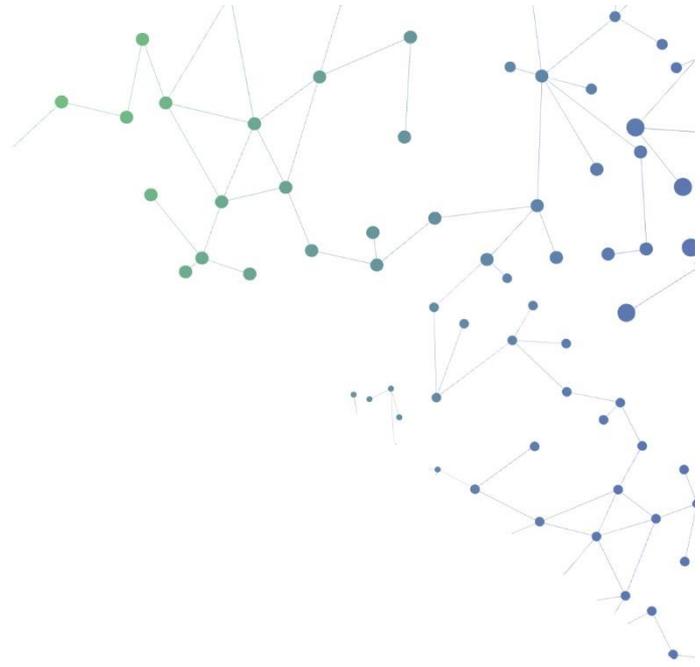


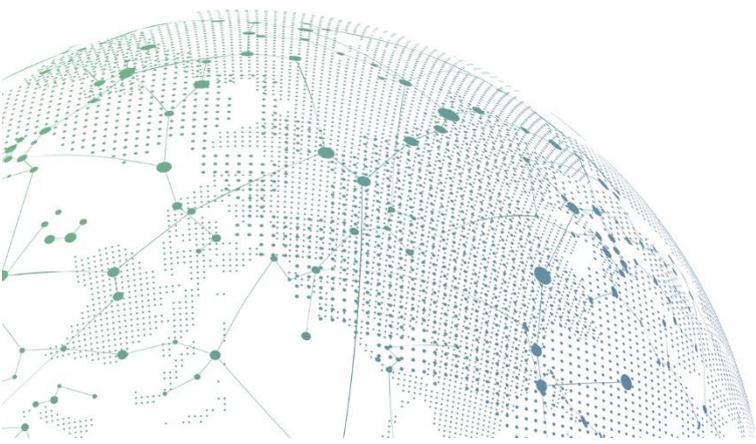


**SANGFOR**



# **Endpoint Secure**

## **Praktek Terbaik untuk\_Pengujian Rating Deteksi Virus Endpoint Secure**



## Catatan Perubahan

Tanggal	Catatan Perubahan
21 Oktober 2020	Penerbitan Dokumen

# DAFTAR ISI

Bab 1 Persiapan Pengujian .....	1
Bab 2 Masalah Pelanggan .....	1
Bab 3 Langkah-langkah Pengujian .....	1
Bab 4 Perkiraan Hasil.....	4
Bab 5 Pencegahan .....	4

## Bab 1 Persiapan Pengujian

Harap persiapkan hal-hal berikut sebelum pengujian:

1. Area pengujian Endpoint Secure, versi terbaru dari Endpoint Secure, dan win7 atau sistem operasi di atasnya untuk klien Endpoint Secure.
2. Sampel pengujian: Sebelum pengujian, konfirmasi penyedia sampel pengujian yang harus memberikan sampel terlebih dahulu. Umumnya, sampel pengujian disediakan dalam salah satu cara berikut:

Disediakan oleh Sangfor

Disediakan oleh pesaing bisnis

Disediakan oleh pelanggan

Disediakan oleh Sangfor, pesaing bisnis dan pelanggan, 1/3 dari masing-masing

## Bab 2 Masalah Pelanggan

1. Pelanggan menangani tingkat deteksi virus. Artinya, bandingkan tingkat deteksi virus dengan membunuh sampel yang sama dengan perangkat lunak antivirus yang berbeda.

