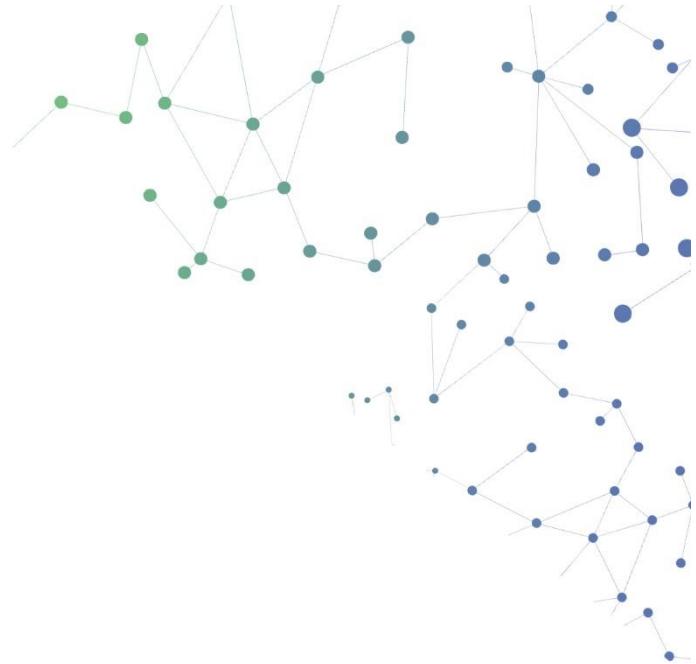




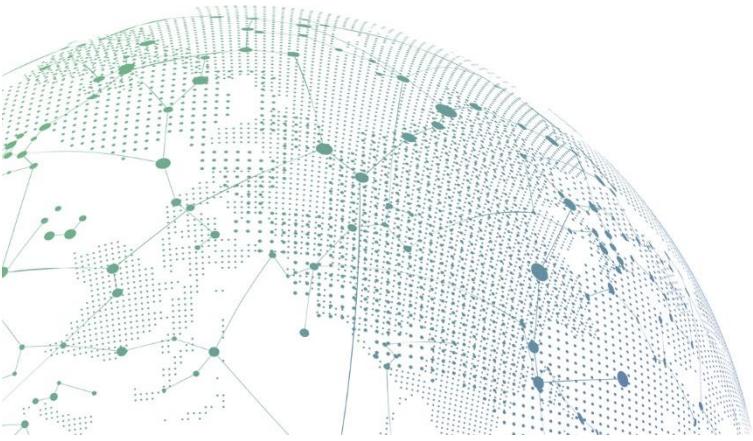
SANGFOR



Endpoint Secure

**Praktik Terbaik untuk Skenario_One Click Kill the
Virus**

Versi 3.2.22



Catatan Perubahan

Tanggal	Deskripsi Perubahan
Feb 25, 2021	Dokumen Terbit.
Mei 17, 2021	Dokumen Diperbarui.

Daftar Isi

Bab 1 Skenario	1
Bab 2 Persiapan	1
2.1 Lingkungan	1
2.1.1 Lingkungan Jaringan	1
2.1.2 Sampel Virus	2
Chapter 3 Proses Demontrasi.....	2
3.1 Pengujian	2
3.1.1 Konten.....	2
3.1.2 Hasil yang diharapkan	2
3.1.3 Langkah-langkah.....	2
3.1.3.1 Pengaturan Policy	3
3.1.3.2 Memulai sebuah Serangan	3
3.1.3.3 Efek Penyerangan	4

