SANGFOR

NGAF

Praktik Terbaik untuk Skenario_Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network

Versi 8.0.26

Catatan Perubahan

Tanggal	Deskripsi Perubahan
Maret 3, 2021	Rilis Dokumen.
Mei 17, 2021	Dokumen update.

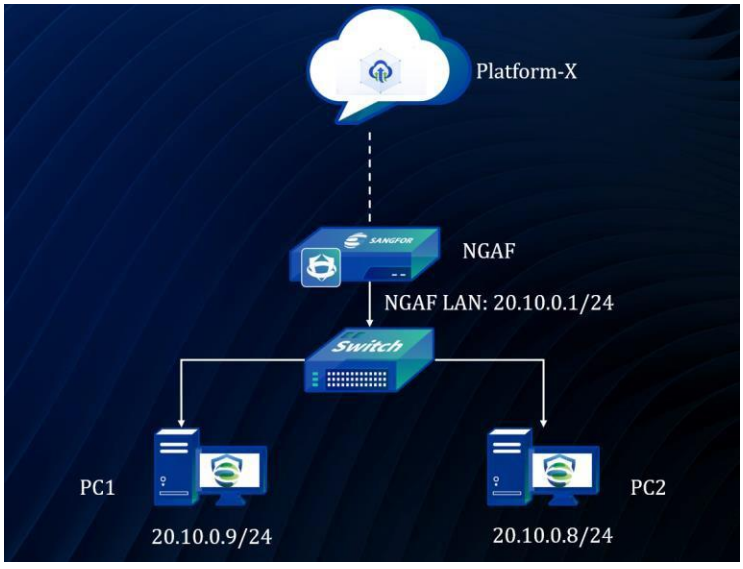
Daftar Isi

Bab 1 Skenario

1.1 Skenario

Mulai dari versi NGAF 8.0.13, NGAF dapat mendukung akses platform-X ke MGR, tetapi sebelum akses platform-X ke MGR, antarmuka management dari MGR
Itu tetap di platform-X. Jika administrator perlu untuk mengelola MGR, dia perlu untuk jump ke platform-X melalui antarmuka management NGAF untuk mengelola platform-X.
MGR membuat management dari antarmuka management MGR sangat tidak nyaman. Pelanggan bisnis kecil (terminal dibawah 300 point, operasi security dan pemeliharaan personil hanya 1-2), efek security tidak tinggi, saat membeli NGAF dan ES produk pada waktu yang sama, pengguna sendiri kekurangan sumber daya server untuk deploy ES management platform MGR, dan tidak ada kelebihan anggaran untuk membeli MGR untuk local deployment.
Pelanggan dalam skala kecil dan telah menggunakan peralatan NGAF. Karena sumber daya dan kendala lingkungan, tidak ada HCI atau sumber daya mesin virtual untuk membangun MGR, tetapi mereka masih ingin menggunakan produk ES untuk bertahan melawan virus.
Skala pelanggan kecil dan jumlah operasi dan pemeliharaan personil kecil. Sementara ingi meningkatkan security, mereka tidak ingin menambah biaya operasi dan pemeliharaan tambahan, dan mencari yang terintegrasi ES management platform.

1.2 Topologi



Device	Account/Password	IP	Description
PC1	administrator/111111	20.10.0.9/24	
PC2	administrator/111111	20.10.0.8/24	
NGAF	admin/@sangfor123	20.10.0.100/24	NGAF Deployed as Gateway

1.3 Pengenalan Tes

1.3.1 Kondisi Tes

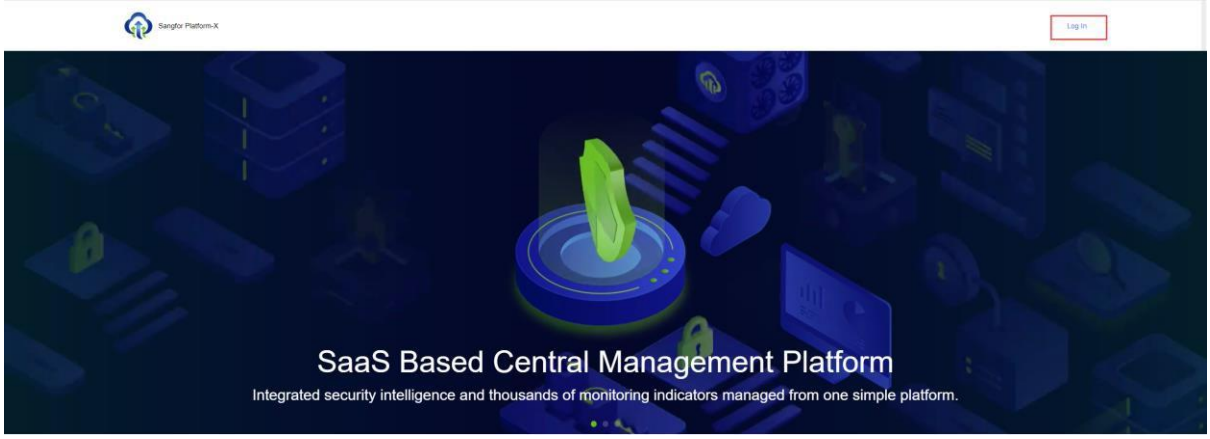
1. NGAF harus menggunakan versi 8.0.26 dan di atas dan pastikan bahwa dapat mengakses address dan port dari Platform-X.

2. Mengenai fungsi Endpoint Secure, tidak perlu untuk mengaktifkan otorisasi pada NGAF, dan otorisasi diaktifkan di Platform-X

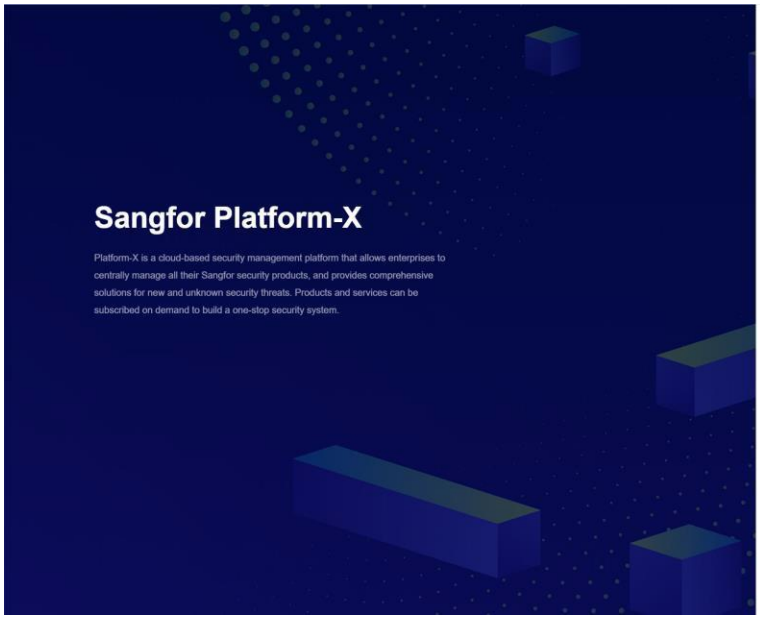
Bab 2 Login ke Platform-X dan Buat branch

