International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Analysis and Implementation of SaaS and XDR Based Endpoint Security in the Context of BSI Bank Information Security: Case Study of the Latest Security System

Andika Febryan[1], Henny Widowati Farida[2]
[1,2]Management System Information, Gunadarma University, Jakarta, Indonesia, 10430
Email Address: [1]andika.febrian92(at)gmail.com, [2]widowati(at)staff.gunadarma.ac.id

Abstract— *This study examines the analysis and implementation of endpoint Security based on Software as a Service (SaaS) and Extended Detection and Response (XDR) in the context of information Security at Bank Syariah Indonesia (BSI). The research aims to evaluate the effectiveness of SaaS and XDR-based Security solutions in protecting the bank's information assets from the continuously evolving cyberSecurity threats. The methodology includes analyzing the information Security needs of Bank BSI, evaluating existing SaaS and XDR solutions, and implementing a pilot project for endpoint Security using these technologies. The findings indicate that the integration of SaaS and XDR significantly enhances the detection, analysis, and response to cyberSecurity incidents. Additionally, the study identifies challenges and recommendations for implementing these Security solutions on a larger scale at Bank BSI. This research provides valuable insights for the banking industry in adopting contemporary information Security technologies to safeguard their critical assets and data.*

Keywords— *Extended Detection and Response (XDR), Software as a Service (SaaS), Trendmicro.*

I. Introduction

In May 2023, Bank Syariah Indonesia (BSI) experienced a significant information security incident, where system damage occurred due to a virus attack. This incident prompted the bank to carry out an in-depth evaluation of the security system in all its branches. Currently, the endpoint security system at Bank Syariah Indonesia branches still relies on On-Premise antivirus. However, the use of these antiviruses revealed security gaps and feature limitations, requiring proactive steps to maintain the security and continuity of bank operations. Operational sustainability and customer trust are top priorities, especially considering the vulnerability of security systems to malware attacks and increasingly complex cyber threats. System damage due to this virus attack results in disruption of banking services, reduces productivity, and has the potential to harm the bank's reputation. Therefore, it is necessary to take innovative steps to improve endpoint security at Bank Syariah Indonesia branches.

Antivirus as a Service Software as a Service (SaaS) is an attractive alternative solution, presenting a cloud-based approach to cyber security. SaaS has the advantage of providing active protection against malware, without having to worry about time-consuming manual updates and feature upgrades. On the other hand, Extended Detection and Response (XDR) brings a more holistic security concept, integrating and analyzing data from multiple sources, including endpoints, networks, and applications. By combining SaaS and XDR, On-Premise antivirus migration into a solution, it is expected to provide a higher level of security. This migration, which will be carried out over a period of four months, starting in November 2023 and ending in April 2024, is not only a technology transfer, but also a transformation of information security at Bank Syariah Indonesia. SaaS's advantages in malware detection and prevention will combine with XDR's ability to provide holistic context, enabling rapid response to security incidents by understanding attacks from multiple angles.

It is expected that within four months, the integration of SaaS and This step will not only prevent a recurrence of system damage due to the virus, but also ensure that Bank Syariah Indonesia can continue to operate safely and provide the best service to its customers.

II. Literatur Review

Collecting information, studying the theoretical basis and research that implements the XDR system. There are 5 similar studies that have been described previously, of which the five different studies are related to the context of improving cyber security, especially in terms of detection and response to increasingly complex threats. The following is the relationship between these studies:

1. Improved Cyber Security, All research highlights the importance of improving cyber security amidst increasingly complex threats. Dedi Soleman and Benfano Soewito (2024) and Seung Jae Yo (2019) both emphasize the importance of more advanced technologies such as XDR and proactive endpoint security solutions to deal with growing threats.
2. Technology and Security Integration, Research by Dedi Soleman and Benfano Soewito (2024) and A. Shaji George et al. (2021) similarly focus on the use of XDR technology to improve integration and automation in cyber security systems. Both highlight how XDR can overcome the limitations of traditional systems and provide a more integrated view of threats.
3. Early Detection and Quick Response, Nazar Firman Pratama (2023) and Dedi Soleman and Benfano Soewito (2024) emphasize the importance of early detection systems and rapid response to cyber threats. The use of SIEM and Wazuh in Nazar Firman Pratama's research is in line with the concept of early

detection which is also promoted in the application of XDR and EDR in Dedi Soleman and Benfano Soewito's research.

