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

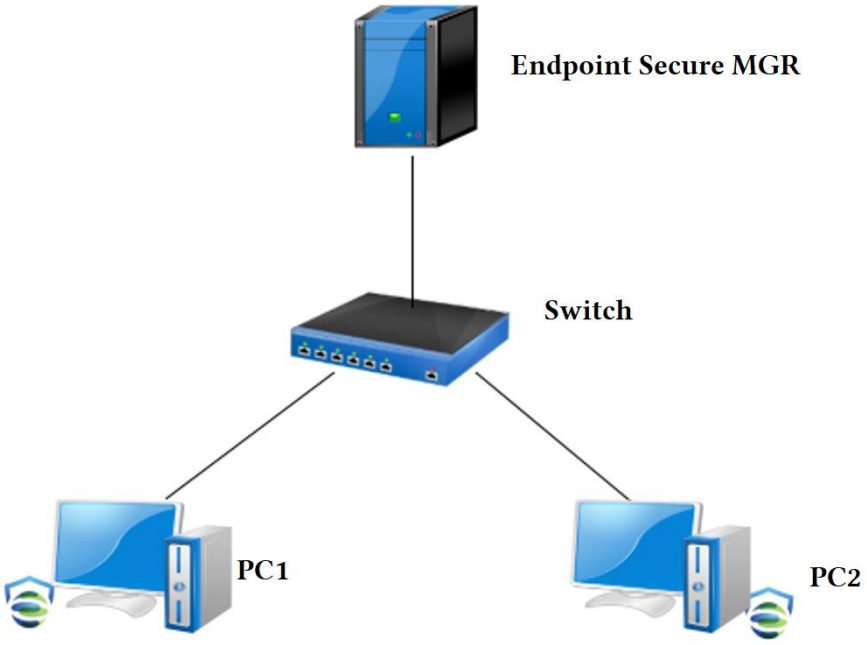
Bab 1 Skenario

Program ini mendemontrasikan 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

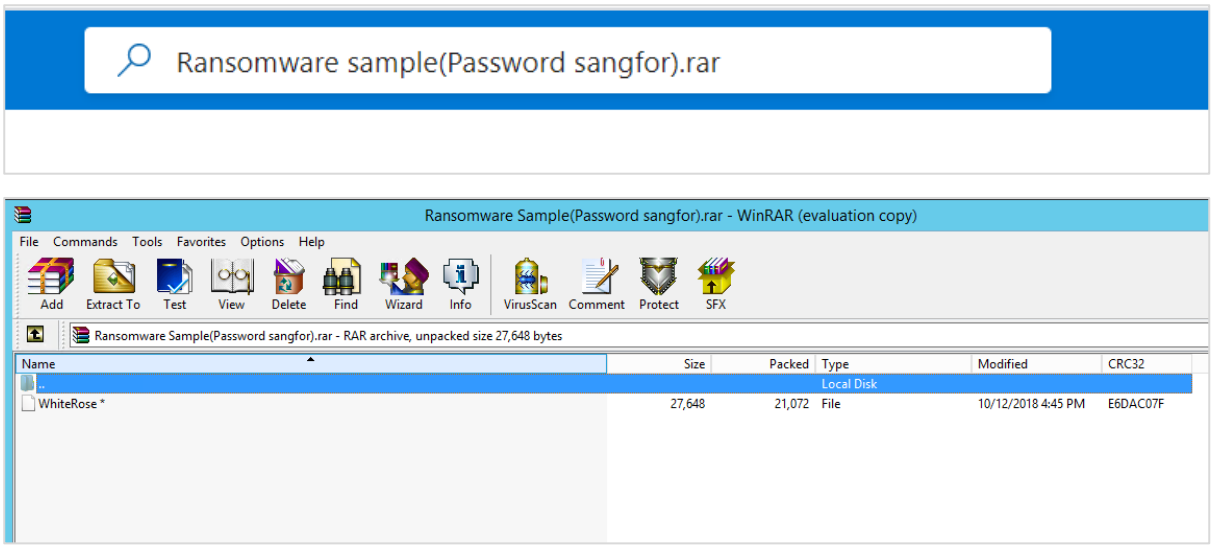


Device	Account/Password	IP	Description
PC1	administrator/111111	20.10.0.3	PC memulai serangan ransomware
PC2	administrator/111111	20.10.0.8	PC diserang oleh ransomware dengan RDP brute-forcec cracking

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.