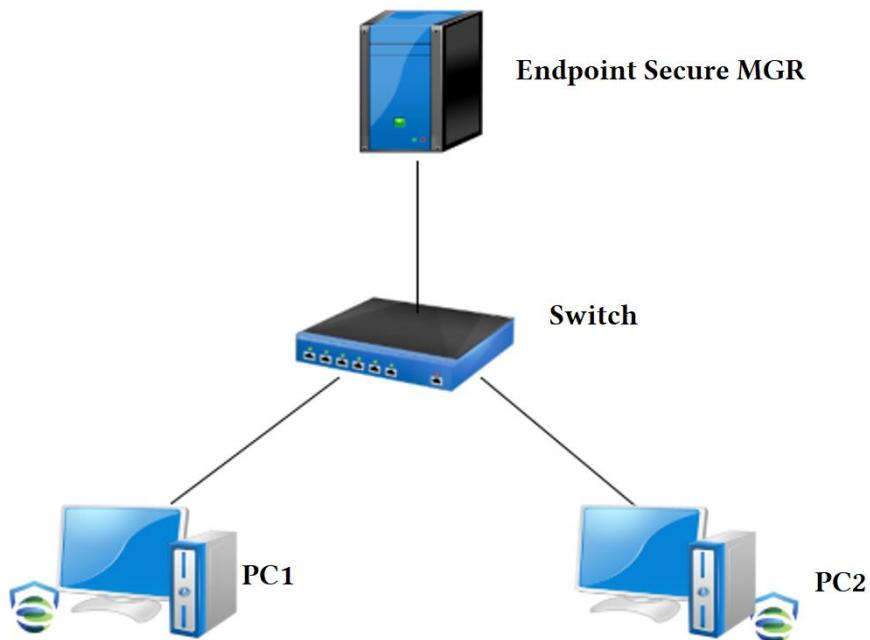
Bab 1 Skenario

Program ini mendemonstrasikan proses dan efek serangan ransomware ketika endpoint tidak menjalankan Endpoint Secure Agent, serta efek deteksi dan perlindungan terhadap serangan ransomware setelah menyebarkan Endpoint Secure Agent. Program ini cocok untuk menunjukkan kustomer bagaimana Endpoint Secure Agent mendeteksi serangan ransomware dan menyediakan perlindungan.

Bab 2 Persiapan

2.1 Lingkungan

2.1.1 Lingkungan Jaringan

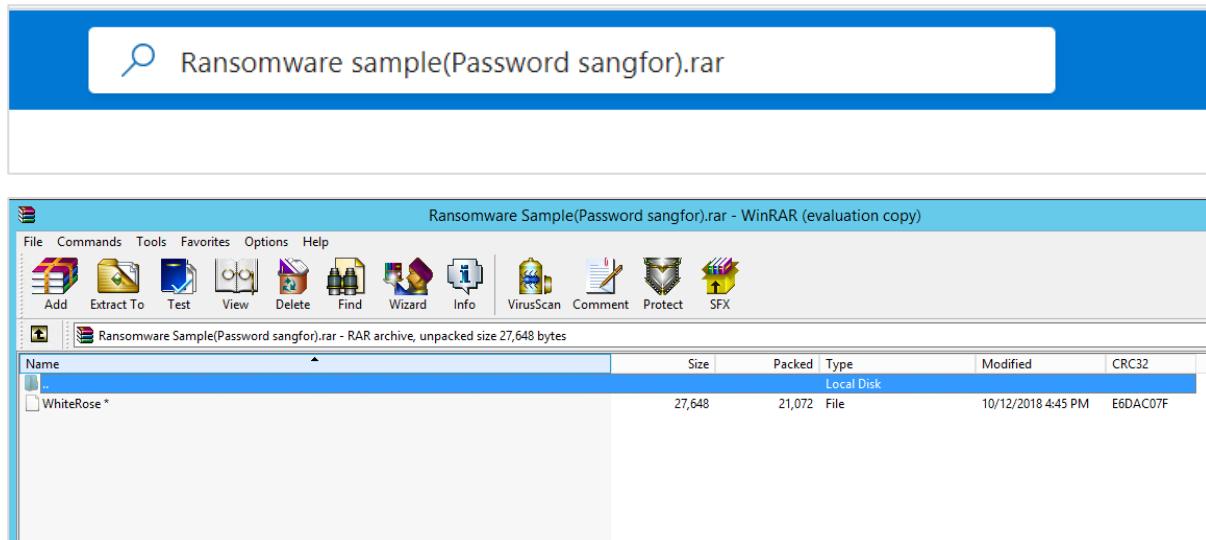


Device	Account/Password	IP	Description
PC1	administrator/111111	20.10.0.3	PC memulai serangan ransomware
PC2	administrator/111111	20.10.0.8	PC diserang oleh ransomware dengan RDP brute-force cracking

MGR	admin/Endpoint Secure@support	20.10.0.100	Endpoint Secure MGR
-----	----------------------------------	-------------	---------------------

2.1.2 Sampel Virus

Sampel Ransomware (Password sangfor).rar dapat digunakan untuk **sampel Ransomware (Password Sangfor).rar**, yang mana dapat diunduh dengan mencari pada PMO tanpa berjalan. Setelah menjalankan real time monitoring dari ES, virus dapat terdeteksi setelah berkas didekompresi.



Chapter 3 Proses Demontrasi

3.1 Pengujian

3.1.1 Konten

Ketika Endpoint Secure mendeteksi berkas virus yang sama pada PC1 dan PC2, maka dapat memperbaiki berkas virus yang sama pada PC1 dan PC2 dengan satu kali klik.