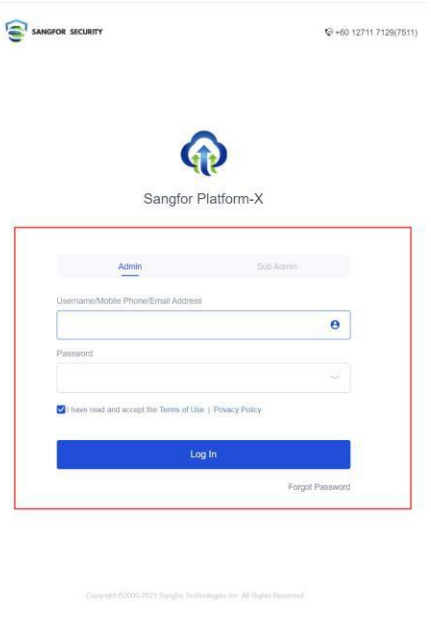
2.1 Login Platform-X

1. Gunakan browser untuk mengakses https://x.sangfor.com dan pilih login untuk login ke Platform-X. Untuk akun Platform-X, Anda dapat memperoleh sesuai dengan proses standar.

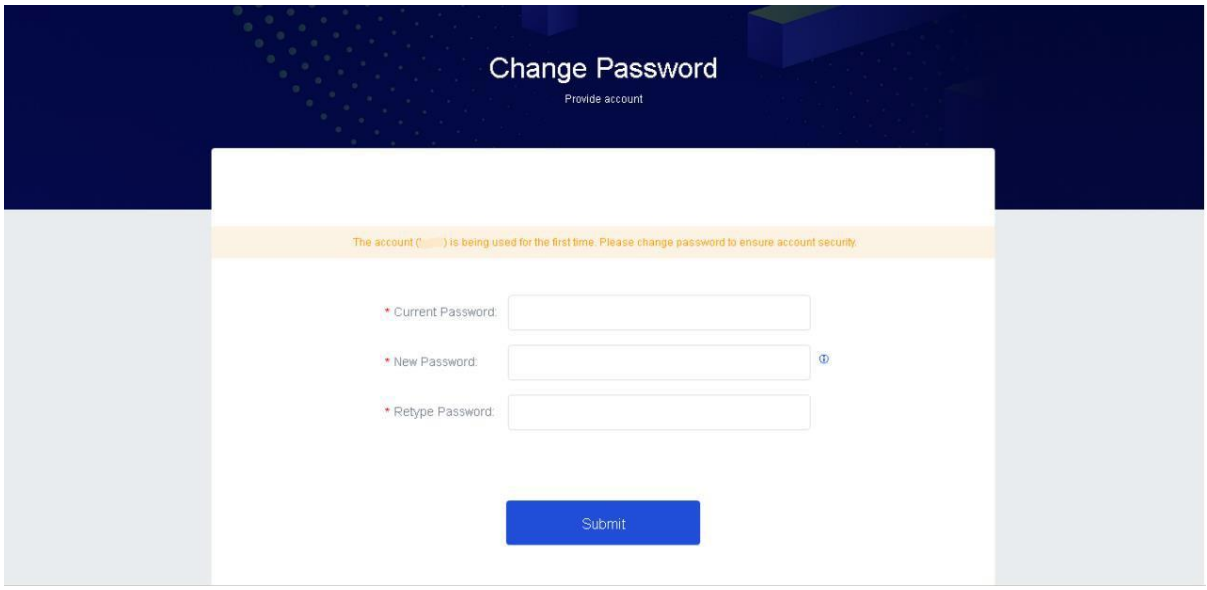


2. Setelah Anda klik log in, Anda akan mengarahkan ke halaman berikut. Anda dapat input akun name dan password untuk login.

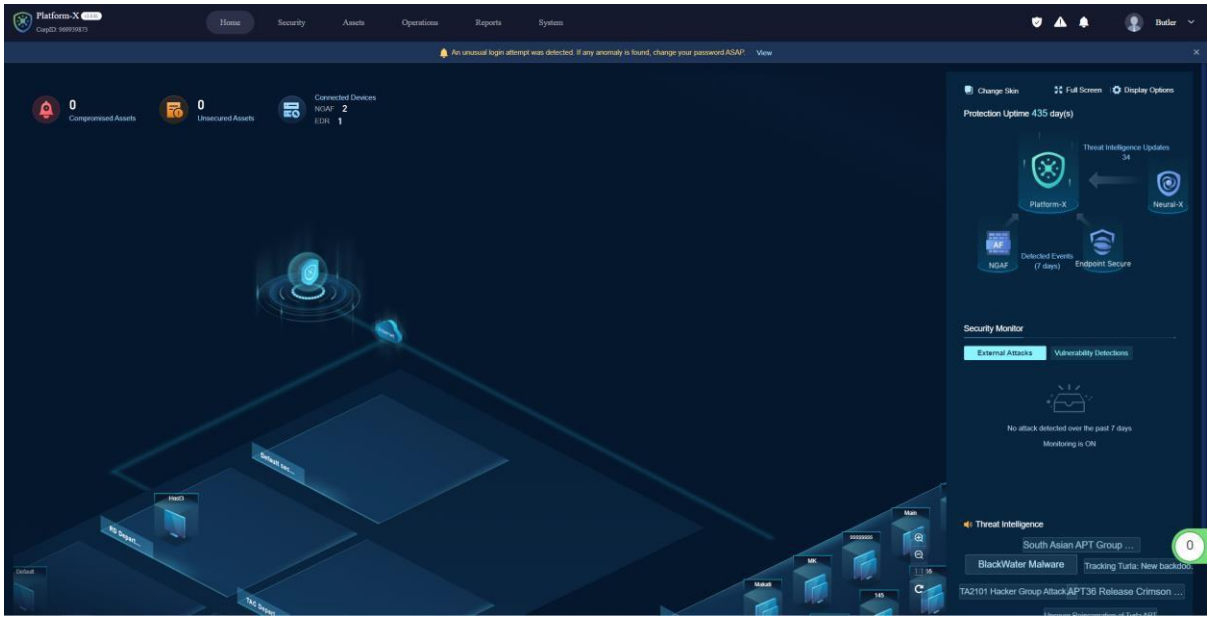




3. Jika Anda login untuk pertama kali, Anda diminta untuk modifikasi password awal. Setelah Anda modifikasi password, Anda harus login lagi ke Platform-X.

