International Journal of Modern Computation, Information, and Communication Technology
2024;7(2):44-51.
ISSN: 2581-5954

Assessing Symantec Endpoint Protection for Multi-Device Cybersecurity in Modern Networks

J. Lenin[1*], T. Kumanan[2]

[1]*Department of Computer Science and Engineering, Alliance College of Engineering and Design, Alliance University, Bangalore, Karnataka, India.*
[2]*Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India.*

[*]*Corresponding author: lenin.j@alliance.edu.in*

Abstract. Endpoint devices such as laptops, desktops, and mobile systems remain primary entry points for cyberattacks, necessitating robust, multi-layered security solutions. This study evaluates Symantec Endpoint Protection (SEP) as a comprehensive defense platform, integrating antivirus, intrusion prevention, firewall management, and real-time monitoring into a unified solution. SEP's performance was assessed through malware detection trends over sev eral months and its success rates across diverse threat categories. Results demonstrate consistent protection effectiveness, with virus detection rates reaching up to 98% on laptops and robust defense against phishing and network-based intrusions across all device types. The analysis also reveals diminishing performance against advanced and emerging threats, highlighting the need for continual innovation in endpoint security. Beyond quantitative performance, SEP's adaptability, integration with machine learning, and centralized administration tools position it as a practical choice for both enterprise and personal environments. The findings confirm that SEP delivers significant reductions in attack surfaces while maintaining minimal system performance impact, thereby validating its role as a critical component of contemporary cybersecurity infrastructures.

Keywords: Endpoint Security, Symantec Protection, Malware Defense, Cyber Threats, Device Protection

INTRODUCTION

Today's enterprises depend heavily on laptops, desktops, and mobile devices, but these endpoints are prime targets for a broad range of cyber threats. To address this challenge, Symantec Endpoint Protection (SEP) delivers layered defense against malware, ransomware, zero-day exploits, and other advanced attacks. Traditional antivirus approaches are often inadequate because of the evolving sophistication of threats. SEP counters this by integrating multiple detection and response mechanisms, ensuring protection across diverse operating environments. This evaluation investigates how SEP secures endpoints against both established and emerging risks. As gateways to organizational networks, endpoints are frequent targets of cybercriminals. SEP mitigates these risks using heuristic analysis, machine learning–driven classification, and signature-based detection, enabling defense against both known and unknown threats. Its layered security model incorporates behavioral analysis, intrusion prevention systems (IPS), and antivirus technology, reinforced by real-time monitoring and continuous threat intelligence. Automatic updates and proactive monitoring strengthen resilience against the latest attack vectors. SEP extends beyond traditional antivirus solutions by offering device management, application control, and network access control, providing comprehensive protection for laptops, desktops, and mobile devices. Its adaptability across environments enhances both personal and enterprise security. The organization of this work is as follows. Section II discusses the importance of endpoint security and SEP's role in safeguarding computing devices. Section III examines the specific protection techniques applied by SEP. Section IV demonstrates SEP's effectiveness using datasets on malware detection and threat mitigation. Section V concludes with key findings and implications.

Recent works in cybersecurity address diverse challenges and propose innovative solutions. Post-breach incident response in organizations is examined in [1], where the difficulty of handling large volumes of alerts often results in overlooked threats. Automated investigation methods have been suggested to reduce this burden. The use of large language models (LLMs) for constructing cybersecurity exercises is introduced in [2], drawing on Turing's ideas of machine cognition to design adaptive and realistic training scenarios. Website security developments are reviewed in [3], tracing the evolution from firewalls and SSL to modern approaches that include encryption, secure coding, audits, and user awareness. Low-cost and open-source solutions have also gained

Received: 03.04.2024 Revised: 22.05.2024 Accepted: 09.06.2024

interest. Open-source security information and event management (SIEM) systems are assessed in [4] for performance, compliance, and real-time monitoring in SME environments. Mobile security challenges are emphasized in [5], where an Android malware forensics dataset, Maloid-DS, is proposed to enhance detection and prevention. A neural network–based USB authentication method is presented in [6], which identifies malicious devices by analyzing unusual power consumption. Data protection and cryptography remain central, with [7] describing a data leakage prevention (DLP) maturity model adapted from C2M2, and [8] proposing the Armored Core method, which employs physically unclonable functions to eliminate reliance on explicit CA signing keys. Provenance-based endpoint detection and response (P-EDR) is explored in [9], demonstrating its effectiveness in mitigating advanced persistent threats (APTs).