3.1.2 Hasil yang diharapkan

Kalian dapat melihat insiden keamanan pada PC1 dan PC2 dalam Endpoint Secure, Insiden Keamanan menggambarkan bahwa Endpoint Secure mendeteksi berkas virus yang sama pada PC1 dan PC2, dan berkas virus file ini memiliki value md5 yang sama. Setelah kalian memilih untuk membenarkan berkas virus ini pada PC1, kalian dapat membernarkan berkas virus yang sama pada PC lainnya.

3.1.3 Langkah-langkah

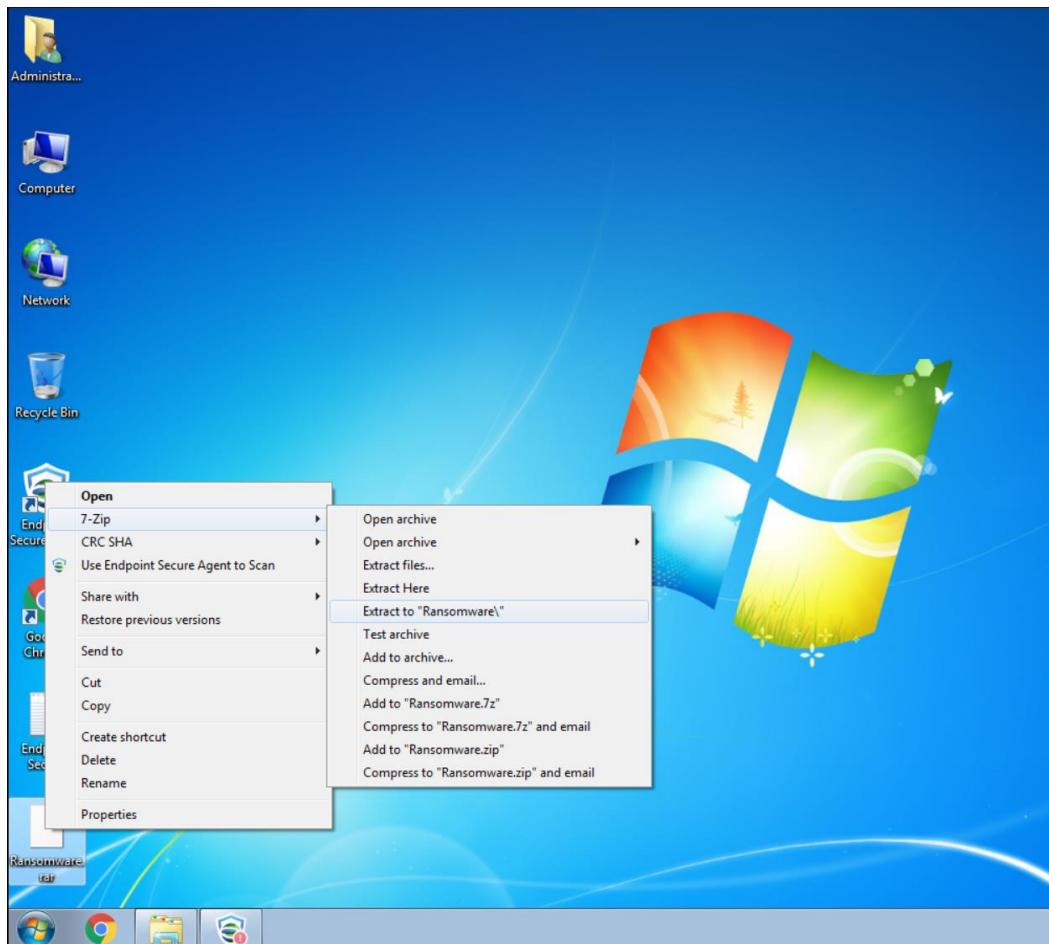
3.1.3.1 Pengaturan Policy

1. Matikan semua policy proteksi. Jika policy proteksi diaktifkan, berkas virus akan dibenarkan secara otomatis oleh Endpoint Secure, jadi kita perlu mematikan proteksi untuk melakukan tes.