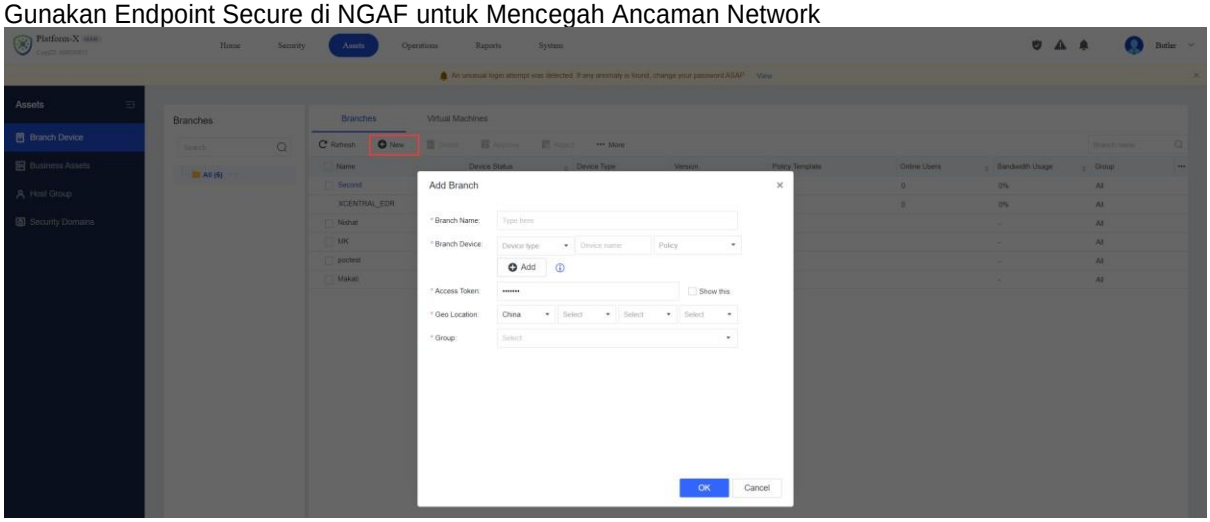


4. Halaman berikut adalah homepage dari Platform-X.

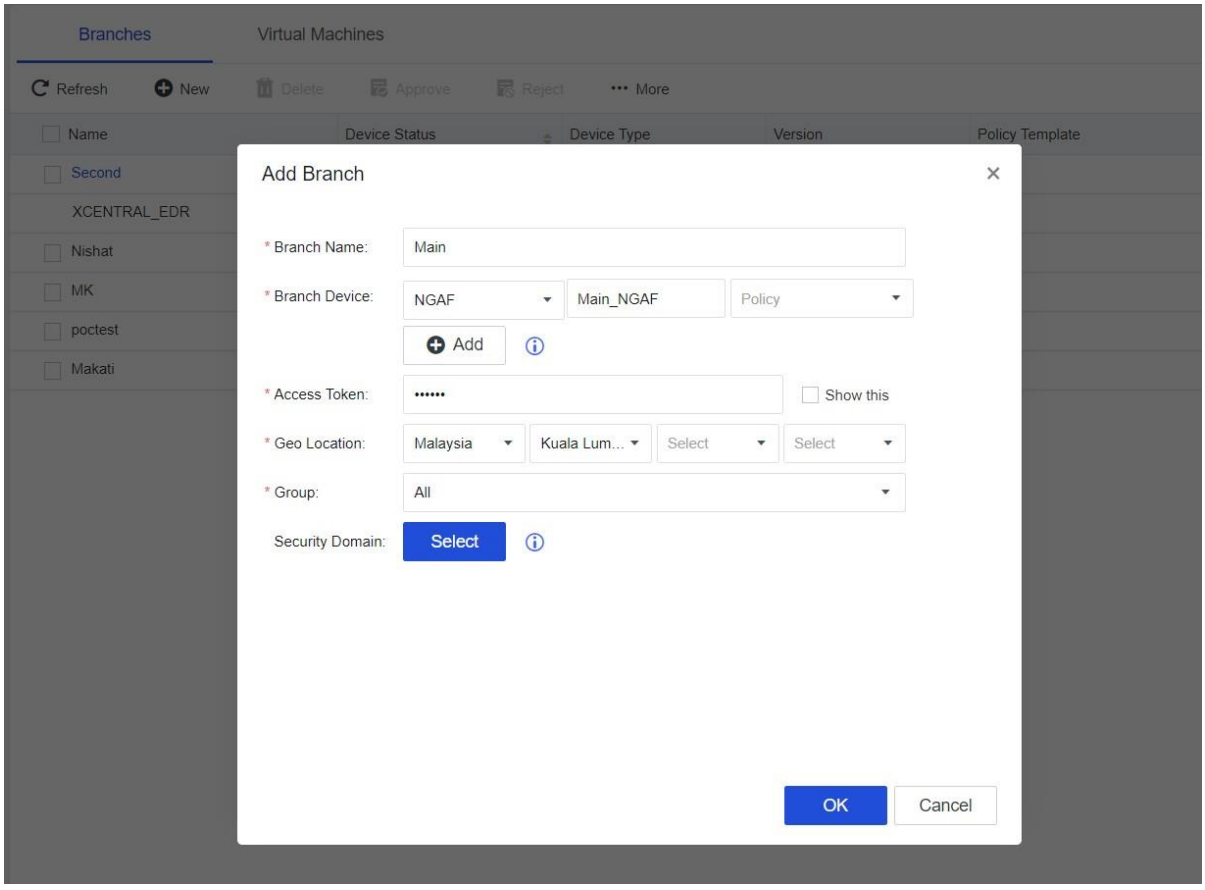


2.2 Buat perangkat branch di Platform-X

1. Pergi ke Assets -> Branch Device dan klik New untuk membuat branches.

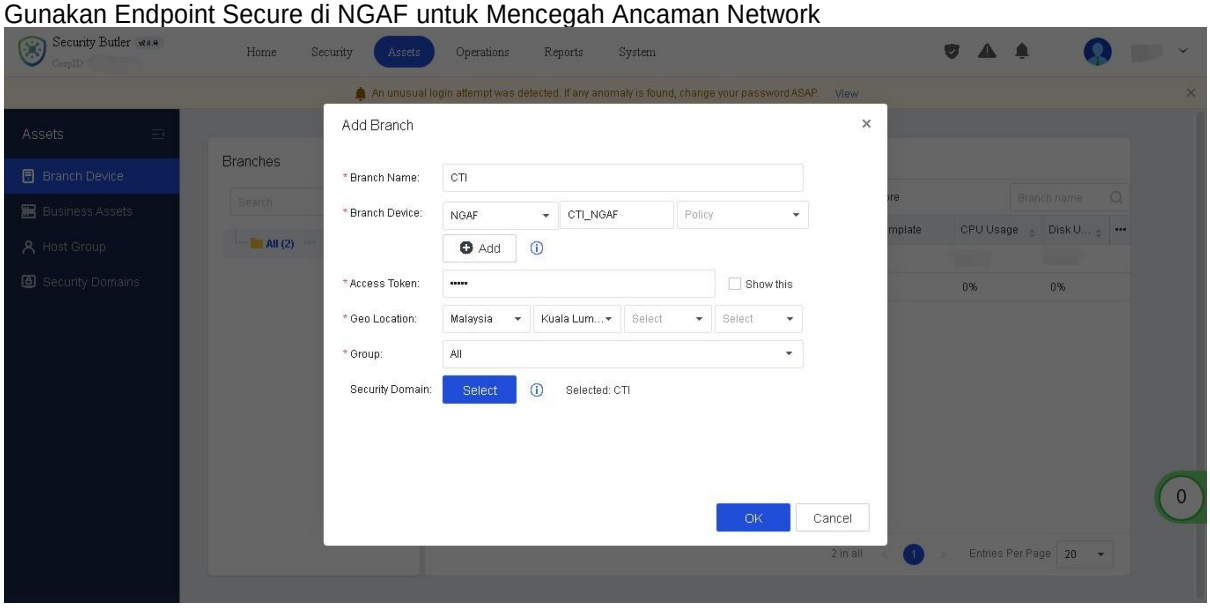


2. Input branch name, branch device type, access token, pilih lokasi perangkat dan pilih group.