4. Comprehensive Protection, Research by Maria Paschalidou et al. (2023) and A. Shaji George et al. (2021) shows the importance of comprehensive cyber protection in dealing with threats to national security and key infrastructure. Both studies highlight the need for a comprehensive and integrated strategy to protect systems from various types of threats.

5. Use of Latest Technology, All five studies emphasize the importance of using the latest technology in cyber security. Seung Jae Yo (2019) highlights the growth of IoT and the need for better endpoint security, while other research emphasizes the importance of XDR and early detection technologies as modern solutions to evolving threats.

Overall, the main link between these five studies is the focus on improving and integrating more sophisticated and effective cyber security technologies to deal with increasingly complex and varied threats. Each study contributes to a better understanding of how technologies such as XDR, EDR, SIEM, and proactive approaches can be used to strengthen cyber security systems in various contexts.

III. Methodology

A. Specific

The specific stage of this research is identifying and analyzing the security system needs of Bank Syariah Indonesia. This includes an evaluation of possible malware threats, as well as an in-depth understanding of the existing security landscape in the bank environment. Identification of Security System Needs, research will begin by identifying and analyzing security system needs at Bank Syariah Indonesia. This will include an evaluation of possible malware threats, as well as an in-depth understanding of the existing security landscape in the bank environment. Evaluation of SaaS anti-malware solutions and

Additionally, it will explain how XDR concepts can be applied and activated to improve detection and response to malware threats. Performance data collection and analysis, during the implementation process, the research will collect data regarding the performance of SaaS and XDR anti-malware solutions in detecting and responding to malware threats.

B. Measurable

This research aims to assess research success through measurable performance indicators, including reduction in malware incidence, response time to threats, and detection success rate by SaaS and XDR Anti-Malware solutions. Decrease in malware incidents, the study will use historical data on malware incidents before and after the implementation of security solutions to measure the decrease in incidents. By comparing the number and types of incidents before and after implementing SaaS and XDR Anti-Malware solutions, it can be identified whether the solutions are effective in reducing the risk of malware attacks. Response time to threats, response time to threats will be measured from the time of detection to the response time taken by the Bank Syariah Indonesia IT security team. Response time data before and after the implementation of the security solution will be compared with the transmission of whether the Anti-Malware SaaS and XDR solutions can help in detecting and responding to threats more quickly and efficiently.

Detection Success Rate: the detection success rate by Anti-Malware SaaS and XDR solutions will be measured by calculating the number of threats successfully detected by the solution compared to the total threats detected. By analyzing the detection success rate, you can evaluate the extent to which the security solution is able to identify incoming threats in an accurate and timely manner.

By using these performance indicators, research will be able to provide a deeper understanding of the effectiveness of Anti-Malware SaaS and XDR solutions in increasing the security level of the Indonesian Syariah Bank system. The results of this evaluation will be an important basis for decision making regarding the development and improvement of security systems in the future.

C. Achievable

The Achievable stage of this research is to ensure that the research can be achieved through the process of identifying and implementing SaaS and XDR Anti-Malware solutions that suit the organization's needs. The first step in achieving the objectives of this research is to conduct an in-depth analysis of the security needs and risks faced by Bank Syariah Indonesia. By understanding existing threats and the banking IT infrastructure, the most suitable Anti-Malware SaaS and XDR solutions can be identified. Furthermore, with the availability of the right technology, namely Anti-Malware SaaS and XDR solutions, as well as adequate resource support, this research can be carried out successfully. This includes selecting a trusted and proven solution provider, as well as allocating sufficient human and financial resources for the implementation and operationalization of security solutions.