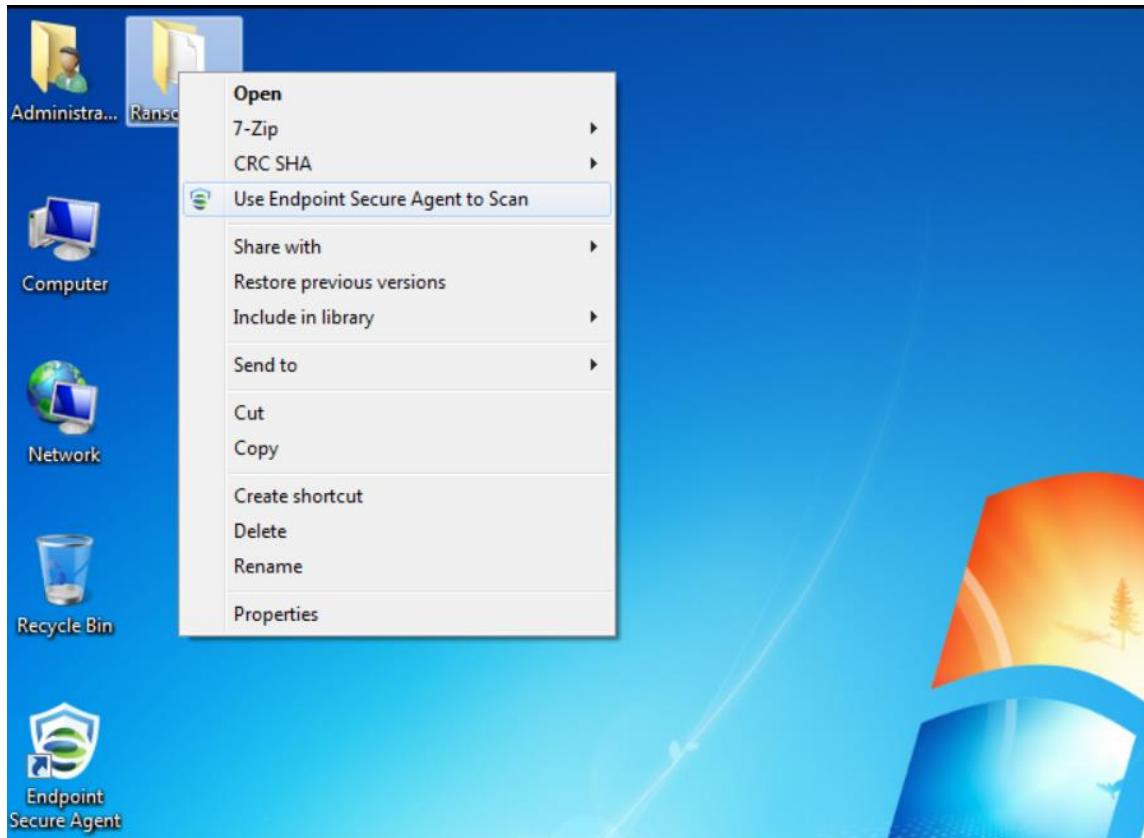
The screenshot shows the Sangfor Endpoint Secure web interface under the 'Realtime Protection' tab. It displays settings for 'Realtime File System Protection' and 'WebShell Detection'. Under 'Realtime File System Protection', the 'Enable realtime file system protection' checkbox is unchecked. The 'Protection Level' dropdown is set to 'Medium'. Scan options include 'Skip files larger than: 50 MB' and 'Scan compressed files up to: 3 hours deep'. Under 'Engine', 'Sangfor Engine Zero' is selected. Action options include 'Standard' and 'No Action - Report Only'. Under 'WebShell Detection', the 'Enable WebShell detection' checkbox is unchecked. The 'Type' dropdown is set to 'One-time'. Action options include 'File' and 'No Action - Report Only'.

3.1.3.2 Memulai sebuah Serangan

1. Unzip berkas virus pada PC1 dan PC2



2. Kalian dapat menggunakan Endpoint Secure Agent untuk memindai direktori virus secara manual, atau kalian dapat menggunakan Endpoint Secure tugas pemindaian untuk semua PC.



3.1.3.3 Efek Penyerangan

1. Kalian dapat melihat Endpoint Secure dapat medeteksi berkas virus pada PC1 dan PC2.

One Click Kill the Virus

The screenshot shows the Protect Agent interface. On the left sidebar, there are five main menu items: Security, Virus Scan, Realtime Protection, Tools, and AI. The Virus Scan item is currently selected. The main content area displays a scan summary: "Custom scanFinish, 1 threats detected". It shows one scanned file (C:\Users\Administrator\Desktop\Ranso...) and two infected files (c:\users\administrator\desktop\ransomware\whiterose). The first file is marked as "ransomware" and "High" severity, with the virus name identified as "Ransom.Win32.WhiteRose.uwzg". Below the summary, there are three buttons: "Quarantine", "Trust", and "Logs".