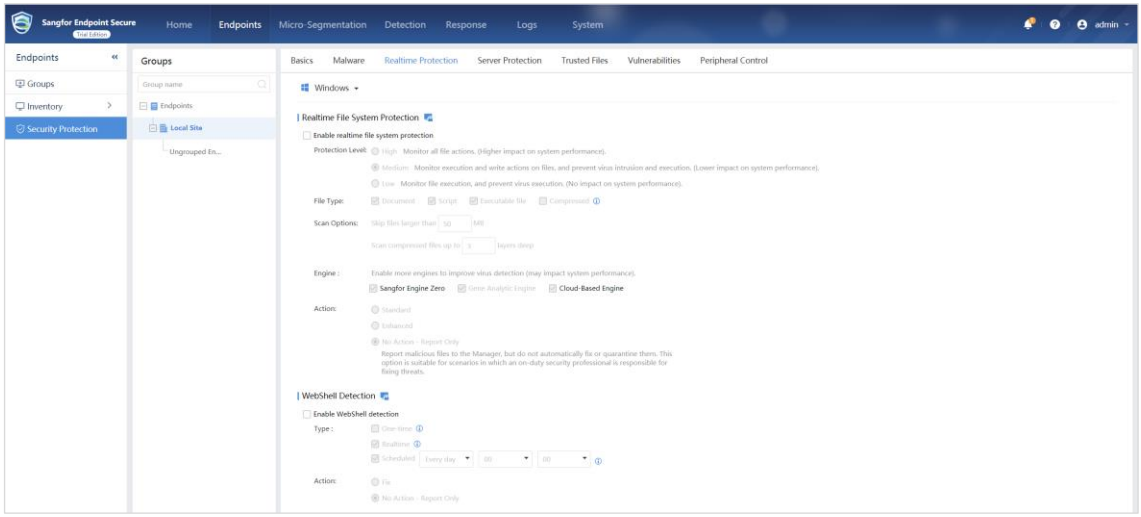
3.1.2 Hasil yang diharapkan

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 memilik 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