In the implementation process, collaboration between the bank's IT security team and the solution provider will be key. The bank's internal team needs to ensure that the IT infrastructure is well integrated with the selected Anti-Malware SaaS and XDR solutions, while the solution provider is responsible for providing the necessary technical support and training. Thus, through a planned approach and supported by appropriate technology and adequate resources. This project has the potential to achieve the goal of increasing the security level of Bank Syariah Indonesia's system through the implementation of Anti-Malware SaaS and XDR solutions.

D. Relevant

This research will use quantitative measures and measurable performance indicators to exemplify the effectiveness of SaaS and XDR Anti-Malware solutions. Solution performance data will be collected and analyzed to provide solution effectiveness in increasing the level of bank system security and reducing the risk of cyber attacks. In a security environment.

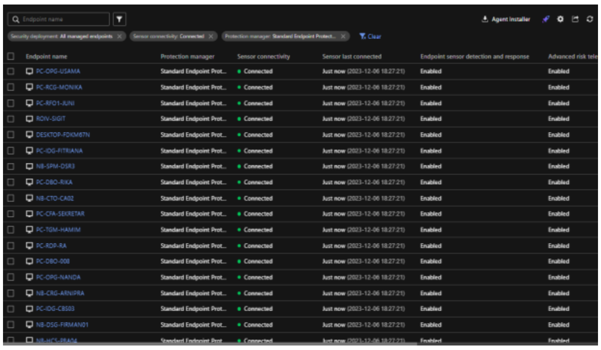
E. Timebound

The Timebound stage of the project is to set a clear timeline for the implementation of the Anti-Malware SaaS and XDR solutions. The implementation process is scheduled to be completed in four months, on or before April 30, 2024. Taking into account realistic timelines and ensuring that deadlines can be achieved without compromising the quality or effectiveness of implementation.

IV. Result

A. *Improved Threat Detection*

In evaluating performance, the first focus is on improvements in the system's ability to detect threats. Evaluation data shows a significant increase in the number and types of threats identified after implementing SaaS and XDR solutions. In-depth statistical analysis confirms these improvements, providing strong evidence of the effectiveness of the adopted security strategy.



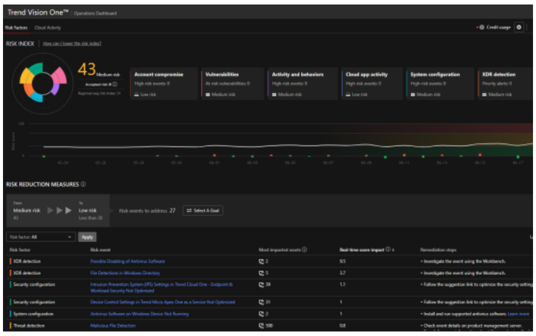
Endpoint name
Agent Installer
Security deployment: All managed endpoints
Sensor connectivity: Connected
Protection manager: Standard Endpoint Protect...
Clear

Endpoint name	Protection manager	Sensor connectivity	Sensor last connected	Endpoint sensor detection and response	Advanced risk tele
PC-OPG-USAMA	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-RCG-MONIKA	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-RFO1-JUNI	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
ROIV-SIGIT	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
DESKTOP-FDKM67N	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-IDG-FITRIANA	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
NB-SPM-OSR3	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-DBO-RIKA	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
NB-CTO-CA02	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-CFA-SEKRETAR	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-TGM-HAMIM	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-RDP-RA	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-DBO-008	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-OPG-NANDA	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
NB-CRG-ARNIPRA	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
PC-IDG-CBS03	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
NB-DSG-FIRMAN01	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled
NB-HCS-PRA04	Standard Endpoint Prot...	● Connected	Just now (2023-12-06 18:27:21)	Enabled	Enabled