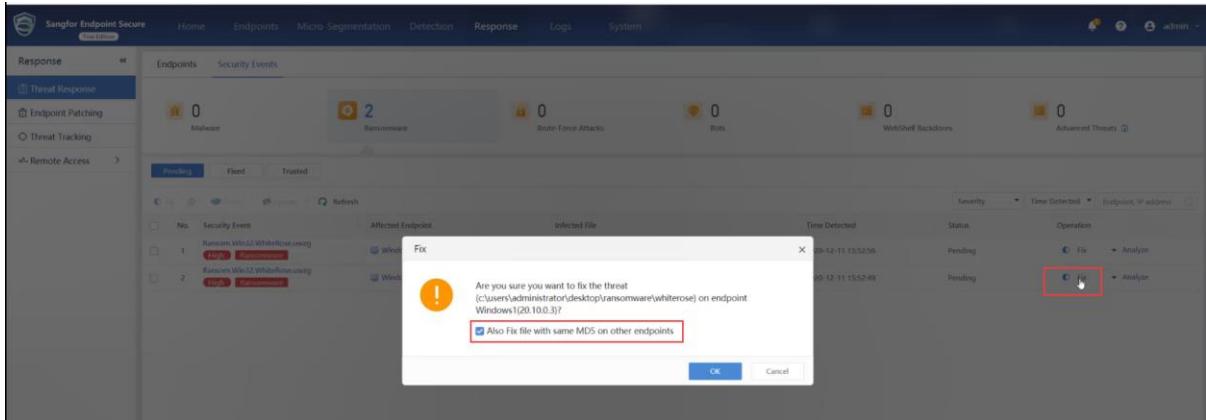
2. Kalian dapat me-query insiden di Endpoint Secure MGR

The screenshot shows the Sangfor Endpoint Secure Response module. The top navigation bar includes Home, Endpoints, Micro Segmentation, Detection, Response, Logs, and System. The Response tab is active. On the left, there are sections for Threat Response (Endpoint Patching, Threat Tracking, Remote Access), and a Pending tab for Threat Events. The main content area displays a dashboard with counts for Malware (0), Ransomware (2), Brute-Force Attacks (0), Bots (0), WebShell Backdoors (0), and Advanced Threats (0). Below this, a table lists security events. The table has columns: No., Security Event, Affected Endpoint, Infected File, Time Detected, Status, and Operation. Two entries are listed:

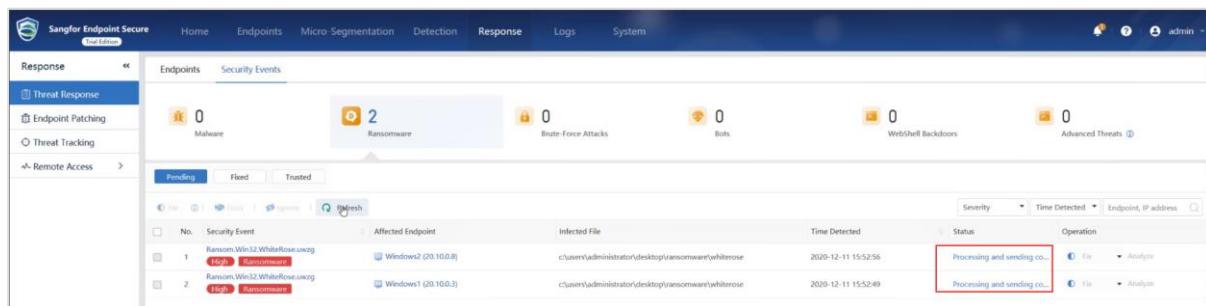
No.	Security Event	Affected Endpoint	Infected File	Time Detected	Status	Operation
1	Ransom.Win32.WhiteRose.uwzg	Windows2 (20.10.0.8)	c:\users\administrator\desktop\ransomware\whiterose	2020-12-11 15:52:56	Pending	<input type="button"/> Fix <input type="button"/> Analyze
2	Ransom.Win32.WhiteRose.uwzg	Windows1 (20.10.0.3)	c:\users\administrator\desktop\ransomware\whiterose	2020-12-11 15:52:49	Pending	<input type="button"/> Fix <input type="button"/> Analyze

3. Pilih satu PC dan klik "Fix". Dan cek "Also Fix file with same MD5 on other endpoints"

One Click Kill the Virus



4. Tunggu tugas Endpoint Secure MGR mebenarkan masalah.



5. Setelah tugas membenarkan selesai, kalian dapat melihat virus di PC1 dan sama di PC2.



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc