Jurnal Sistem Informasi dan Ilmu Komputer
Volume. 2 No. 2 Mei 2024
e-ISSN: 2986-4976; dan p-ISSN: 2986-5158, Hal. 113-121
DOI: https://doi.org/10.59581/jusiik-widyakarya.v2i2.3994
Available online at: https://journal.widyakarya.ac.id/index.php/jusiik-widyakarya

Strategi Pengembangan Sistem Operasi Windows untuk Memperkuat Proteksi Windows terhadap Ancaman Malaware

Rakhmadi Rahman, M. Faiz Ilyas, Muhammad Alfarizky Yusuf
[123]Program Studi Sistem Informasi Institut Tekhnologi BJ Habibie, Indonesia

Alamat: Kampus 1 Jalan Balai Kota No.1 & Kampus 2 Jalan Pemuda No.6 Kota Parepare, Sulawesi Selatan, Indonesia
Koresprodensi Penulis : muhammadfaizilyas750@gmail.com

Abstract. *Behind the widespread proliferation of malware, IT experts have developed robust security systems to minimize the risk of malware infection. In the Windows security system, numerous software solutions have been created to prevent malware threats, including Windows Defender, which serves as the core of Windows security, virus & threat protection, real-time protection, firewall & network protection, account protection, and many more. This study uses a qualitative approach based on literature review. The results indicate that by integrating machine learning technology, enhancing security features, and adopting a layered approach, the strategy for developing the Windows operating system has successfully strengthened protection against malware threats. These measures not only improve the ability to detect and respond to threats but also ensure that users can enjoy a safe and protected computing experience.*
Keywords: *Malware, Proteksi windows, Ancaman malware*

Abstrak. Dibalik maraknya penyebaran malware, tentu saja para ahli dibilang IT membuat sebuah sistem keamanan yang kuat untuk meminimalisir risiko terkena malware. Pada sistem keamanan windows, sudah banyak perangkat lunak yang diciptakan untuk mencegah ancaman malware, diantaranya Windows defender yang merupakan induk atau inti dari sistem keamanan windows, virus & threat protection, real-time protection, firewall & network protection, account protection dan masih banyak lagi. Penelitian ini menggunakan pendekatan kualitatif berbasis studi literatur. Hasil penelitian menunjukkan dalam penggabungkan teknologi machine learning, peningkatan fitur keamanan,dan pendekatan berlapis, strategi pengembangan sistem operasi Windows berhasil memperkuat proteksi terhadap ancaman malware. Langkah-langkah ini tidak hanya meningkatkan kemampuan deteksi dan respons terhadap ancaman, tetapi juga memastikan bahwa pengguna dapat menikmati pengalaman komputasi yang aman dan terlindungi
Kata kunci: Malware, Proteksi windows, Ancaman malware

1. LATAR BELAKANG

Di era digital sekarang, keamanan computer sekarang merupakan suatu hal yang sangat penting. Transformasi sistem menjadi sangat penting ketika teknologi baru muncul dan memiliki potensi untuk meningkatkan kinerja sistem yang ada. Terlebih lagi di dalam komputer menjadi tempat penyimpanan data-data penting, baik itu berupa data pribadi, data Perusahaan, ataupun data-data lainnya. Tentu saja data tersebut memiliki sebuah informasi, yang Dimana informasi adalah data yang diolah agar menjadi lebih berguna dan sangat berartu yang menerimanya (Adhikari, & Sharma, 2020)

Namun, dibalik canggihnya teknologi di zaman sekarang, muncul orang-orang yang tidak bertanggung jawab dengan membuat software jahat dengan tujuan ingin mencuri data-data

Received Maret 12, 2024; Received Maret 28, 2024; Accepted April 24, 2024; Published Mei 30, 2024
** Rakhmadi Rahman, muhammadfaizilyas750@gmail.com*

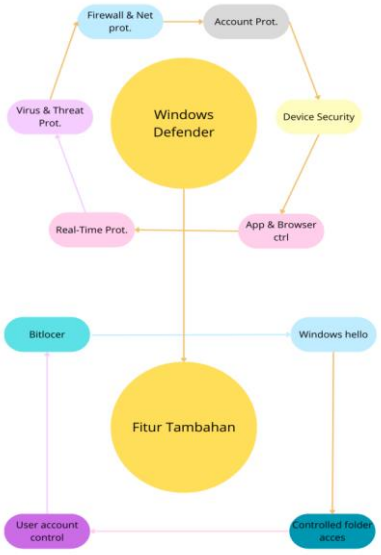
informasi, merusak sistem dan masih banyak lagi. Malware merupakan software jahat yang ingin mencuri data-data penting, bahkan orang yang membuat malware tidak segan-segan untuk merusak device seseorang. Terlebih lagi, windows merupakan target dalam penyebaran malware di sistem operasi windows (Prasetyo & Wahyudi, 2021)