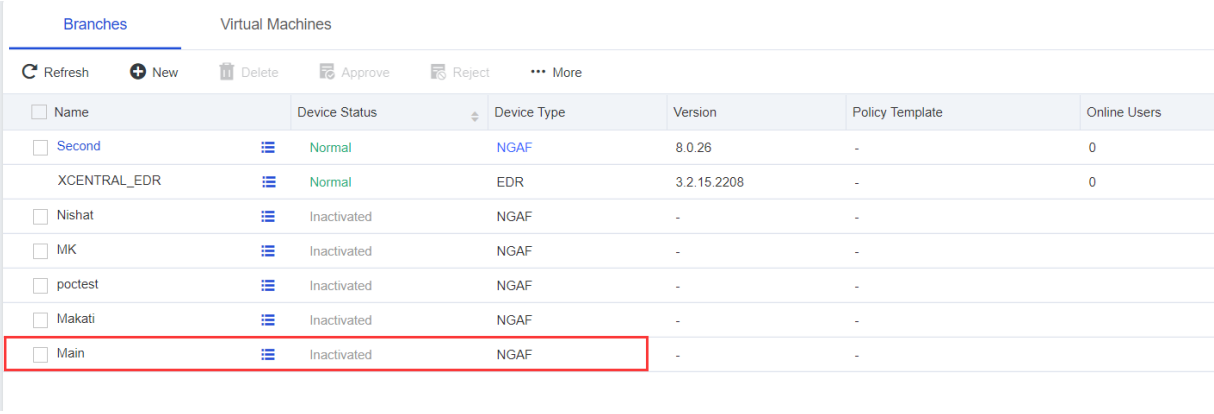


Catatan: Token akses dibuat secara acak secara default. Anda dapat modifikasi token akses sesuka Anda.

3. Setelah semua informasi telah diisi, Anda dapat klik OK.



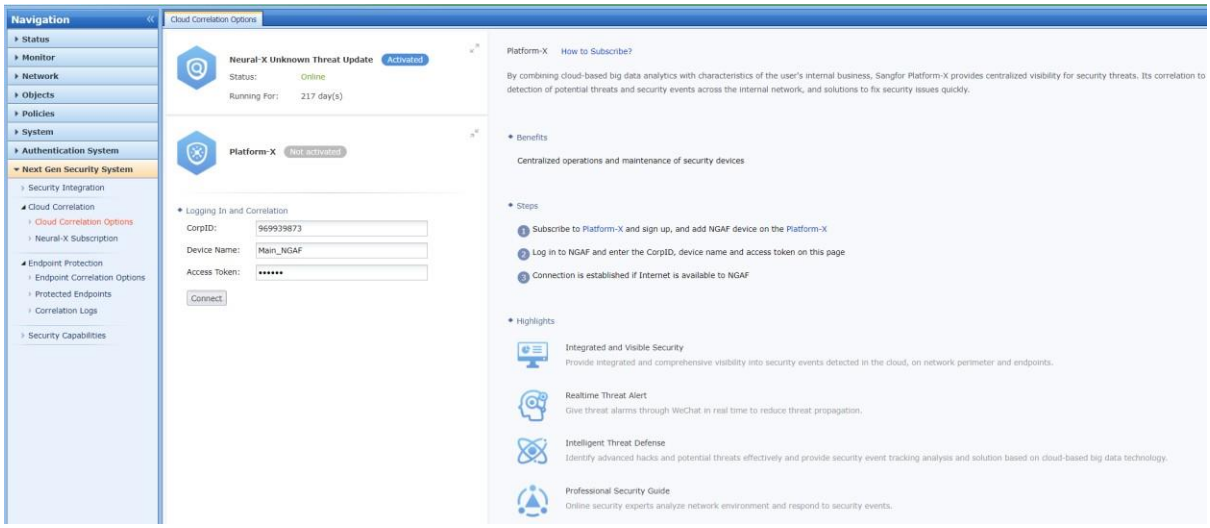
4. Setelah Anda klik OK, new branch dengan asset akan dibuat.