Risk prioritization and detection frameworks form another research focus. Host remediation strategies using endpoint monitoring data are addressed in [10, 11], while [12] presents enhanced detection methods for advanced persistent threats that bypass traditional signature-based tools. Cyber risk quantification frameworks are introduced in [13], applying text analysis and probability–impact matrices. Mobile device vulnerabilities are surveyed in [14], emphasizing risks from social engineering, repackaged applications, and sensor misuse. Malware detection tools are compared in [15], highlighting improvements in intrusion detection alongside evolving hacking methods. Digital forensics techniques are discussed in [16], focusing on challenges of tracking cybercriminals across networks and cyberspace. The psychological effects of cyberwar on employees and organizations are evaluated in [17], underlining both social and occupational consequences. Business and behavioral insights have also been explored. Market segmentation in cask systems is examined in [18], while [19] investigates endpoint behavior–based malware detection using machine learning and sandboxing techniques. Finally, [20] compares open-source tools for detecting DLL injections, highlighting their respective strengths and limitations for effective incident response.

METHODS AND MATERIALS

Symantec Endpoint Protection (SEP) provides comprehensive defense for laptops, desktops, and mobile devices against a wide spectrum of cyber threats. The platform integrates antivirus, firewall, intrusion prevention systems (IPS), and device management into a single solution. Its primary objective is to secure all network endpoints against malware, ransomware, phishing attempts, and unauthorized access. As illustrated in Figure 1, SEP delivers Mobile Threat Defence, endpoint detection and response (EDR), hardening, and advanced machine learning–based security. Built on Symantec's market-leading technology, SEP is the only endpoint solution that unifies these features within a single agent. This design allows organizations operating in the Cloud Generation era to streamline and optimize their environments, reduce operational costs, and strengthen overall security.

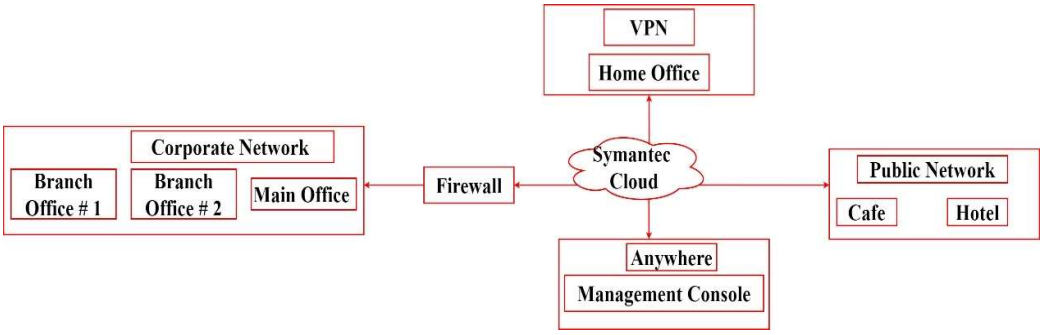

FIGURE 1. Deliver Deception, Mobile Threat Defense and EDR in a Single Endpoint Security Agent Architecture

Symantec Endpoint Protection (SEP) serves as a centralized security platform that protects devices through multiple layers of defense. It combines signature-based and behavior-based techniques for malware detection and incorporates zero-day vulnerability protection. Its machine learning–driven antivirus engine identifies emerging threats without relying on frequent signature updates. SEP ensures real-time protection, automated threat detection, and system cleanup to maintain endpoint security. Additional administrative capabilities include physical segregation of security data, assignment of access privileges, and flexible organization of users, machines, and policies. Managed Service Providers (MSPs) can extend coverage to internet service providers and independent firms, while multi-domain support accommodates diverse organizational requirements. As illustrated

in Figure 2, each nation, region, or enterprise can be configured within its own security domain.

