Journal of Secure Enterprise Infrastructure

ENDPOINT PROTECTION SOFTWARE FOR PREVENTING MALWARE, RANSOMWARE, AND UNAUTHORIZED SYSTEM ACCESS

Nasser Al-Khaldi
Kuwait

ABSTRACT

Endpoint protection software secures computers, mobile devices, servers, and other connected systems against malware, ransomware, and unauthorized access. The platform continuously monitors files, applications, network activity, user behaviour, and system processes to identify suspicious actions and emerging threats. Antivirus scanning, behavioural analysis, application control, firewalls, and device encryption strengthen endpoint security. Automated response tools can block malicious programs, quarantine infected files, isolate compromised devices, and prevent unauthorized changes. Real-time dashboards help administrators monitor security alerts, device compliance, software vulnerabilities, and incident severity. Centralized management allows organizations to apply security policies, updates, and access controls across distributed endpoints. Overall, endpoint protection software can reduce cyberattack risks, prevent data loss, strengthen system availability, and support secure enterprise operations.

keywords: Endpoint Protection Software; Malware Prevention; Ransomware Protection; Unauthorized Access Control; Device Security.

1. Introduction

Enterprise applications depend on reliable diagnostics to detect runtime errors, failed workflows, API issues, slow transactions, and integration faults [1]. Logs are the main evidence source for understanding what happened before, during, and after an incident. Effective application diagnostics require structured logging, traceability, contextual metadata, error classification, and operational visibility [2]. However, fixed logging strategies often create two problems. Low-detail logs may miss important causes, while high-detail logs may generate excessive storage cost and alert noise [4].

The main challenge is that diagnostic needs change during runtime. A normal transaction may require only basic logs, but a failing workflow, repeated exception, or security-sensitive event may need deeper traces [5]. Adaptive logging improves this process by changing log depth according to system condition, transaction risk, and error behavior. AI-assisted monitoring can identify when additional diagnostic detail is needed and when logging can return to normal levels. This article proposes an adaptive logging framework for enterprise application diagnostics.

2. Methodology

The proposed framework captures log metadata from application servers, API gateways, databases, background jobs, authentication modules, and integration services [6]. It records event type, severity, timestamp, user role, transaction ID, request path, error frequency, response time, affected component, and workflow state [7]. These features are converted into diagnostic context profiles. Adaptive logging requires context because the same event may be low-risk in one workflow but critical in another.

The logging controller classifies runtime states as normal, warning, error-prone, performance-risk, security-sensitive, workflow-critical, or incident-active [8]. Based on this classification, it adjusts log level, trace depth, parameter capture, correlation ID tracking, and diagnostic enrichment. Lightweight scoring and policy rules are used so logging decisions remain fast and explainable [9]. Sensitive fields are masked before storage, and transaction-critical events are linked with workflow and database identifiers for easier diagnosis.

The framework is evaluated using simulated enterprise applications involving APIs, database workflows, authentication events, scheduled jobs, and service integrations. Static logging is compared with adaptive logging under repeated exceptions, slow requests, failed jobs, API timeout, suspicious login, and workflow interruption scenarios [10]. Evaluation metrics include diagnosis time, log volume reduction, root-cause evidence quality, missed-event rate, storage overhead, alert usefulness, and administrator acceptance rate. Feedback from resolved incidents, ignored logs, and administrator notes is used to refine logging policies over time.

3. Results and Discussion

The results show that adaptive logging improves diagnostics by capturing richer evidence only when runtime risk increases. In the baseline condition, static logs either lack enough detail or produce large volumes of low-value records. With the proposed framework, detailed traces are activated for high-risk events and reduced during normal execution. The strongest improvement appears in intermittent failures, where deeper logs are needed only around the failure window.

The discussion shows that adaptive logging must balance diagnostic depth with privacy and storage cost. Excessive logging can expose sensitive data or overload monitoring systems, while weak logging may hide failure causes. The main limitation is that log-level decisions depend on accurate runtime classification. Regular policy review and masking controls are necessary for safe long-term use.

4. Conclusion

This article presented an adaptive logging framework for enterprise application diagnostics. The framework adjusts log detail using runtime context, risk scoring, workflow state, and error behavior. It improves troubleshooting by increasing diagnostic evidence during abnormal conditions while reducing unnecessary log noise during normal operation. The study shows that adaptive logging can strengthen enterprise diagnostics when combined with structured metadata, privacy controls, and continuous incident feedback.

References

1. Tarofder, A. K., Haque, A., Hashim, N., Azam, S. M., & Sherief, S. R. (2019). Impact of ecological factors on nationwide supply chain performance. Ekoloji Dergisi, (107).
2. STARSurg Collaborative, Writing Committee Nepogodiev D dnepogodiev@ doctors. org. uk Walker K Glasbey JC Drake TM Borakati A Kamarajah S McLean K Khatri C Arulkumaran N Harrison EM Fitzgerald JE Cromwell D Prowle J Bhangu A overall guarantor, Data analysis Walker K Drake TM Cromwell D, Steering committee Glasbey JC Borakati A Drake TM Kamarajah S McLean K Bath MF Claireaux HA Gundogan B Mohan M Deekonda P Kong C Joyce H Mcnamee L Woin E Burke J Khatri C Fitzgerald JE Harrison EM Bhangu A Nepogodiev D, & Advisory group Arulkumaran N Bell S Duthie F Hughes J Pinkney TD Prowle J Richards T Thomas M. (2018). Prognostic model to predict postoperative acute kidney injury in patients undergoing major gastrointestinal surgery based on a national prospective observational cohort study. BJS open, 2(6), 400-410.

3. Haque, A., Khatibi, A., & Mahmud, S. A. (2009). Factors determinate customer shopping behaviour through internet: The Malaysian case. Australian Journal of Basic and Applied Sciences, 3(4), 3452-3463.
4. Maruf, T. I., Manaf, N. H. B. A., Haque, A. K. M. A., & Maulan, S. B. (2021). Factors affecting attitudes towards using ride-sharing apps. International Journal of Business, Economics and Law, 25(2), 60-70.
5. Shafiq, A., Haque, A., & Omar, A. (2015). Multiple halal logos and Malays' beliefs: a case of mixed signals. International Food Research Journal, 22(4), 1727-1735.
6. Iqbal, M., Yasmin, F., Haque, A., Rashid, M. A., Pervin, K., & Maziz, M. N. H. (2022). The study of the perception of diabetes mellitus among the people of Petaling Jaya in Malaysia. International Journal of Health Sciences, (I), 1263-1273.
7. Rahman, S., Hussain, B., & Haque, A. (2011). Organizational politics on employee performance: an exploratory study on readymade garments employees in Bangladesh. Business Strategy Series, 12(3), 146-155.
8. Haque, A., Sarwar, A., Azam, F., & Yasmin, F. (2014). Total quality management practices in the Islamic banking industry: comparison between Bangladesh and Malaysian Islamic bank. International Journal of Ethics in Social Sciences, 2(1).
9. Karim, M. W., Chowdhury, M. A. M., & Haque, A. A. (2022). A study of customer satisfaction towards E-wallet payment system in Bangladesh. American Journal of Economics and Business Innovation, 1(1), 1-10.
10. Azam, S. M. F., Haque, A., Sarwar, A., & Anwar, N. (2014). Training Program Effectiveness of Service Initiators: Measuring Perception of Female Employees of Bank Using Logistic Approach. Asian Research Journal of Business Management, 1(2), 98-108.