Fig. 1. Dashboard XDR Endpoint

B. *Positive Impact on System Integrity*

The evaluation results also include an assessment of the resulting positive impact on the integrity of the entire system. Improved security and rapid response to threats contribute to reduced security incidents and system vulnerabilities. This data provides a holistic picture of how implementing SaaS and XDR antivirus solutions positively impacts system operational integrity and sustainability. Below is a display of the Application Dashboard menu which displays the risk factors currently affecting the environment at Bank Syariah Indonesia. This dashboard provides detailed information regarding various risk events originating from these risk factors. Apart from that, there is also a list of affected assets along with their scores, which shows the severity of the impact on each asset. For each risk factor, mitigation steps are included that need to be taken to remediate and reduce the risk. These mitigation measures are designed to strengthen security and ensure operational continuity.



Risk factor	Risk event	Most impacted assets	Real-time score impact	Remediation steps
XDR detection	Possible Disabling of Antivirus Software	2	9.5	• Investigate the event using the Workbench.
XDR detection	File Detections in Windows Directory	5	3.7	• Investigate the event using the Workbench.
Security configuration	Intrusion Prevention System (IPS) Settings in Trend Cloud One - Endpoint & Workload Security Not Optimized	39	1.1	• Follow the suggestion link to optimize the security setting
Security configuration	Device Control Settings in Trend Micro Apex One as a Service Not Optimized	31	1	• Follow the suggestion link to optimize the security setting
System configuration	Antivirus Software on Windows Device Not Running	2	1	• Install and run supported antivirus software. Learn more
Threat detection	Malicious File Detection	500	0.8	• Check event details on product management server.

Fig. 2. Operation Dashboard

C. *Analysis of Trial Results Data*

In addition, the test results are described and analyzed in depth. These data include test scenarios that have been designed before implementation. Analysis of the test results provides additional insight into the extent to which SaaS and XDR antivirus solutions can engage and respond to situations that may occur in daily operational environments. Through this comprehensive performance evaluation, a comprehensive picture can be produced of the extent to which the implementation of SaaS and XDR antivirus solutions has succeeded in achieving the security objectives set out in the action plan. Evaluate the effectiveness of SaaS solutions in detecting and addressing security threats. This includes malware detection rates, the ability to identify behavior-based attacks, and rapid response to threats.

1 *Malware detection rate*

In facing increasingly complex and varied threats, continuous evaluation of malware detection levels is crucial for Bank Syariah Indonesia. This evaluation includes an analysis of the security solution's ability to identify various types of malware, from conventional viruses to emerging threats with more sophisticated tactics. Through data collection and analysis, the Bank can assess the effectiveness of security solutions in detecting file-based and non-file-based attacks, as well as responding quickly and timely to attacks. The results of this evaluation not only provide a better understanding of the reliability of current security solutions, but also provide a foundation for customizing security strategies that can improve detection capabilities, minimize risks, and protect organizational assets from evolving security threats. Following are the details:

December 2023:

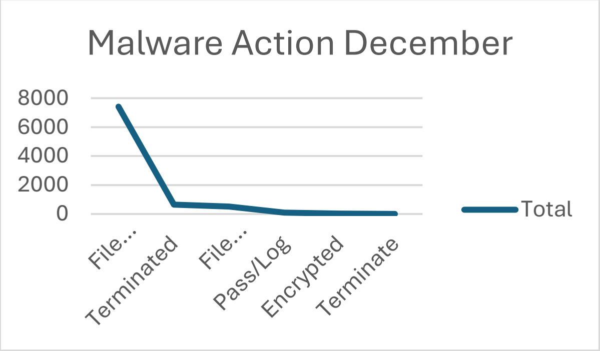


Fig. 3. Malware Action December

Total Files Cleaned, 7,414 files successfully cleaned from malware infection.