## Bab 3 Langkah-langkah Pengujian

1. Nonaktifkan Real-time File System Protection dan fungsi Ransomware Protection dari Endpoint Secure

Fungsi real-time file system protection harus dinonaktifkan saat membersihkan sampel dan mempengaruhi hasilnya. Klik **Endpoints** -> **Security Protection** dan konfigurasi grup real-time protection policy dimana pengujian endpoint terletak seperti tampilan dibawah ini. Nonaktifkan Real-time File System Protection dan fungsi Ransomware Protection.

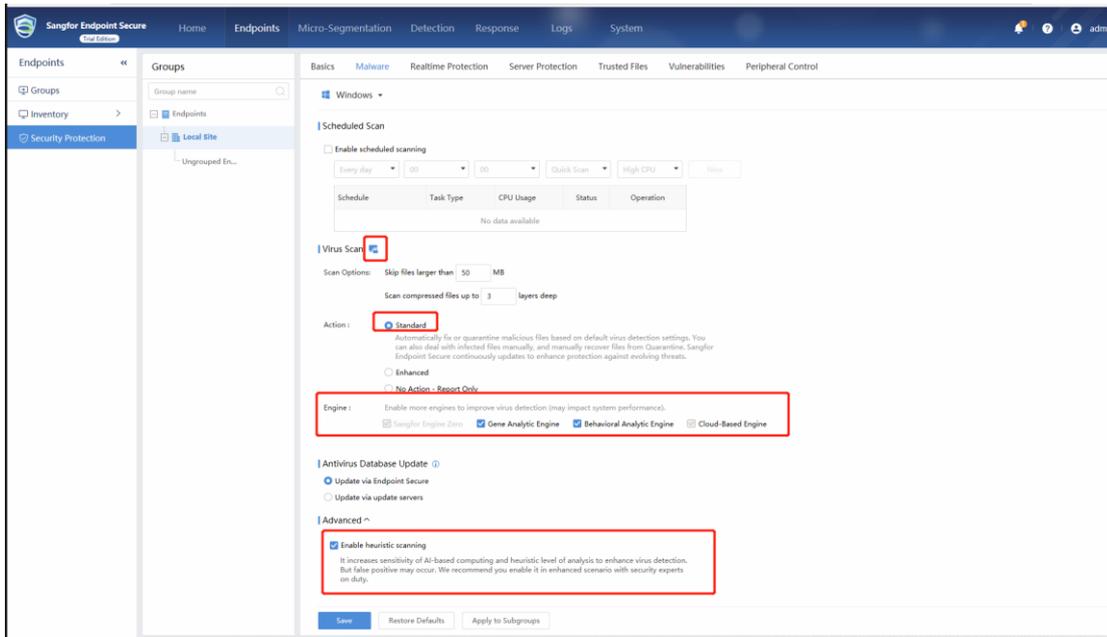
## Pengujian Rating Deteksi Virus Endpoint Secure

The image displays two screenshots of the Sangfor Endpoint Secure management console. The top screenshot shows the 'Realtime File System Protection' settings under the 'Malware' tab. The 'Enable realtime file system protection' checkbox is highlighted with a red box. Below it, there are options for Protection Level (High, Medium, Low), File Type (Document, Script, Executable file, Compressed), Scan Options (Skip files larger than, Scan compressed files up to), Engine (Sangfor Engine Zero, Some Analytic Engine, Cloud-Based Engine), and Action (Standard, Enhanced, No Action - Report Only). The bottom screenshot shows the 'Ransomware Protection' settings. The 'Enable ransomware honeypot' checkbox is highlighted with a red box. Other settings include Action (Fix, Alert - Fix Manually) and Fileless Attack Protection (Enable suspicious PowerShell script detection, Action: Block script execution, No Action - Alert Only). Both screenshots show a sidebar with 'Endpoints' and 'Local Site' selected, and a top navigation bar with 'Home', 'Endpoints', 'Micro-Segmentation', 'Detection', 'Response', 'Logs', and 'System'.