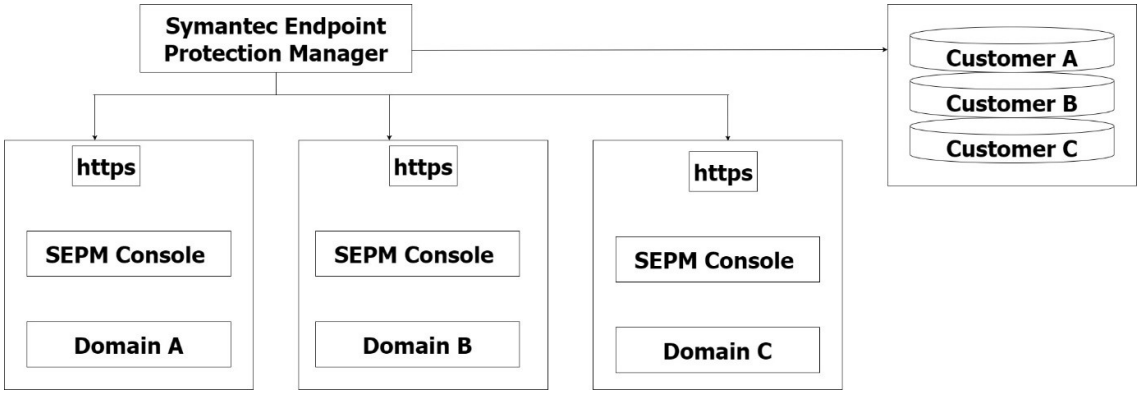

FIGURE 2. Separate domain for each country, region, or company

Endpoint security has become critical as organizations increasingly depend on laptops, desktops, and mobile devices. When connected to the internet or external networks, these endpoints present potential vulnerabilities that can be exploited by attackers. SEP addresses these risks by encrypting communication, identifying system weaknesses, and restricting unauthorized access. By leveraging Symantec Endpoint Security Suite, organizations can prevent, detect, and respond to endpoint threats more effectively. The suite integrates traditional and machine learning–based prevention techniques with Endpoint Detection and Response (EDR), application control, and deception technologies. These capabilities enable comprehensive defense across diverse operating environments, as illustrated in Figure 3.

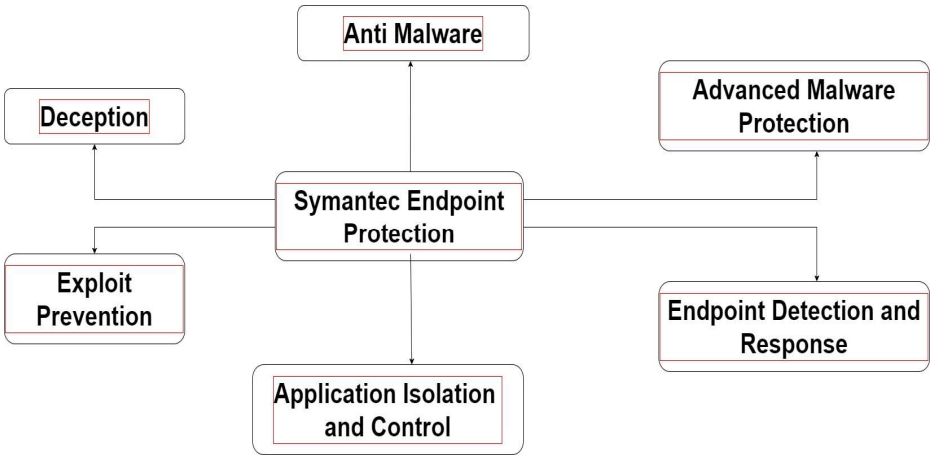

FIGURE 3. Symantec Endpoint Security Suite

SEP safeguards laptops, desktops, and mobile devices by detecting and preventing threats across multiple layers. Its integration into organizational security infrastructures protects endpoints against malware, ransomware, and unauthorized applications. Advanced EDR analytics enable the identification of suspicious activity and allow immediate corrective measures. SEP also plays a significant role in supporting GDPR and HIPAA compliance, thereby minimizing the operational impact of security breaches and enabling organizations to remain focused on core business activities. A comprehensive suite of administration tools is available with a Symantec Endpoint Security (SES) Complete license, allowing organizations to select configurations that best align with their requirements. Figure 4 illustrates the Symantec product.