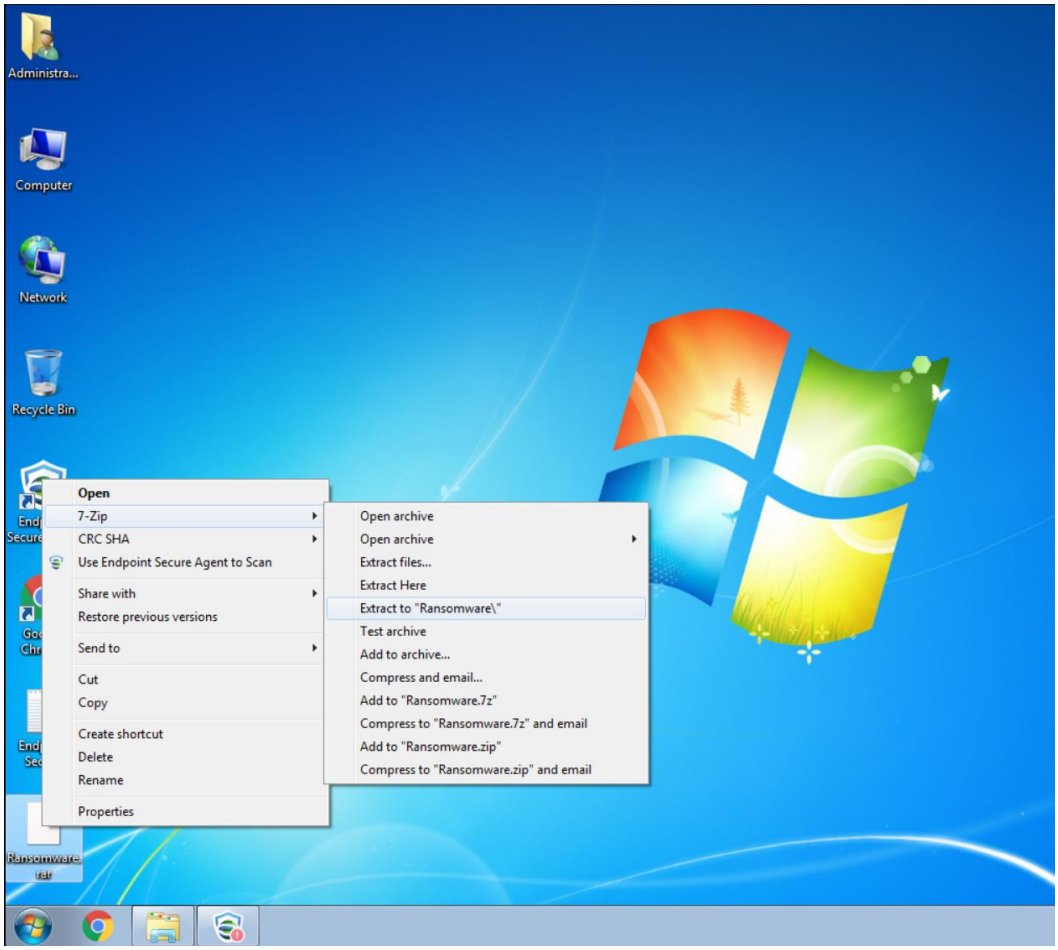
3.1.3.1 Pengaturan Policy

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

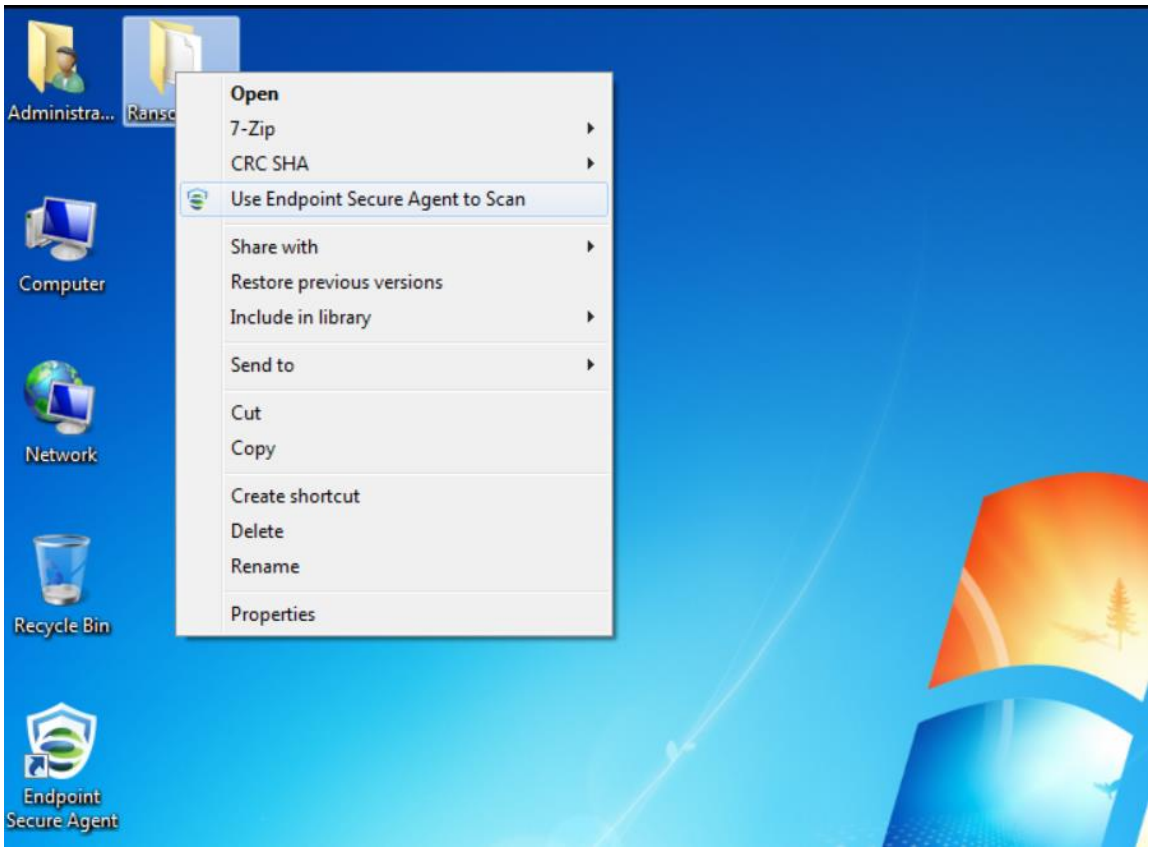


3.1.3.2 Memulai sebuah Serangan

1. Unzip berkas virus pada PC1 dan PC2