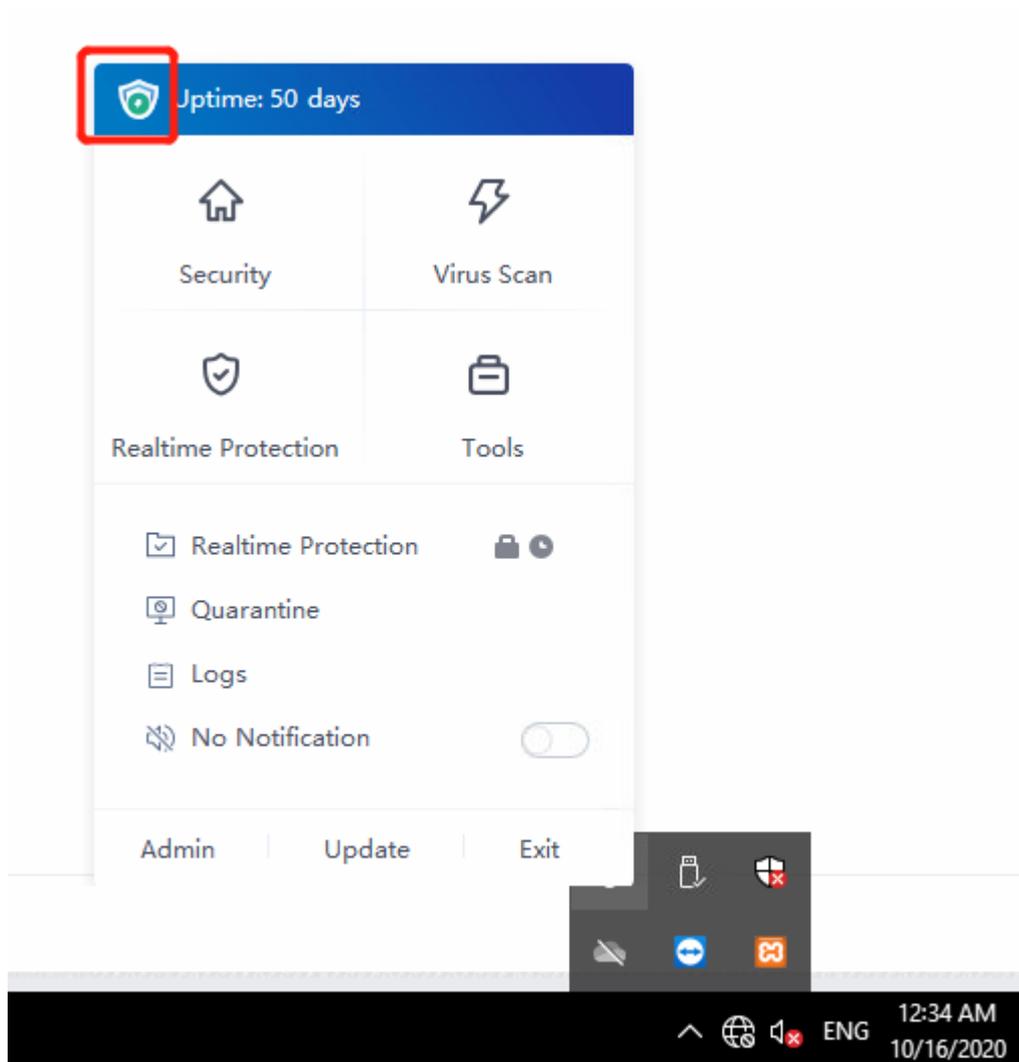
### 2. Aktifkan heuristic scanning

Klik **Endpoints** -> **Malware** dari Endpoint Secure dan atur kelompok virus killing test dimana komputer pengujian berada. Aktifkan semua virus scanning engines dan "Enable heuristic scanning" (ini membantu meningkatkan tingkat deteksi virus). Seperti tampilan di bawah ini:

## Pengujian Rating Deteksi Virus Endpoint Secure



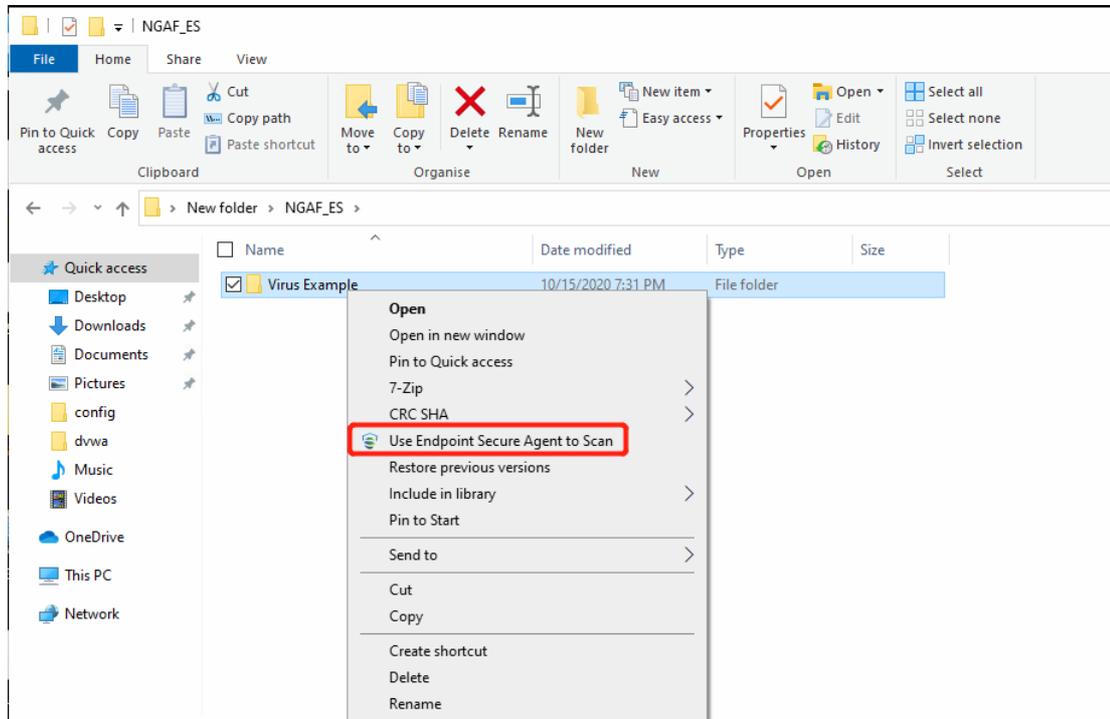
Setelah menyelesaikan pengaturan di atas, klik kanan pada ikon  pada test endpoint Agent. Seperti tampilan pada gambar berikut, ikon green lightning menunjukkan bahwa "Enable heuristic scanning" is enabled.



## Pengujian Rating Deteksi Virus Endpoint Secure

### 3.Perbandingan

Scan sample virus melalui fungsi "custom killing" dari Endpoint Secure klien, dan kemudian bandingkan tingkat deteksi virus dari produsen software antivirus yang berbeda, seperti tampilan pada gambar berikut:

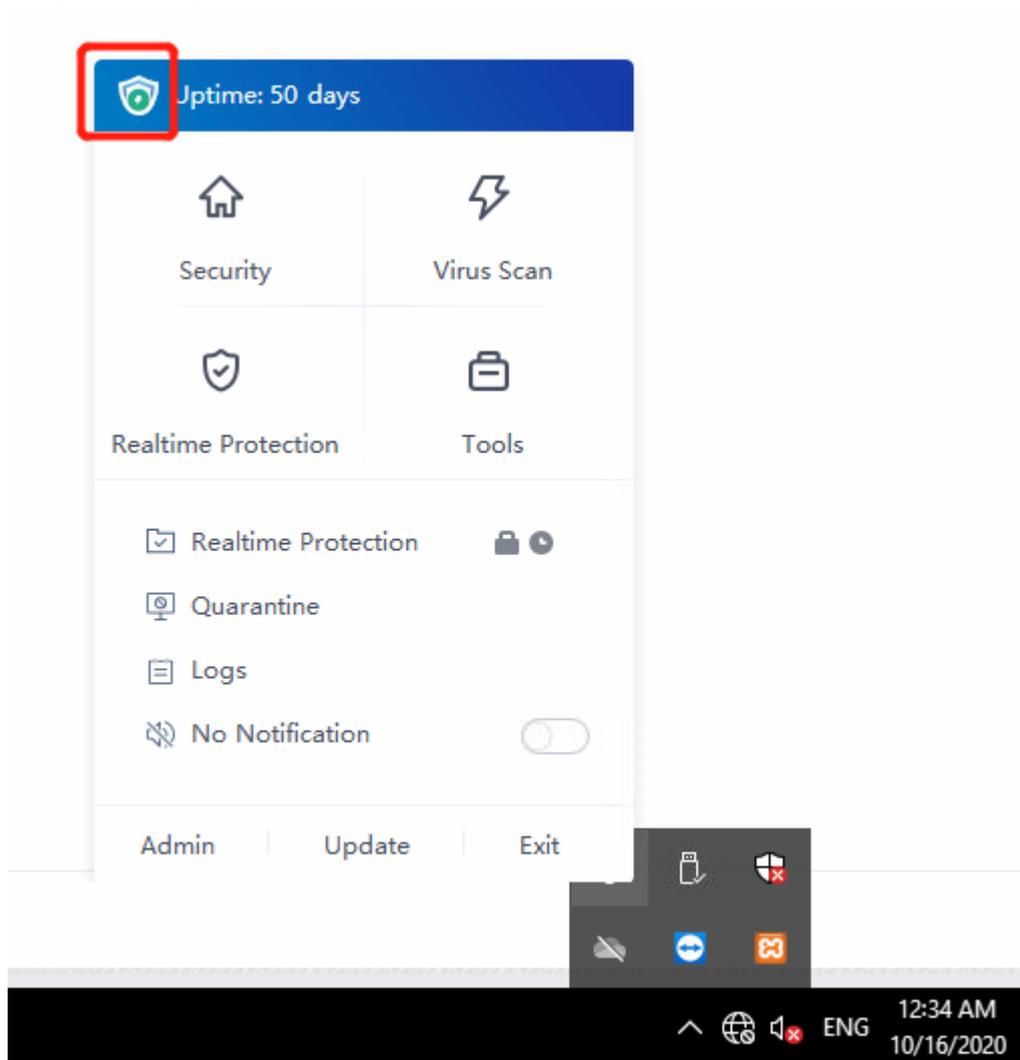


## Bab 4 Perkiraan Hasil

Perbandingan tingkat deteksi virus dari software antivirus yang berbeda untuk memindai dan killing sampel virus yang sama menunjukkan bahwa tingkat deteksi virus Endpoint Secure lebih unggul dari yang lain.

## Bab 5 Pencegahan

1. Setelah "Enable heuristic scanning" is enabled, dapat meningkatkan tingkat deteksi virus, Namun juga membawa beberapa kesalahan penilaian. Oleh karena itu, fungsi ini hanya digunakan untuk meningkatkan tingkat deteksi virus, dan harus digunakan dengan hati-hati dalam skenario lain.
2. Silakan hubungi Expert of TAC dan HQ kami setidaknya satu hari sebelumnya jika Anda ingin kami memberikan sampel pengujian.
3. Jika tingkat deteksi virus Endpoint Secure lebih rendah daripada software antivirus lainnya dalam proses pengujian, periksa hal-hal berikut.
  - (1) Periksa apakah langkah-langkah pengujian di atas diikuti secara ketat. Terutama memeriksa apakah ada ikon green lightning  pada Endpoint Secure klien di komputer pengujian, karena ikon ini berarti bahwa konfigurasinya benar, seperti tampilan pada gambar berikut.



(2) Periksa apakah sampel yang disediakan oleh pesaing bisnis dienkripsi, dengan cara membukanya dengan perangkat lunak dekompresi untuk melihat apakah kata sandi diperlukan. Jika dienkripsi, ini milik operasi yang tidak konvensional. Hanya software pesaing bisnis yang dapat memindai dan membunuhnya, dan software antivirus lainnya tidak dapat memindai dan membunuhnya.

(3) Periksa apakah sampel yang disediakan oleh pesaing bisnis adalah sampel yang dibentuk oleh karakter khusus, yang sebenarnya adalah file non-virus. Dalam hal ini, itu hanya dapat mencocokkan database virus dari pesaing bisnis, dan software antivirus lainnya tidak dapat mendeteksinya. Ini juga merupakan operasi yang tidak konvensional. Jika dicurigai, Anda dapat mengunggah sampel virus ke situs web intelijen pihak ketiga. (<https://www.virustotal.com/gui/>) untuk mengidentifikasi apakah itu file virus.

4. Jika false positives diberikan selama pengujian, unggah file false positives ke situs web intelijen pihak ketiga. (<https://www.virustotal.com/gui/>) untuk mengidentifikasi apakah itu false positive. Situs web intelijen memiliki puluhan mesin untuk menganalisis file tersebut dan Anda dapat menentukan apakah itu false positive sesuai dengan hasil analisis yang diberikan oleh situs web ini.

5. Jika ada masalah yang tidak terpecahkan yang ditemukan selama tes, tolong simpan tangkapan layar hasil virus killing dan sampel virus.



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