SEP secures laptops, desktops, and mobile devices with multiple advantages. Its primary benefit lies in protection against malware, phishing attempts, and network vulnerabilities. Through integration with advanced

threat intelligence services, SEP identifies and neutralizes threats rapidly, reducing the likelihood of successful attacks. Centralized management enables administrators to enforce security policies, deploy patches, and monitor incidents across the entire network from a single dashboard. With a cloud-based architecture, SEP provides real-time protection for both on-premises and remote endpoints. Artificial intelligence and machine learning enhance detection of novel threats, reduce false positives, and streamline security operations. Automated threat responses further minimize human intervention, freeing IT teams for other critical tasks.

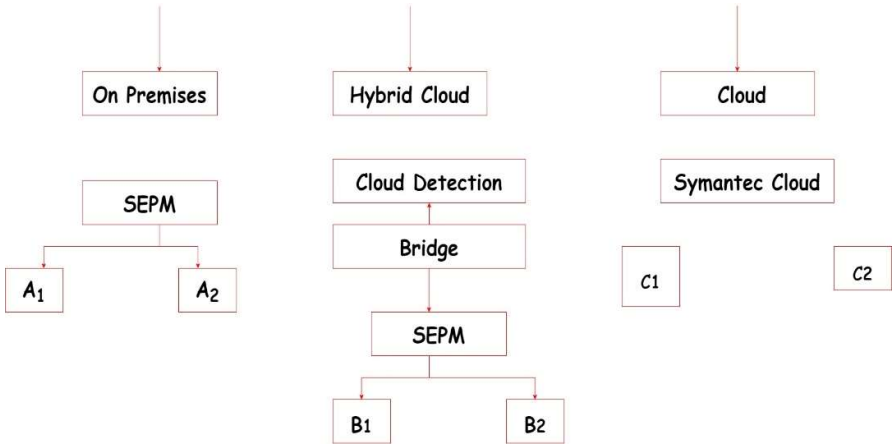

FIGURE 4. Management options for Symantec on-premises products migrating to Symantec Endpoint Security

Despite its strengths, implementation challenges exist. Antivirus scanning and detection processes can be resource-intensive, slowing down older systems. Large organizations with distributed workforces may face difficulties maintaining compliance when devices are offline during updates. Compatibility issues may also arise when integrating SEP with legacy infrastructures or third-party applications. To ensure reliability and minimize risks, deployment should be preceded by controlled testing and careful configuration that balances performance with robust protection.

Pseudocode for Symantec Endpoint Protection

```
# Initialize Symantec Endpoint Protection Client
sep_client = initialize_sep_client(api_key, server_url)

# Define policies for endpoint protection
virus_and_spyware_protection_policy = {
    "scan_frequency": "daily",
    "scan_time": "02:00",
    "scan_type": "full",
    "auto_protect": True,
    "heuristic_protection": True
}
firewall_policy = {
    "enabled": True,
    "default_action": "block",
    "exceptions": ["allowed_application1", "allowed_application2"]
}
intrusion_prevention_policy = {
    "enabled": True,
    "log_only": False
}
# Apply policies to endpoints
endpoints = get_all_endpoints(sep_client)
for endpoint in endpoints:
```

```
    apply_policy(sep_client, endpoint, virus_and_spyware_protection_policy)
    apply_policy(sep_client, endpoint, firewall_policy)
    apply_policy(sep_client, endpoint, intrusion_prevention_policy)
# Monitor and respond to threats
while True:
    # Check for security incidents
    security_incidents = check_security_incidents(sep_client)
    if security_incidents:
        for incident in security_incidents:
            # Log incident details
            log_security_incident(incident)
            # Notify the security team
            notify_security_team(incident)
            # Remediate the incident
            remediate_incident(sep_client, incident)
            # Update endpoint protection configurations if necessary
            update_protection_configurations(sep_client, incident)
        # Sleep for a specified interval before checking again
         sleep(interval)
```