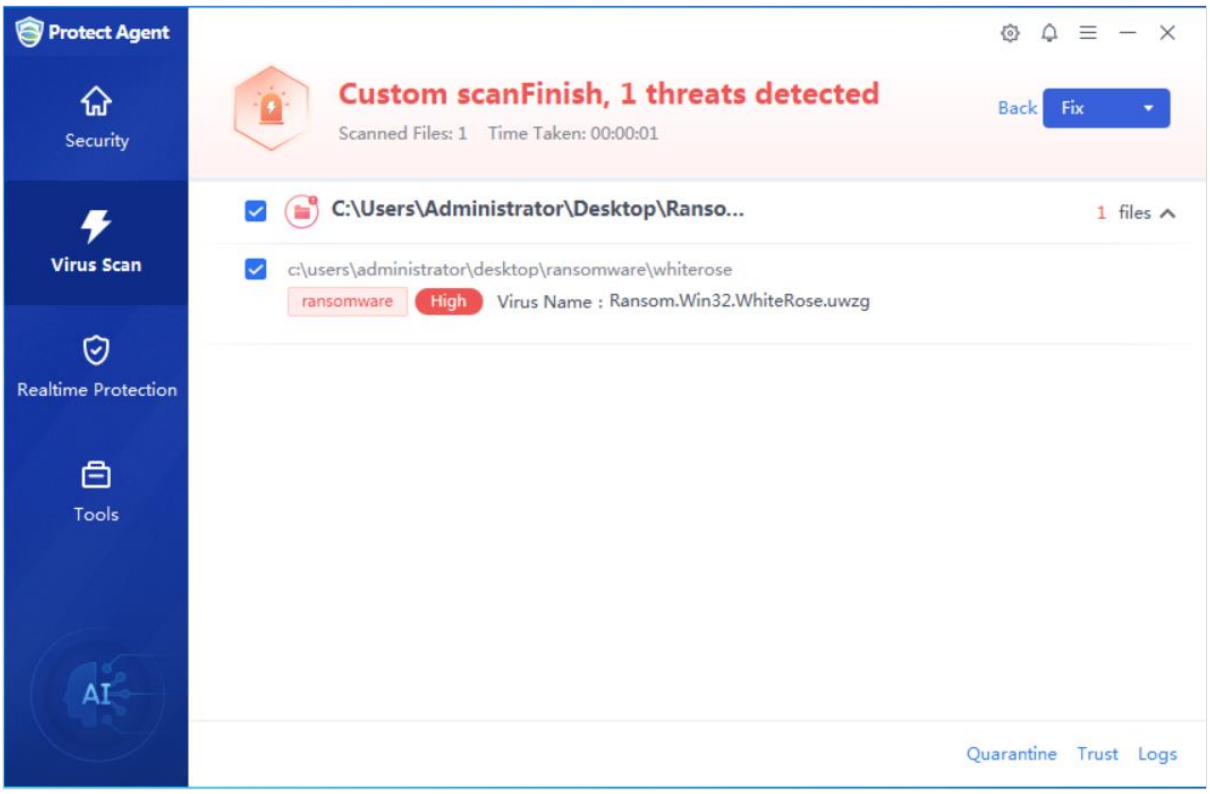


2. Kalian dapat menggunakan Endpoint Secure Agent untuk memindai direktori virus secara manual, atau kalian dapat menggunakan Endpoint Secure tugas pemindaian untuk semua PC.