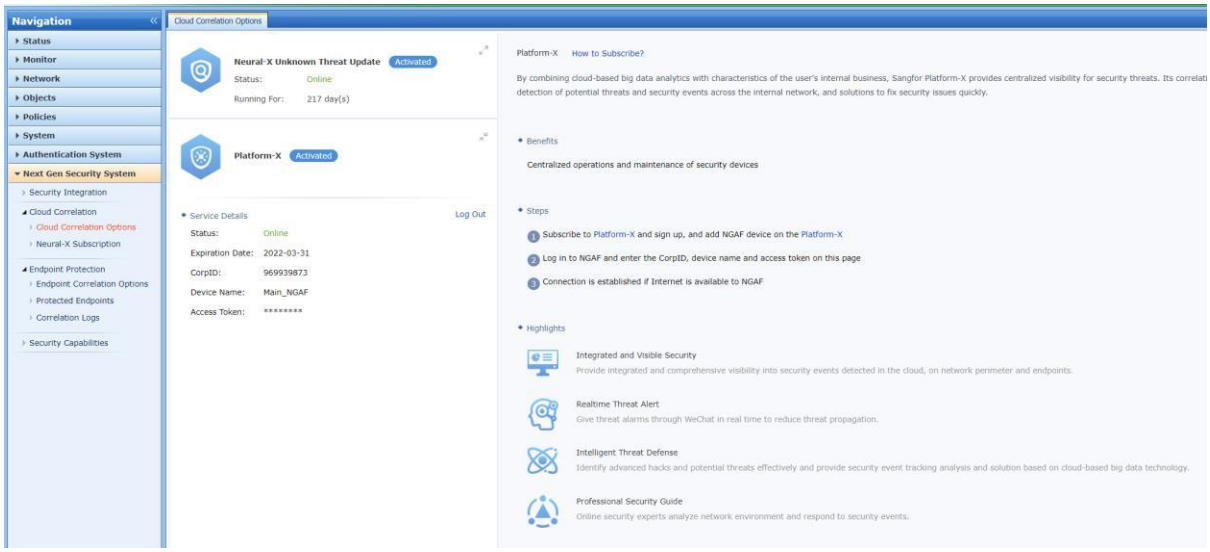
2.3 Connect NGAF ke Sangfor Platform-X

Akses NGAF Web console, pergi ke Next Gen Security System -> Cloud Correlation -> Cloud Correlation Options, pilih Platform-X.

1. Input CorpID, Device name dan Access Token, dan then klik tombol Connect.



2.Setelah beberapa saat dan refresh halaman, Anda dapat melihat status connect di web console.