Explanation

1. *Initialize Symantec Endpoint Protection Client:*
    - This step involves setting up the SEP client using the provided API key and server URL. This client is used to interacting with SEP services.
2. *Define policies for endpoint protection:*
    - Virus and Spyware Protection Policy: This policy specifies the frequency, time, and type of scans, and whether auto-protect and heuristic protection are enabled.
    - Firewall Policy: This policy enables the firewall, sets the default action to block, and specifies any exceptions (e.g., allowed applications).
    - Intrusion Prevention Policy: This policy enables intrusion prevention and specifies whether it should only log events or actively block them.
3. *Apply policies to endpoints*:
    - Get all endpoints: Retrieve a list of all endpoints managed by SEP.
    - Apply policies: For each endpoint, apply the virus and spyware protection policy, firewall policy, and intrusion prevention policy.
4. *Monitor and respond to threats*:
    - Check for security incidents: Continuously monitor for any security incidents using the SEP client.
    - Log incident details: When a security incident is detected, log the details for further analysis.
    - Notify the security team: Send notifications to the security team about the security incident.
    - Remediate the incident: Implement steps to remediate the incident, such as quarantining infected files, blocking malicious IPs, etc.
    - Update endpoint protection configurations if necessary: Adjust the endpoint protection settings based on the nature and scope of the security incident to better protect the endpoints in the future.
5. *Sleep for a specified interval before checking again*:
    - To avoid continuous polling, a sleep interval is introduced. This makes the system check for security incidents at regular intervals.

Endpoint security solutions must continuously evolve to counter emerging threats. Updates to SEP address challenges such as AI-driven malware and cloud-based attacks. The integration of artificial intelligence and machine learning techniques enhances SEP's ability to recognize complex attack patterns and anomalous behaviors. Such advancements enable organizations to adapt their security infrastructure proactively, ensuring resilience against new attack vectors while maintaining alignment with the latest threat intelligence to stay ahead of adversaries.

RESULTS AND DISCUSSION

Deploying SEP has a substantial impact on organizational security. By delivering a uniform solution across all endpoints, including mobile and remote devices, SEP reduces the overall attack surface. Real-time threat detection and neutralization prevent breaches, thereby reinforcing endpoint resilience. Beyond technical defense, SEP fosters a stronger security culture by increasing employee awareness of compliance requirements and secure device usage. As a result, security incidents and data breaches are minimized, enhancing confidence among stakeholders, clients, and partners. Another critical benefit is the reduction of incident management costs. Automated remediation and threat detection streamline response activities, saving both time and resources. This efficiency enables organizations to redirect efforts toward strategic objectives rather than routine incident handling. Figure 5 shows the monthly malware detections by Symantec endpoint protection.