Files Deprecated, 639 files were discontinued to prevent further distribution.

Quarantined Files, 518 files were quarantined for further analysis.

Encrypted Files, 26 files were found to have been encrypted by malware.

January 2024 :

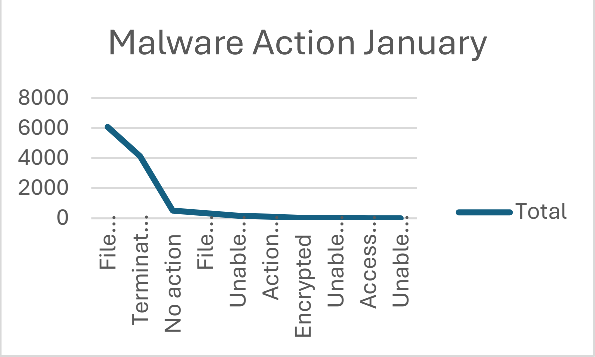


Fig. 4. Malware Action January

Total Files Cleaned, 6,079 files successfully cleaned of malware infection.

Files Deprecated, 4,125 files were stopped completely to prevent further distribution.

Files Without Action, 506 files received no action, risking system security.

Quarantined Files, 342 files were quarantined for further analysis to understand the source and nature of the attack.

Files Could Not Be Uploaded, 165 files could not be uploaded, indicating possible damage to the system.

Endpoints Requiring Restart, 118 endpoints required further action in the form of a restart to complete the cleanup process.

Encrypted Files, 16 files were found to have been encrypted by malware, hindering data recovery.

February 2024 :

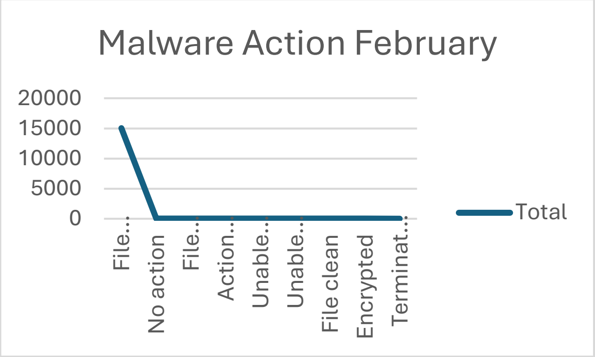


Fig. 5. Malware Action February

Total Files Cleaned, 15,036 files successfully cleaned from malware infection.

No Action Files, 55 files received no action, increasing the risk to system security.

Quarantined Files, 53 files were quarantined for further analysis to understand the source and nature of the attack.

Endpoints Requiring Restart, 48 endpoints required further action in the form of a restart to complete the cleanup process.

Files Could Not Be Uploaded : 42 files could not be uploaded, indicating possible damage to the system.

Files Could Not Be Cleaned, 23 files could not be cleaned of infection, demonstrating the complexity and resilience of the malware.

Files Cleaned Successfully, 6 files were successfully cleaned of infection, indicating there is hope of successful data recovery.

Conclusion:

There was a significant increase in the number of files cleaned in February compared to December and January. A spike in malware attack activity in January demonstrated the need for rapid response and more intensive preventive measures. In-depth analysis of quarantined and unuploadable files is critical to further understand and address threats. The successful cleanup of some files in February demonstrated the effectiveness of some security solutions in dealing with more complex threats.

2 *Response to Threats*

Effectiveness of Malware Cleaning, In December 2023, Trendmicro Apex One SaaS successfully cleaned 7,414 files infected with malware. This number decreased slightly in January 2024, with 6,079 files successfully cleaned, but increased significantly in February 2024 with a total of 15,036 files successfully cleaned.

Terminated Files, In December 2023, a total of 639 files were retired to prevent further spread of the malware. This number increased sharply in January 2024, with 4,125 files having to be retired. Data for February 2024 is not available for this category.

