scalable for resource-constrained environments such as small businesses or educational institutions. Furthermore, concerns around cloud-based intelligence raised by both participants and (Popryho, 2023) highlight an underexplored issue: privacy. As NGAV systems rely on continuous data sharing and global threat intelligence, organizations must weigh improved detection capabilities against potential risks to sensitive data.

Another limitation identified was NGAV's occasional false negatives (12% of participants reported missed stealthy attacks). This echoes the observations of (Arabo, Dijoux, Poulain, & Chevalier, 2020), who caution that sophisticated APTs designed for stealth can sometimes bypass behavioral analysis. Therefore, while NGAV represents a significant advancement, it is not a silver bullet; the risk of overreliance remains.

A final insight from both participant feedback and academic literature is the potential role of hybrid strategies. Several respondents advocated combining traditional AV's strengths in handling known, catalogued threats with NGAV's behavioral and machine learning–based capabilities. This layered defense model reflects broader calls in cybersecurity scholarship for multi-layered frameworks (Azeem et al., 2023), ensuring redundancy while mitigating the limitations inherent in relying on a single approach.

In sum, the results (Table 1) demonstrate that NGAV substantially enhances organizational resilience against ransomware, phishing, and APTs. Yet, practical challenges—including cost, resource requirements, privacy concerns, and occasional false negatives—demand a more nuanced adoption strategy. Organizations seeking to strengthen cybersecurity must therefore consider not only the technological superiority of NGAV but also the economic, operational, and ethical implications of its deployment.

CONCLUSION

In the ever-changing landscape of cybersecurity, the role of antivirus software remains pivotal, yet it is undergoing a significant transformation. Traditional antivirus solutions, while foundational in the fight against malware, often fall short against sophisticated threats such as ransomware, zero-day exploits, and advanced persistent threats (APTs). In contrast, next generation antivirus (NGAV) solutions leverage cutting-edge technologies, including artificial intelligence, machine learning, and behavioral analysis, to proactively detect and neutralize threats before they can inflict damage.

As cybercriminals continue to evolve their tactics, the effectiveness of antivirus software must also adapt. Today's threats are not only more complex but also more varied, requiring a multilayered defense approach that traditional antivirus alone cannot provide. NGAV solutions enhance traditional methods by incorporating real-time threat intelligence and automated response capabilities, ensuring that organizations can respond swiftly to emerging dangers.

Ultimately, while traditional antivirus software laid the groundwork for cybersecurity measures, the next-generation solutions represent a necessary evolution in defense strategy. Organizations must embrace these advanced tools to safeguard their digital assets effectively. As the cybersecurity landscape continues to evolve, so too must our strategies and technologies, ensuring that we remain one step ahead of cyber adversaries. The future of cybersecurity will depend on a comprehensive approach that integrates both traditional and next-gen antivirus solutions, fostering a resilient defense against the myriad of threats that lie ahead.

REFERENCES

Albshaier, L. (2024). Earlier decision on detection of ransomware identification: A systematic literature review. Information, 15(8), 484. MDPI. https://doi.org/10.3390/info15080484

Arabo, A., Dijoux, R., Poulain, T., & Chevalier, G. (2020). Detecting ransomware using process behavior analysis. Procedia Computer Science, 176, 3210–3219. https://doi.org/10.1016/j.procs.2020.09.238

Azeem, M., Riaz, M., & Shahzad, R. (2023). Malware detection and classification using modern machine learning approaches: A comprehensive review. Computational Intelligence and Neuroscience, 2023, 1–25. https://doi.org/10.1155/2023/6647735

CISA. (2021). Ransomware guidance. Cybersecurity Infrastructure Security Agency. Retrieved from https://www.cisa.gov/ransomware-guidance

Gartner. (2022). Market guide for endpoint protection platforms. Retrieved from https://www.gartner.com/en/documents/4003765

Gartner. (2022). Market Guide for Endpoint Protection Platforms. Retrieved from https://www.gartner.com/en/documents/4003765

Han, J., Lin, Z., Porter, D., & Polychronakis, M. (2020). On the effectiveness of behavior-based ransomware detection. In Proceedings of the 16th International Conference on Security and Privacy in Communication Networks (SecureComm 2020) (pp. 1–20). Springer. https://doi.org/10.1007/978-3-030-63086-7_19

Institute, P. (2021). The Cost of Cybercrime Study. Retrieved from https://www.ibm.com/security/data-breach

Kaspersky. (2021). Cybersecurity Threats: The Year in Review. Retrieved from https://www.kaspersky.com

Kritika, E., Dhanya, R., & Sanjay, H. A. (2024). A comprehensive literature review on ransomware detection using deep learning. Computers and Security, 139, 103801. https://doi.org/10.1016/j.cose.2024.103801

McAfee. (2020). *Threats report*. Retrieved from https://www.mcafee.com/enterprise/enus/assets/reports/rp-threats-report-2020.pdf

Networks, B. (2022). Phishing: The New normal. Retrieved from https://www.barracuda.com

Popryho, L. (2023). Behavior-based ransomware detection in cloud environments (Master's thesis). Linnaeus University, Växjö, Sweden. Retrieved from https://www.diva-portal.org/smash/get/diva2:1773681/FULLTEXT02.pdf

Research, F. (n.d.). The Future of Endpoint Security. Retrieved from https://go.forrester.com/research

Symantec. (2021). Internet security threat report. Retrieved from https://www.broadcom.com/company/newsroom/press-releases?filtr=internet-securitythreat-report