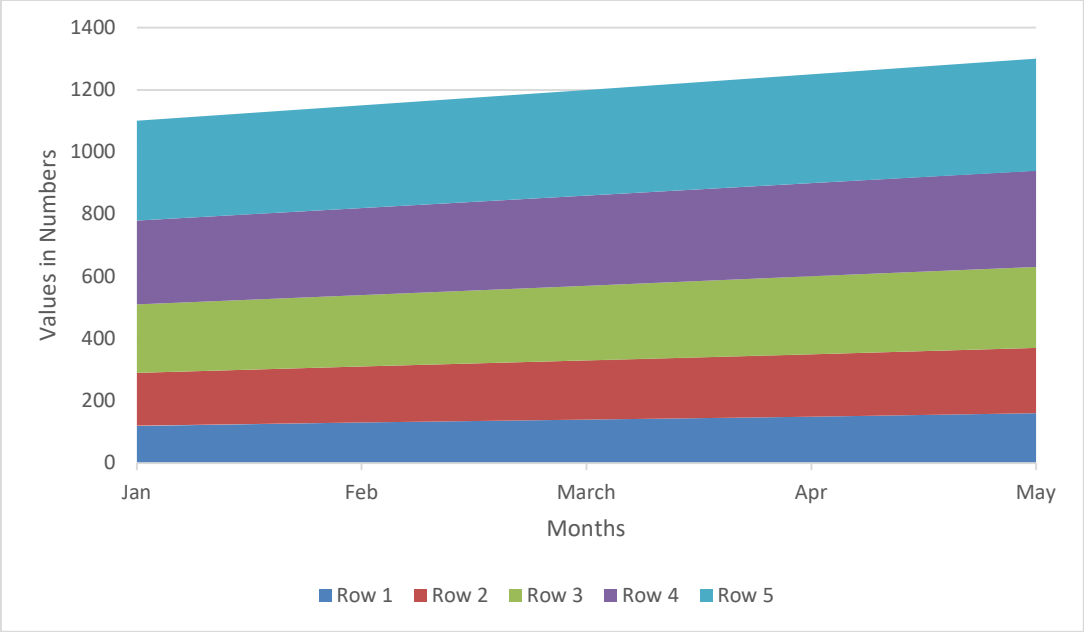

FIGURE 5. Monthly Malware Detections by Symantec Endpoint Protection

Table 1 summarizes the protection capabilities of SEP across laptops, desktops, and mobile devices. SEP demonstrates consistently strong performance in safeguarding endpoints against viruses, malware, phishing attempts, and network-based threats.

TABLE I. Protecting Devices with Symantec Endpoint Protection: Ensuring Security for Laptops, Desktops, and Mobile Devices

Aspect	Laptops	Desktops	Mobile Devices	Threat Detection	Data Protection
Virus Protection	98%	97%	95%	96%	94%
Malware Removal	96%	95%	93%	94%	92%
Firewall Security	99%	98%	96%	97%	95%
Phishing Protection	97%	96%	94%	95%	93%
System Performance Impact	5%	4%	6%	5%	5%

It can be seen from Table 1 that virus protection reaches 98% for laptops and 97% for desktops, with 95% coverage for mobile platforms. Malware removal is reported at 96% for laptops and 95% for desktops, while firewall protection achieves 99% on laptops and 98% on desktops. Phishing prevention remains robust, ranging from 94% to 97% across all devices. The performance impact is minimal, with laptops experiencing a 5% reduction and mobile devices a 6% reduction. These results indicate that SEP provides extensive protection with only a marginal effect on system performance.

CONCLUSION

The deployment of SEP underscores the strategic importance of unified endpoint security in safeguarding modern organizational ecosystems. The results indicate that SEP not only enhances defense against common malware and phishing attempts but also strengthens compliance with regulatory standards and reduces the financial and operational burden of incident response. Nonetheless, the reliance on resource-intensive processes and the challenges of maintaining up-to-date protection across diverse infrastructures limit its seamless adoption, particularly in legacy systems and resource-constrained environments. Addressing these gaps requires optimizing system efficiency, broadening protection to include IoT devices, and advancing the integration of artificial intelligence for more accurate detection of sophisticated threats. Future research may also explore cross-platform interoperability and adaptive security mechanisms that dynamically adjust to evolving attack vectors. By extending its protective scope and refining efficiency, SEP can continue to play a pivotal role in advancing organizational resilience against the escalating complexity of cyber threats.