Quarantined Files, a total of 518 files were quarantined in December 2023 for further analysis. This number decreased to 342 files in January 2024 and further decreased to 53 files in February 2024.

Files that cannot be uploaded or cleaned, in January 2024, there were 165 files that could not be uploaded, and in February 2024, this number had decreased to 42 files. Additionally, in February 2024, 23 files were recorded that could not be cleaned of malware infection.

Files Encrypted by Malware, in December 2023, 26 files were found to have been encrypted by malware. This number decreased to 16 files in January 2024. Data for February 2024 is not available for this category.

Endpoints that Require Restart, in January 2024, 118 endpoints required a restart to complete the security threat cleanup process. This number decreases to 48 endpoints in February 2024.

Files Without Any Action, as of January 2024, there were 506 files that had received no action, potentially posing a risk to system security. This number dropped drastically to 55 files in February 2024.

Overall, the data shows increased effectiveness in response to malware threats from December 2023 to February 2024. Bank Syariah Indonesia has succeeded in increasing malware cleaning, reducing the number of files that cannot be uploaded or cleaned, and reducing the need for endpoint restarts. This shows that the security strategies implemented are increasingly effective in dealing with complex and varied threats.

3 *Performance Benchmarking with On – Premises*

In December 2023, Trendmicro On-Premises security systems successfully cleaned 7,414 malware-infected files and stopped 639 files to prevent further spread. Additionally, 518 files were quarantined for further analysis, and 26 files were found to have been encrypted by malware.

In contrast, after migrating to Trendmicro SaaS (Apex One), there was a significant improvement in the effectiveness of malware detection and removal. In January 2024, despite a spike in malware attacks, Trendmicro SaaS successfully cleaned 6,079 infected files, terminated 4,125 files, and quarantined 342 files for further analysis. Additionally, only 16 files were found to have been encrypted by malware, demonstrating improvements in early detection and encryption prevention.

In February 2024, Trendmicro SaaS demonstrated further improvement by cleaning 15,036 malware-infected files. The number of files that could not be uploaded decreased from 165 in January to 42, and files that could not be cleaned decreased to 23, indicating better system stability. Additionally, the number of endpoints requiring restarts decreased from 118 in January to 48 in February, demonstrating improved operational efficiency.

With an On-Premises system, there is no data available regarding files that could not be uploaded or cleaned, as well as the number of endpoints that required a restart. However, data from Trendmicro SaaS shows a significant decrease in the number of files without action, from 506 in January to 55 in February, indicating a better automated response to threats.

Overall, the Trendmicro SaaS (Apex One) integration provides clear improvements in performance and operational efficiency over on-premises solutions. Improvements in malware detection and removal, a decrease in files that cannot be uploaded or cleaned, and a decrease in the need to restart endpoints indicate a better ability to address threats automatically and proactively. This proves that cloud-based solutions are more effective in dealing with increasingly complex and dynamic malware threats.

V. Conclusions and Recommendations

A. Conclusion

Based on the implementation steps for endpoint security using Antivirus Software as a Service (SaaS) and Extended Detection and Response (XDR) solutions have shown positive results in significantly increasing the level of security. Performance evaluation during the implementation process provides a deep understanding of the effectiveness of these solutions and provides a strong foundation for continuous improvement in security strategies.

Implementation of SaaS and XDR Antivirus Solutions, The implementation process begins with the deployment of a SaaS antivirus solution that provides protection against malware and virus threats in real-time across all device endpoints. The addition of XDR broadens the security scope by providing more advanced detection of more complex attacks, including zero-day attacks and behavior-based threats.

Performance Evaluation During Implementation, during implementation, various performance metrics are periodically evaluated, including detection rate, response time to threats, and impact on system performance. Through analysis of evaluation data provides valuable insight into the effectiveness of security solutions and identifies areas where further improvements are needed.