Dibalik maraknya penyebaran malware, tentu saja para ahli dibilang IT membuat sebuah sistem keamanan yang kuat untuk meminimalisir risiko terkena malware. Pada sistem keamanan windows, sudah banyak perangkat lunak yang diciptakan untuk mencegah ancaman malware, diantaranya Windows defender yang merupakan induk atau inti dari sistem keamanan windows, virus & threat protection, real-time protection, firewall & network protection, account protection dan masih banyak lagi (Adhikari & Sharma, 2020). Macam-macam proteksi windows, sudah pastinya memiliki tugas yang berbeda akan tetapi memiliki tujuan yang sama yaitu untuk melindungi sistem operasi windows dari ancaman malware.

Di samping banyaknya jenis-jenis dari keamanan windows, tentu saja tidak menjamin terlindungi sepenuhnya dari ancaman malware. Maka dari itu, perlunya fitur-fitur tambahan untuk lebih memperkuat proteksi keamanan windows, seperti User Account Control (UAC), BitLocker dan masih banyak lagi fitur-fitur tambahan untuk memperkuat proteksi windows.

Keamanan sistem operasi merupakan ilmu yang berfokus pada perlindungan sebuah sistem komputer dari ancaman malware yang dapat merusak dan mengambil data-data informasi (Susanto & Setiawan, 2022). Sistem operasi windows adalah sistem operasi yang paling banyak digunakan, dari itu sistem operasi windows memerlukan tingkat keamanan yang tinggi untuk mencegah terjadinya risiko pembobolan data dan untuk memberikan rasa aman dan nyaman kepada pengguna. Malicious software atau yang biasa dikenal dengan sebutan malware merupakan software jahat yang dirancang untuk mengganggu dan merusak sebuah sistem operasi. Malware mempunyai beragam jenis seperti virus, worm, trojan, ransomware, spyware, dan masih banyak lagi (Wijaya, & Nugroho, 2023).

Sistem operasi windows sudah dilengkapi dengan fiur-fitur keamanan, tetapi ancaman malware masih tetap ada. Dari itu, proteksi windows diberikan fitur-fitur keamanan tambahan seperti BitLocker, User Account Control (UAC), controlled folder acces, dan windows hello. Yang dimana fitur ini bertujuan untuk membuat lapisan keamanan keamanan windows.



Gambar 2.1 diagram

Windows defender merupakan salah satu proteksi utama windows dalam hal mencegah terjadinya ancaman malware. Yang dimana windows defender dan fitur tambahan saling bekerja sama dalam hal melindungi sistem operasi, windows defender merupakan pusat kontrol dari semua sistem keamanan seperti virus & threat protection, firewall & nerwork protection dan lain masih banyak lagi. Contohnya real-time protection dan virus &threat protection yang bekerja sama dalam melindungi sistem operasi secara terus-menerus.