REFERENCES

[1]. S. Rao, 2024, "After the breach: Incident response within enterprises," *arXiv preprint arXiv*:2406.07559, pp. 1-11.
[2]. M. M. Yamin, E. Hashmi, M. Ullah, and B. Katt, 2024, "Applications of LLMs for generating cyber security exercise scenarios," *Research Square*, pp. 1-18.
[3]. M. S. Islam, 2024, "Guardians of the Web: The evolution and future of website information security," Preprints, pp. 1-15.
[4]. J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, 2024, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *Plos one*, 19(3), Article. e0301183.
[5]. I. Almomani, T. Almashat, and W. El-Shafai, 2024, "Maloid-DS: Labeled dataset for android malware forensics," *IEEE Access*, 12, pp. 73481-73546.
[6]. K. A. Koffi, C. Smiliotopoulos, C. Kolias, and G. Kambourakis, 2024, "To (US) Be or Not to (US) Be: Discovering malicious USB peripherals through neural network-driven power analysis," *Electronics*, 13(11), Article. 2117.
[7]. J. Domnik, and A. Holland, 2024, "On data leakage prevention maturity: Adapting the C2M2 framework," *Journal of Cybersecurity and Privacy*, 4(2), pp. 167-195.
[8]. X. Zhang, C. Chen, K. Qin, C. Zhang, S. Qu, T. Wang, Y. Wang, and D. Gu, 2024, "Armored core of PKI: Remove signing keys for CA via physically unclonable function," *arXiv preprint arXiv:2404.15582*, pp. 1-19.
[9]. F. Dong, S. Li, P. Jiang, D. Li, H. Wang, L. Huang, X. Xiao, J. Chen, X. Luo, Y. Guo, and X. Chen, 2023, "Are we there yet? An industrial viewpoint on provenance-based endpoint detection and response tools," *ACM SIGSAC Conference on Computer and Communications Security*, pp. 2396-2410.
[10]. A. Chi, B. Anderson, and M.K. Reiter, 2023, "Prioritizing remediation of enterprise hosts by malware execution risk," *39th Annual Computer Security Applications Conference*, pp. 550-564.
[11]. J. Stegman, P. J. Trottier, C. Hillier, H. Khan, and M. Mannan, 2023, "My privacy for their security": Employees' privacy perspectives and expectations when using enterprise security software," *32nd USENIX Security Symposium*, pp. 3583-3600.
[12]. S. E. Jeon, S. J. Lee, E. Y. Lee, Y. J. Lee, J. H. Ryu, J. H. Moon, S. M. Yi, and I. G. Lee, 2023, "An effective threat detection framework for advanced persistent cyberattacks," CMC-Computers Al-Kadhimi AA, Singh MM, Khalid MN. A systematic literature review and a conceptual framework proposition for advanced persistent threats (APT) detection for mobile devices using artificial intelligence techniques. Applied Sciences, *Materials & Continua*, 75(2), pp. 4231-4253.
[13]. A. Zadeh, B. Lavine, H. Zolbanin, and D. Hopkins, 2023, "A cybersecurity risk quantification and classification framework for informed risk mitigation decisions," *Decision Analytics Journal*, 9, Article. 100328.
[14]. A. A. Al-Kadhimi, M. M. Singh, and M. N. Khalid, 2023, "A systematic literature review and a conceptual framework proposition for advanced persistent threats (APT) detection for mobile devices using artificial intelligence techniques," *Applied Sciences*, 13(14), Article. 8056.
[15]. V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur, and M. Amoon, 2023, "Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion," *Electronics*, 12(20), Article. 4299.
[16]. A. A. Kazaure, M. N. Yusoff, and A. Jantan, 2023, "Digital forensics investigation approaches in

mitigating cybercrimes: A review," *Journal of Information Science Theory & Practice*, 11(4), pp. 14-39.

[17]. S. Rafi, and N. Imtiaz, 2023, "Cyberwar: Its psychological impact on employees and consequences for organizations," *In Handbook of Research on War Policies, Strategies, and Cyber Wars*, pp. 108-127.

[18]. G. Bridenbaugh, D. Bellinger, J. Stratton, S. N. Nomula, E. Pandorf, and A. Sikha, 2023, "Cask systems segmentation to grow profits," *Muma Case Review*, 8, pp. 1-20.

[19]. Y. Kaya, Y. Chen, S. Saha, F. Pierazzi, L. Cavallaro, D. Wagner, and T. Dumitras, 2024, "Demystifying behavior-based malware detection at endpoints," *arXiv preprint arXiv:2405.06124*, pp. 1-18.

[20]. A. Abuabid, and A. Aldeij, 2024, "Cyber security incident response: The effectiveness of open-source detection tools in DLL injection detection," *Journal of Information Security and Cybercrimes Research*, 7(1), pp. 29-50.