Improved Security and Adaptation Foundations, Performance evaluation results form the foundation for continuous improvements in security strategies. Information obtained from evaluations is used to adjust security solution configurations and improve detection and response capabilities. Implementing a continuous learning cycle ensures that security strategies are always relevant and adaptive to new threats as they arise. Through implementation steps, performance evaluation, and continuous adaptation, this research makes significant contributions to understanding and improving endpoint security. With this strong foundation, organizations can continue to protect their infrastructure from evolving security threats by adopting a proactive and responsive approach.

B. Suggestion

Periodic Monitoring and Evaluation, this suggestion emphasizes the importance of regular system monitoring and evaluation. Conducting regular reviews of the effectiveness of SaaS and XDR antivirus solutions, as well as general security performance, will allow for early detection of potential issues and quick adjustments.

Security Training and Awareness, continue training efforts and increase security awareness among end users. User engagement in understanding security policies, as well as how to use security solutions, is an ongoing investment to prevent security incidents caused by human error.

Testing on a Larger Scale, testing the solution on a larger scale and in various organizational environments to ensure its scalability and effectiveness. This includes testing across various industry sectors that have different security needs.

Improved Integration with Other Security Systems, research ways to improve integration between SaaS and XDR antivirus solutions with other security systems such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Comparative Study with Other Solutions, conduct comparative studies between SaaS and XDR antivirus solutions with other endpoint security solutions. This will provide insight into the relative advantages and disadvantages of various approaches.

References

[1] Waterson, D. (2020). Managing endpoints, the weakest link in the Security chain. Network Security, 2020(8), 9–13. https://doi.org/10.1016/s1353-4858(20)30093-3

[2] Yanto, S. (2023). New normal Dan Entrepreneur Bidang Keamanan Cyber. PROSIDING, 3, 64–71. https://doi.org/10.59134/prosidng.v3i.336.

[3] Chandel, Sonali & Yu, Sun & Yitian, Tang & Zhili, Zhou & Yusheng, Huang. (2019). Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat. 81-89. 10.1109/CyberC.2019.00023.

[4] Sapdiaz, M., Panggabean, T. E., & Tarigan, I. J. (2023). Building E-Learning Application Using Cloud Computing with Software as a Service (SAAS) Model. Anti Virus, 17(1), 123–134. https://doi.org/10.35457/antivirus.v17i1.3172

[5] Kurniawati, A., & Ardiansyah, A. (2020). Analisis Performa Perangkat Lunak Antivirus Dengan Menggunakan Metodologi Pengukuran Performance. Jurnal Ilmiah Matrik, 22(1), 43–54. https://doi.org/10.33557/jurnalmatrik.v22i1.838

[6] George, A., George, A. S. H., Baskar, T., & Pandey, D. (2021). XDR: The evolution of Endpoint Security Solutions - superior extensibility and analytics to satisfy the organizational needs of the future. International

Journal of Advanced Research in Science, Communication and Technology, 493–501. https://doi.org/10.48175/ijarsct-1888

[7] Richings, D. (2022). Rethinking endpoint management for the modern age. Network Security, 2022(10). https://doi.org/10.12968/s1353-4858(22)70060-8

[8] Soleman, D., & Soewito, B. (2024). Information Security System Design Using XDR And EDR. Inform : Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi, 9(1), 51-57. https://doi.org/10.25139/inform.v9i1.7331

[9] Nazar, F. (2023). Perancangan Sistem Deteksi Dini Keamanan Informasi DISKOMINFOKabupaten Bandung. Jurnal Teknik Informatika dan Sistem Informasi, 808-820.

[10] Kalogiannidis, S.; Paschalidou, M.; Kalfas, D.; Chatzitheodoridis, F. Relationship between Cyber Security and Civil Protection in the Greek Reality. Appl. Sci. 2023, 13, 2607. https://doi.org/10.3390/app13042607

[11] Yoo, Seung Jae (2019) . Study on Improving Endpoint Security Technology. Department of Information Security, Joongbu University.