2. METODOLOGI

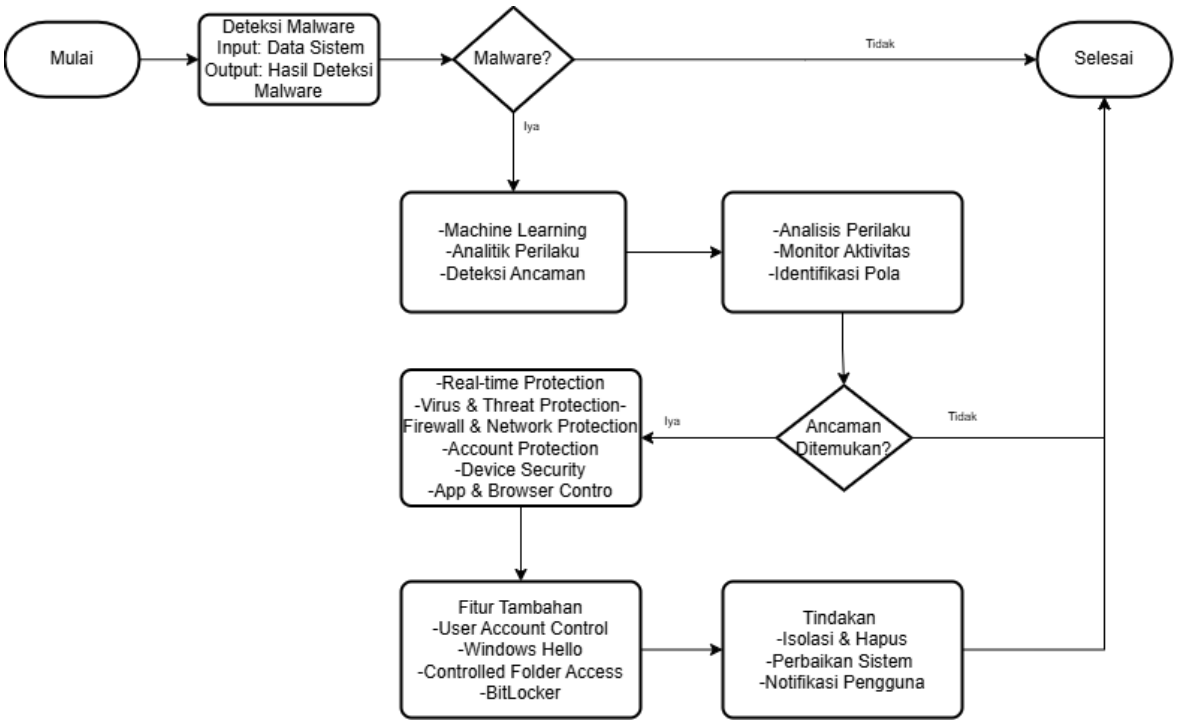
Metode yang digunakan pada judul "strategi pengembangan sistem operasi windows untuk memperkuat protuksi windows terhadap ancaman malware" adalah metodologi penilitian kualitatif berbasis studi literatur. Dengan mengambil judul seperti ini, tentunya memerlukan pemahaman yang lebih mendalam karena melibatkan banyak aspek teknis dan non-teknis. Dan ketika ingin menguji sistem operasi dan keamanan *cyber* tentunya memerlukan sumber daya yang besar dan membutuhkan waktu yang lama. Sedangkan studi literatur hanya memanfaatkan penilitian yang sudah ada dan tidak membutuhkan waktu yang lama, tetapi hanya dengan mengakses sumber terpercaya seperti jurnal , artikel, buku dan sumber-sumber terpercaya lainnya yang membahas mengenai proteksi windows dari ancaman malware.

3. HASIL DAN PEMBAHASAN

1. Cara Kerja Sistem Keamanan Dalam Bentuk Flowchart

Metode kualitatif yang berbasis literatur merupakan metode yang digunakan untuk mengembangkan dan memperkuat proteksi windows dengan cara memanfaatkan penilitian yang sudah ada untuk dikembangkan lagi melalui referensi yang terpercaya seperti jurnal, artikel, dan buku.

Pengembangan ini dilakukan karena windows merupakan sistem operasi yang sangat banyak digunakan dan windows sering menjadi target dari ancaman sebuah malware, maka diperlukan pengembangan dan memperkuat sistem keamanannya. Berikut contoh pengoperasian dalam bentuk flowchart:

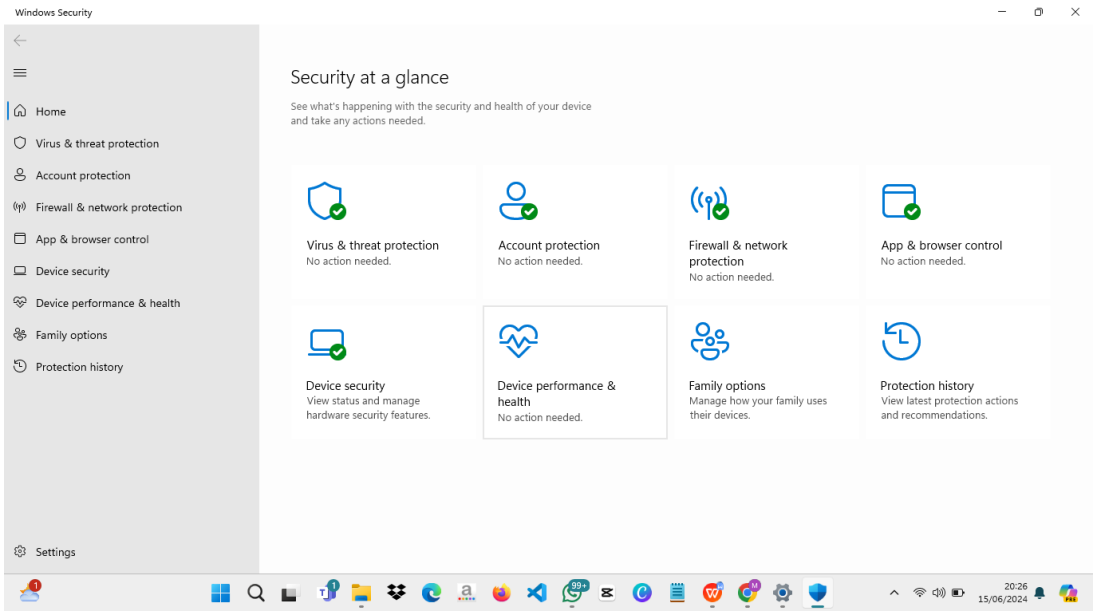


Gambar 4.1 flowchart

Flowchart ini menjelaskan bagaimana cara sistem bekerja ketika mendapat suatu ancaman dari malware. Ketika sistem mendeteksi adanya ancaman malware, maka program akan berjalan sesuai dengan tugasnya dan akan dibantu oleh program-program tambahan.

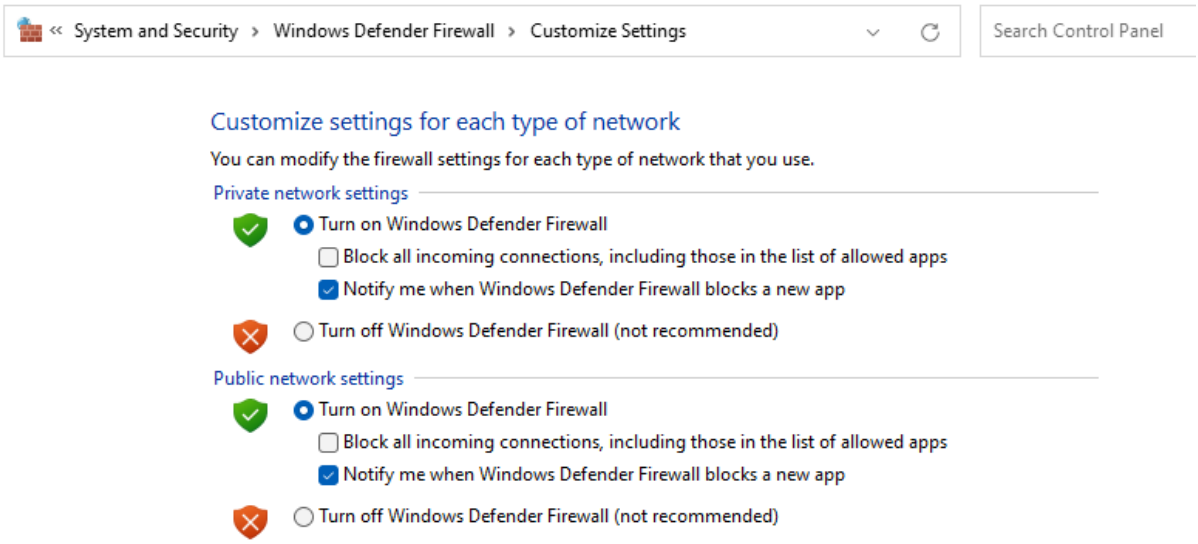
2. Konsep UI/UX

Adapun salah satu contoh keamanan proteksi windows adalah firewall & network protection, yang dimana teknologi firewall dapat digunakan untuk melindungi jaringan dengan memasangnya secara strategis di satu titik layar keamanan dimana jaringan pribadi atau internet terhubung ke internet publik. Firewall juga dapat mengisolasi sub-jaringan guna memberikan sebuah lapisan keamanan tambahan.



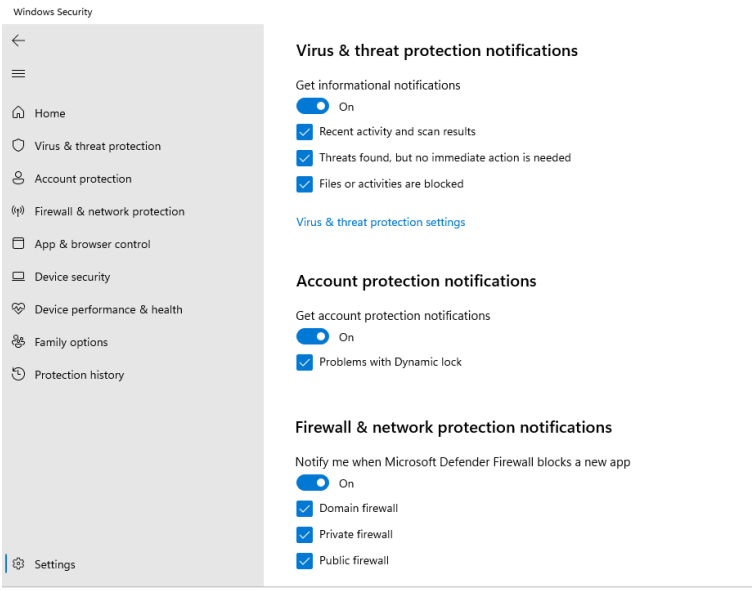
Gambar 4.2 tampilan UI

Ini adalah tampilan *home* ketika user ingin masuk ke fitur firewall. Tetapi cara masuk ke fitur firewall ada 2 cara, yang pertama masuk melalui ***settingan*** kemudian pilih opsi ***privacy & security*** lalu pilih lagi opsi ***windows security***. Atau user bisa juga searching ***windows defender firewall.***



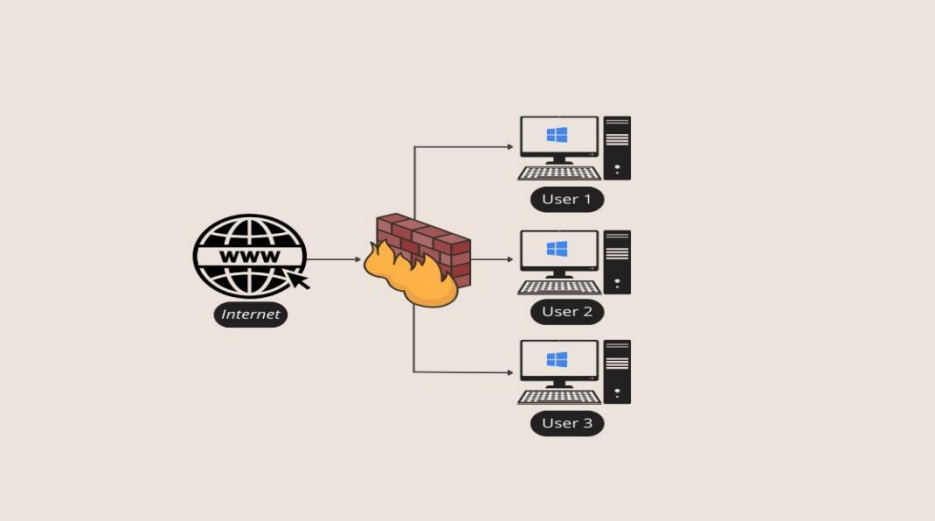
Gambar 4.3 tampilan UX

Di dalam gambar diatas terdapat 2 pilihan , ada private network settings dan ada juga public network settings. Kedua opsi tersebut tentunya berbeda, private network settings lebih di anggap aman, seperti jaringan wifi dirumah dan dikantor, dengan adanya private network setting, diharapkan berada pad a lingkungan yang aman dan terlindungi. Sedangkan public network settings lebih dianggap tidak aman, seperti wifi di kafe, bandara dan tempat umum lainnya.



Gambar 4.4 tampilan UX

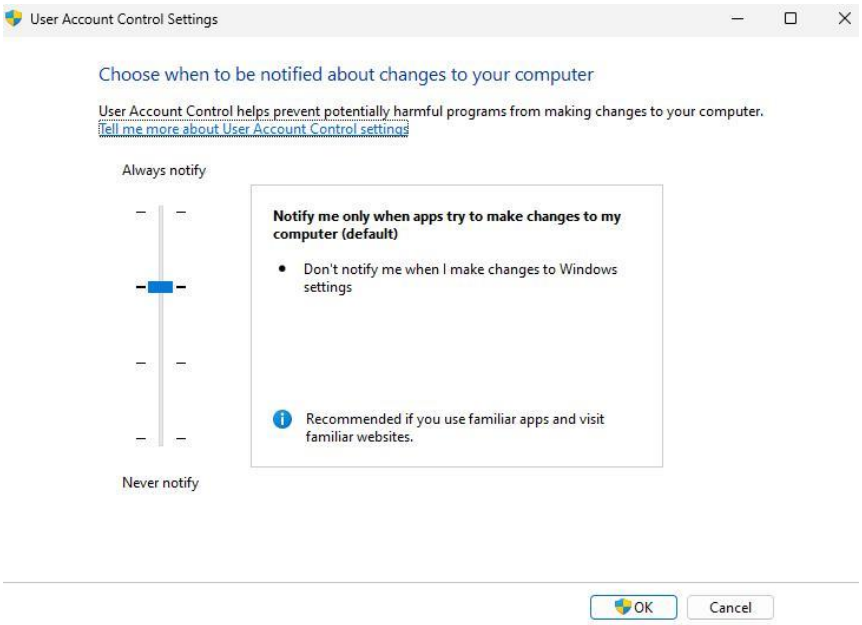
User bisa mengaktifkan notifikasi agar sistem memberitahu ketika ada aplikasi baru yang di blokir dan ketika ada ancaman malware.



Gambar 4.5 ilustrasi firewall

Ini adalah ilustrasi bagaimana ketika firewall bekerja. Dimana setiap internet yang ingin masuk ke jaringan komputer pasti akan melewati firewall dulu untuk mengantisipasi jaringan-jaringan yang tidak aman. Komputer yang ke terhubung jaringan internal agar dilindungi firewall, dan firewall memastikan hanya jaringan-jaringan yang mendapatkan izin saja yang boleh masuk.

Adapun salah satu contoh penggunaan dari fitur tambahan untuk lebih memperkuat keamanan sistem adalah User Account Control (UAC). UAC merupakan sistem keamanan yang sudah ada sejak zaman windows vista, yang dimana UAC bertujuan untuk mencegah malware untuk merusak komputer atau perangkat. Berikut adalah tampilan dari User Account Control:



Gambar 4.6 tampilan UAC

Di tampilan ini, user diperlihatkan 4 macam tingkatan. Tingkatan ke-4 atau yang paling atas, komputer akan terus memberikan notifikasi ketika ada software baru yang di instal dan ketika ada perubahan pengaturan di dalam komputer. Selanjutnya, tingkatan ke-3 komputer hanya memberitahu ketika ada aplikasi yang ingin mengubah pengaturan. Tingkatan ke-2, ini untuk meredupkan dekstop komputer. Dan terakhir pada tingkatan ke-1, dimana komputer tidak akan memberikan notifikasi biarpun ketika menginstal aplikasi atau membuat perubahan di komputer.

3. KESIMPULAN

Dengan menggabungkan teknologi machine learning, peningkatan fitur keamanan,dan pendekatan berlapis, strategi pengembangan sistem operasi Windows berhasil memperkuat proteksi terhadap ancaman malware. Langkah-langkah ini tidak hanya meningkatkan kemampuan deteksi dan respons terhadap ancaman, tetapi juga memastikan bahwa pengguna dapat menikmati pengalaman komputasi yang aman dan terlindungi. Strategi yang komprehensif dan adaptif ini adalah kunci untuk menghadapi tantangan keamanan di masa depan dan menjaga integritas serta keamanan sistem operasi Windows.

.

DAFTAR PUSTAKA

Adhikari, B., & Sharma, S. (2020). Analisis Strategi Keamanan Windows 10 Terhadap Ancaman Malware. *Jurnal Teknologi dan Keamanan Siber, 8(2)*, 125-134.

Prasetyo, A., & Wahyudi, R. (2021). Implementasi Teknologi Windows Defender dalam Meningkatkan Keamanan Sistem Operasi Windows. *Jurnal In formatika dan Keamanan Jaringa*, 10(1), 57-64.

Susanto, H., & Setiawan, I. (2022). Evaluasi Kebijakan Keamanan pada Sistem Operasi Windows untuk Perlindungan terhadap Malware. *Jurnal Riset Teknologi dan Informasi*, 15(3), 203-212.

Wijaya, M., & Nugroho, B. (2023). Pengembangan Fitur Keamanan Windows 11 dalam Menghadapi Ancaman Malware Modern. *Jurnal Teknologi Informasi dan Komputer*, 13(1), 78-86.