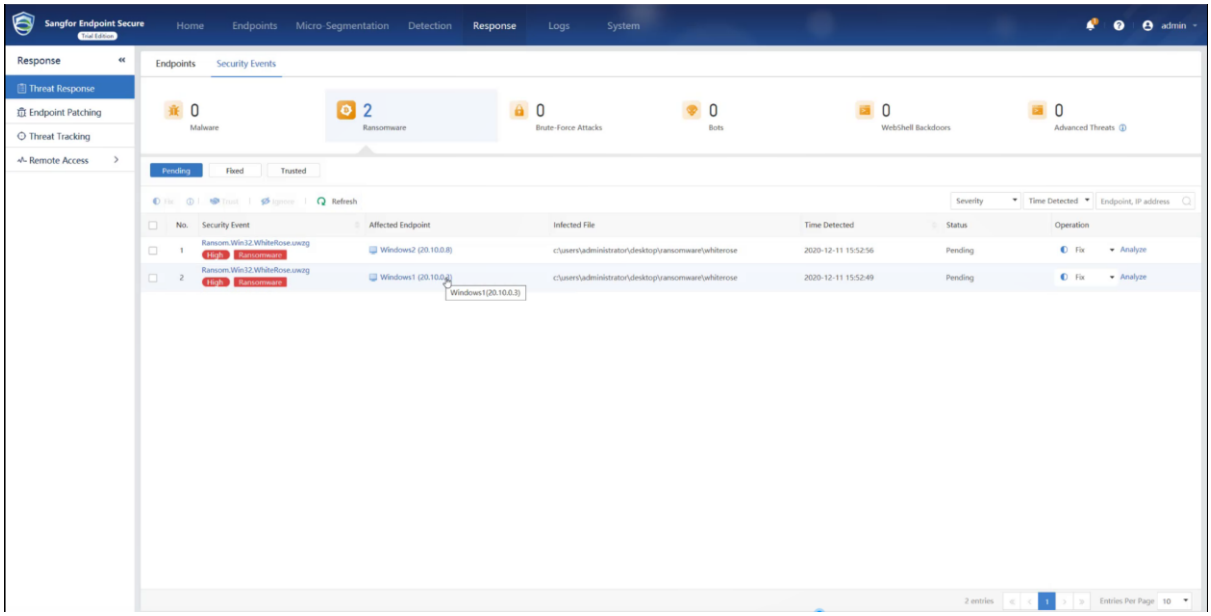


3.1.3.3 Efek Penyerangan

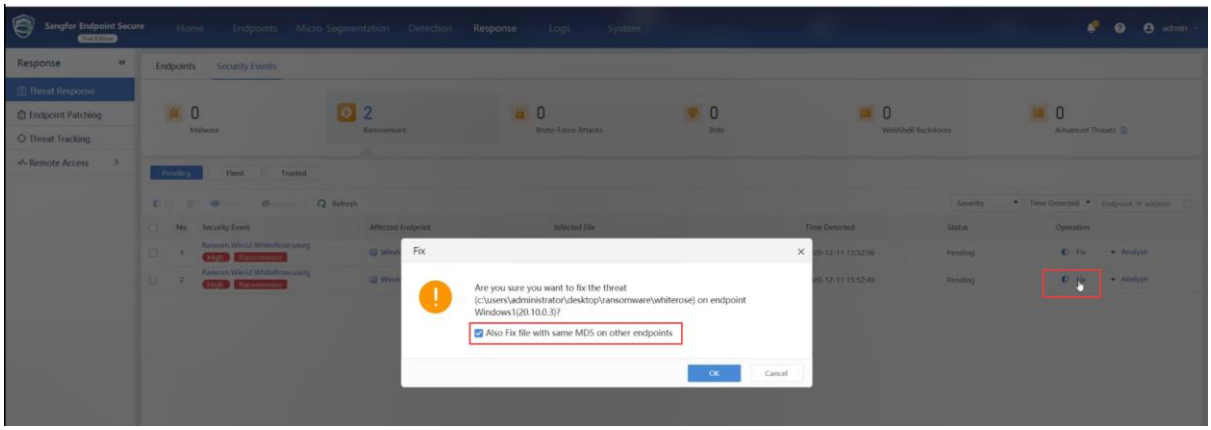
1. Kalian dapat melihat Endpoint Secure dapat medeteksi berkas virus pada PC1dan PC2.



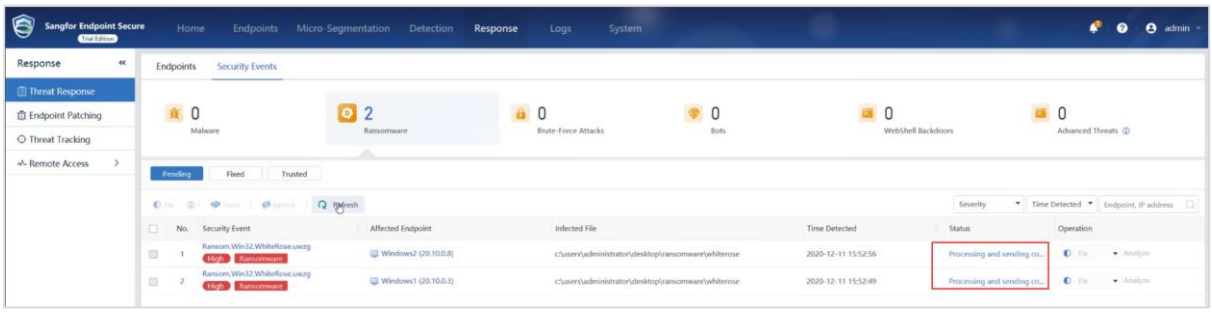
2. Kalian dapat me-query insiden di Endpoint Secure MGR



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



4. Tunggu tugas Endpoint Secure MGR mebenarkan masalah.



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