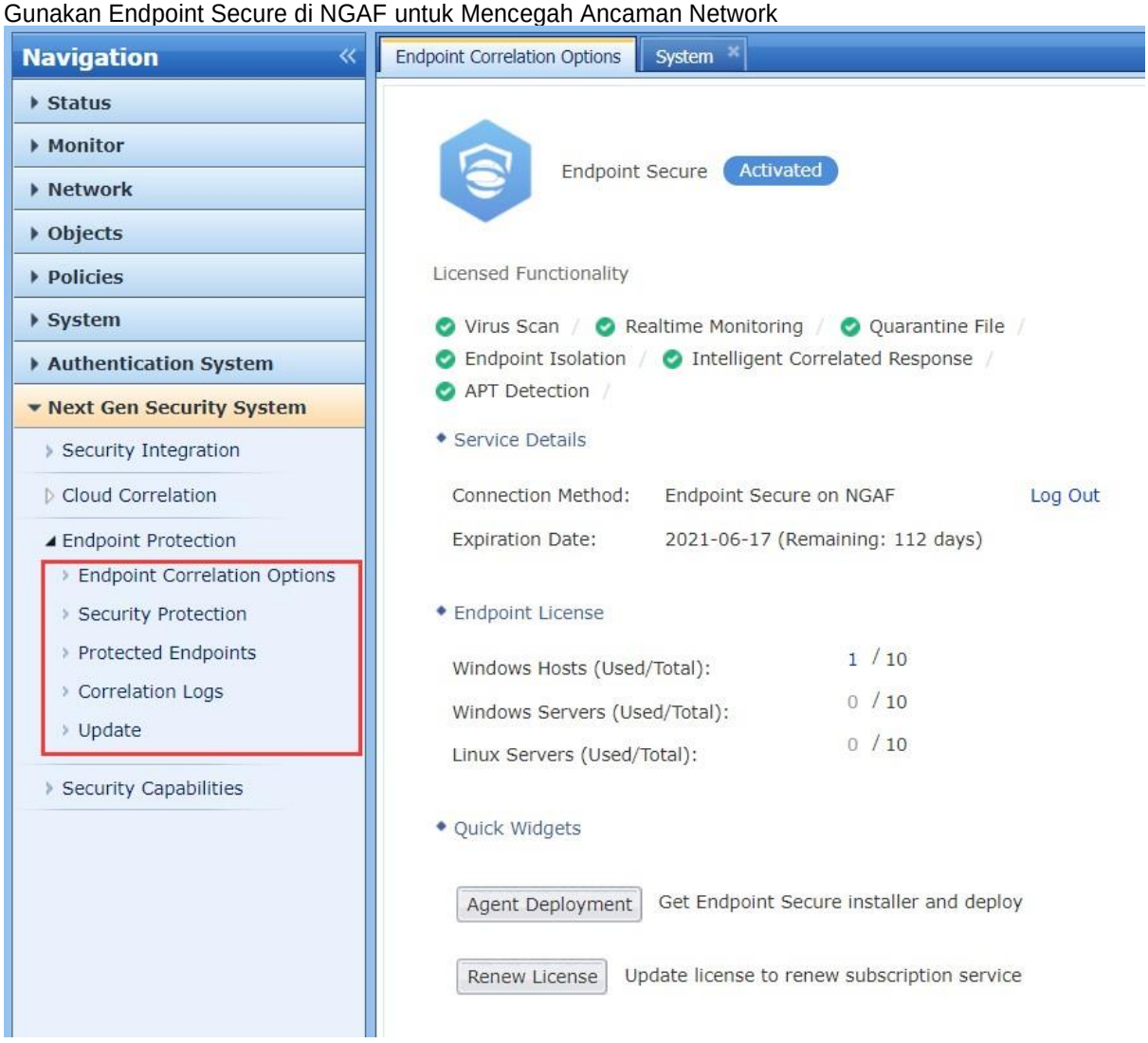


2.4 Activate Endpoint Secure di NGAF

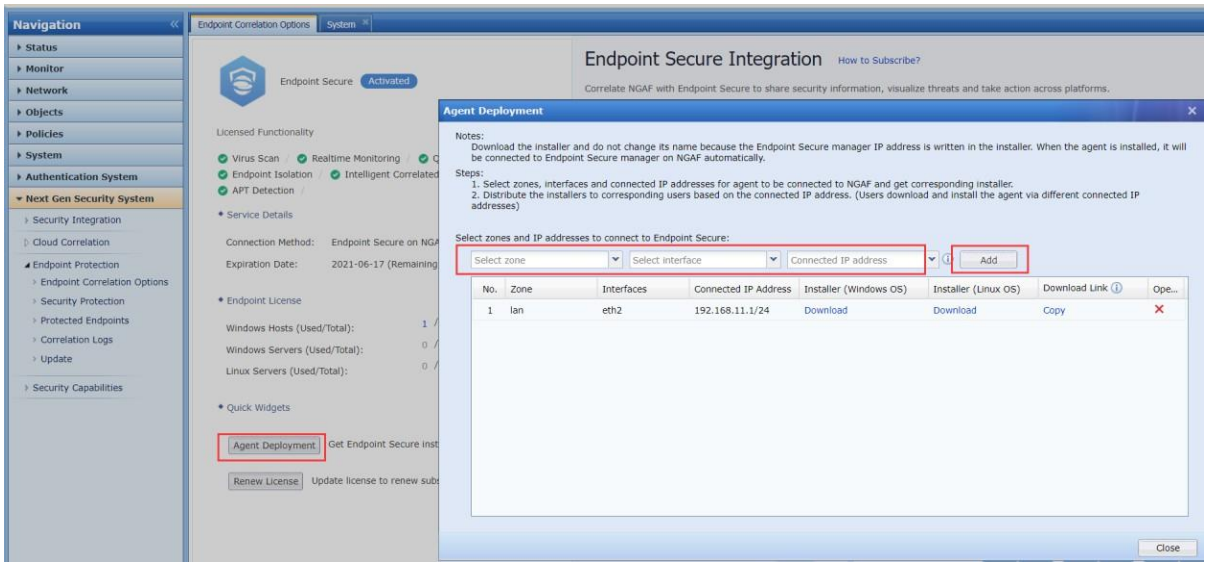
1. Pergi ke Next Gen Security System -> Endpoint Protection -> Endpoint Correlation, dan pilih Endpoint Secure di NGAF.

Bab 3 Instal Agent dan Konfigurasi Policy

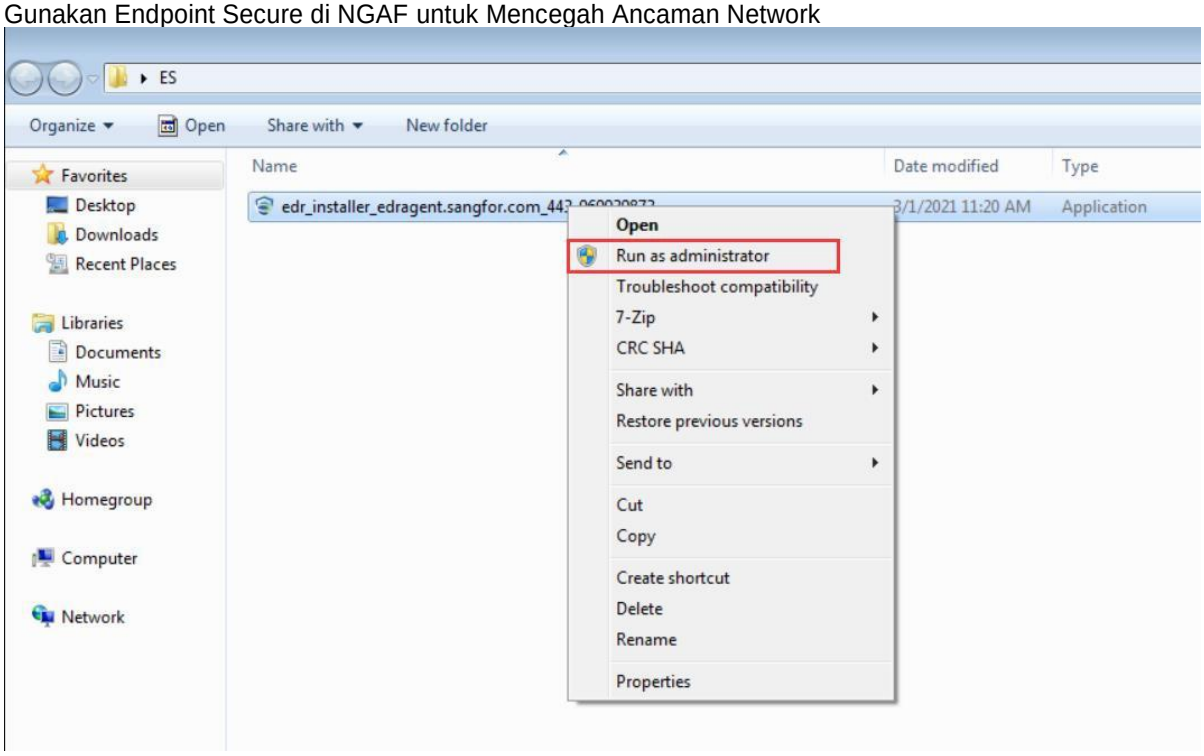
1. Setelah activate Endpoint Secure di NGAF, web console akan update dan menambahkan halaman konfigurasi terkait.



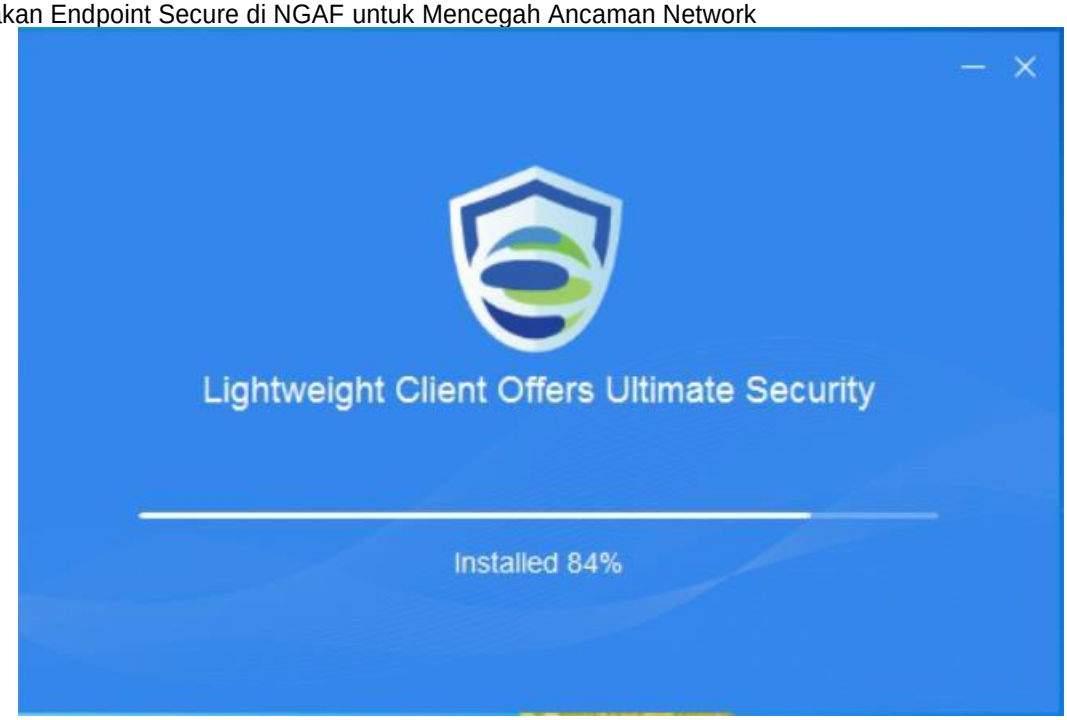
2. Buat ES agent download link, dan pilih Zone Interface dan address, kemudian klik add untuk menghasilkan paket instalasi ES agent.



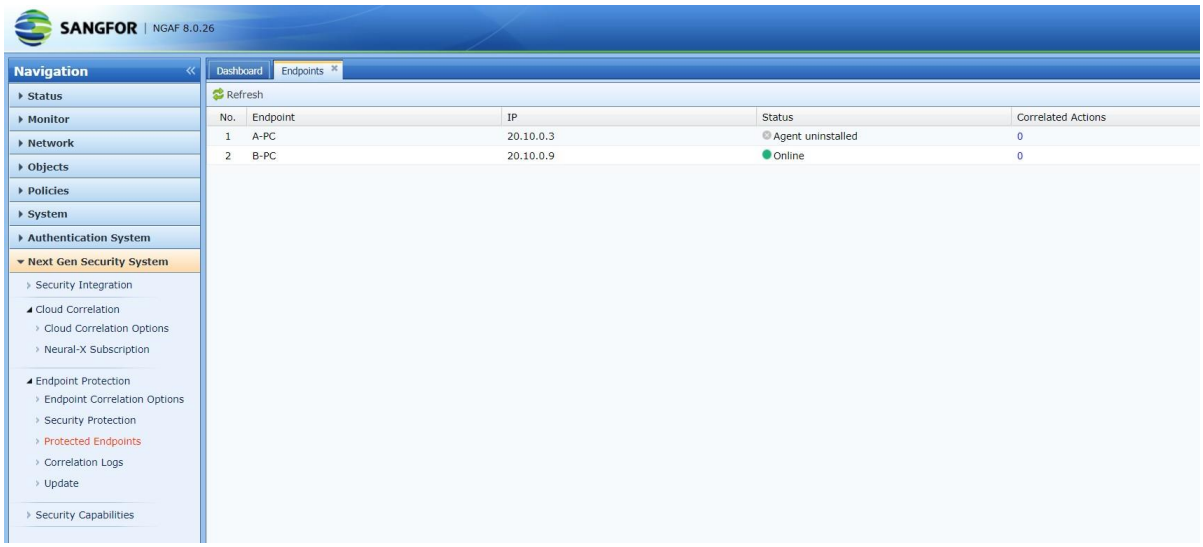
2. Kirim download link ke pengguna endpoint dan instal ES agent secara manual.


ES
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
edr_installer_edragent.sangfor.com_443
3/1/2021 11:20 AM
Application
Open
Run as administrator
Troubleshoot compatibility
7-Zip
CRC SHA
Share with
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

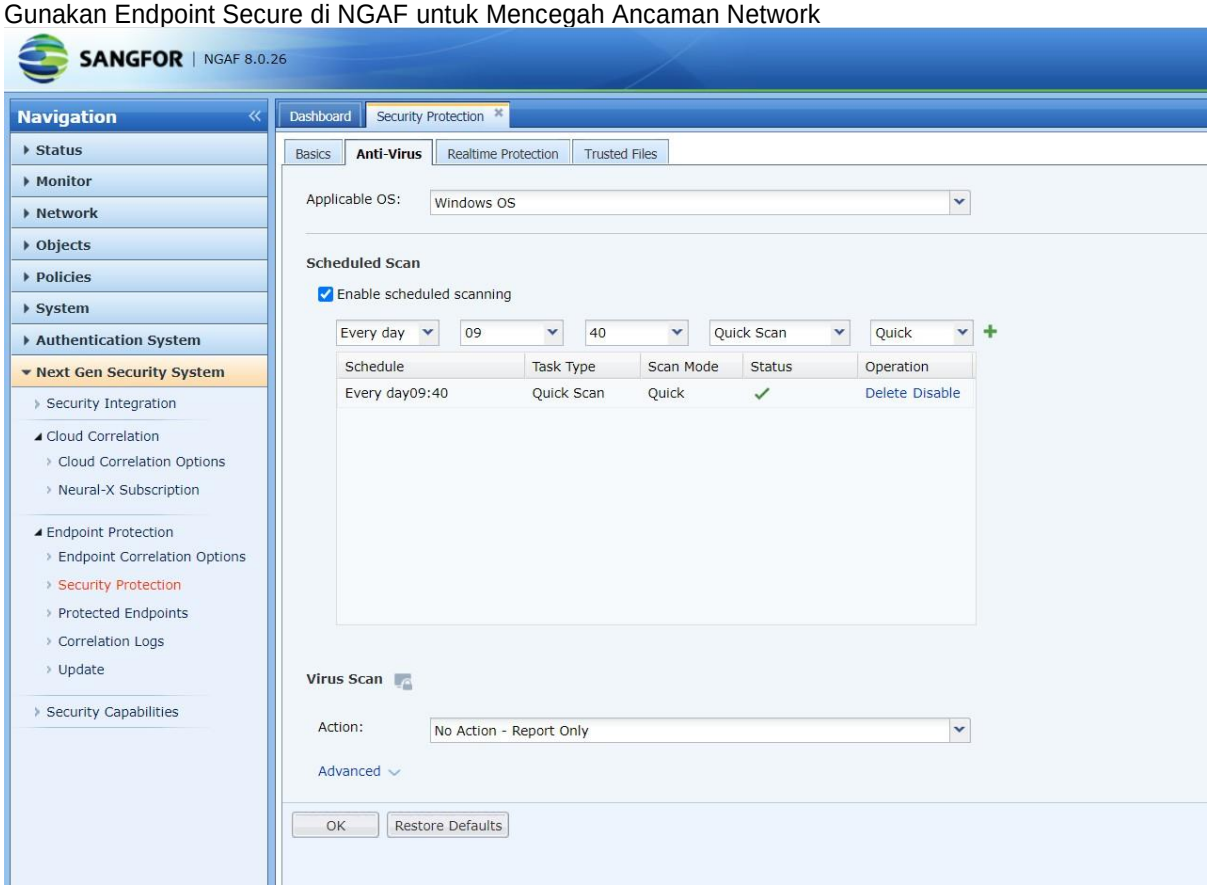

Lightweight Client Offers Ultimate Security
Downloaded 97%

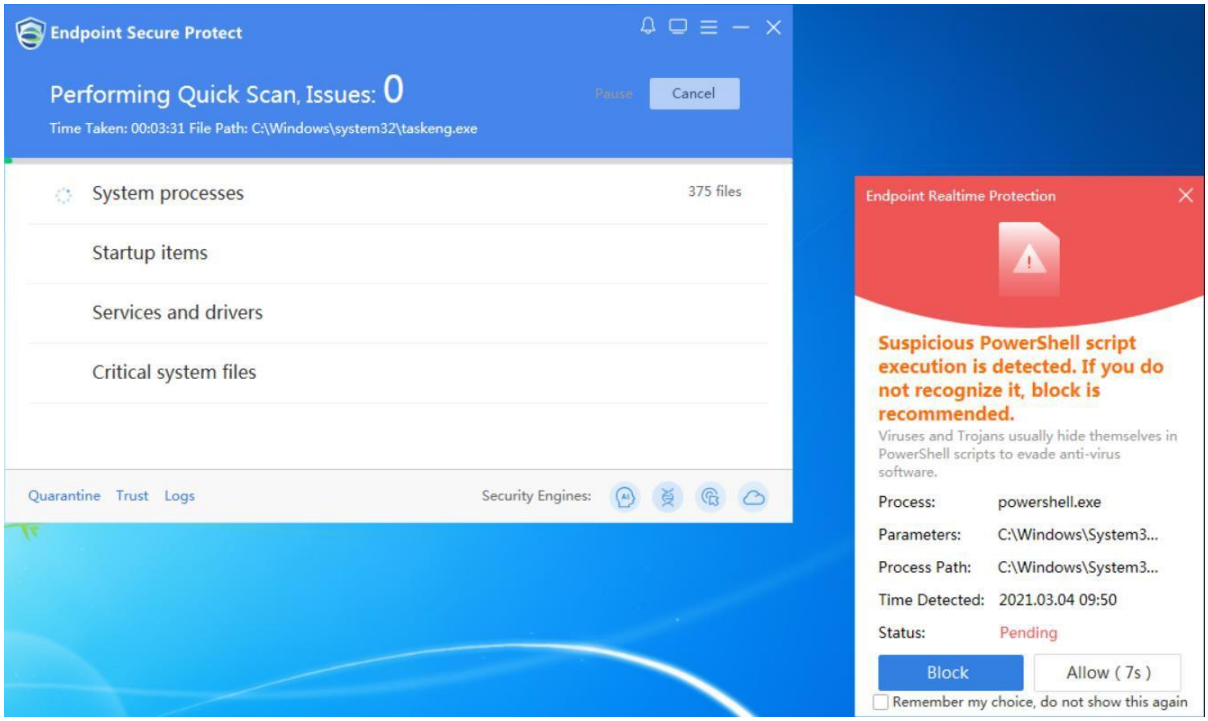


3. Anda dapat melihat status ES agent di Web Console.



4. Anda dapat merencanakan issue scan dan anti-virus policy pada ES agent di Web Console.

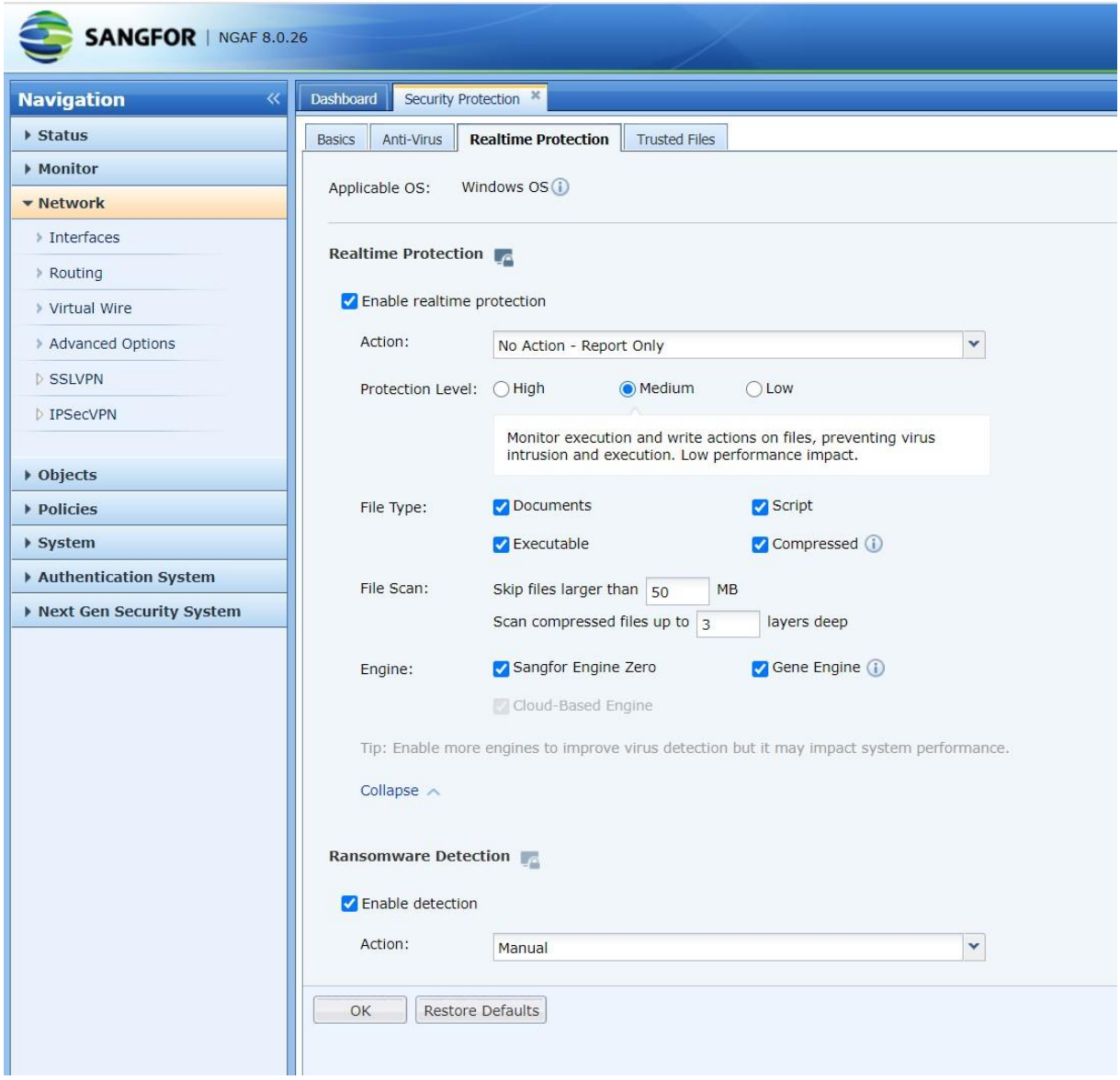




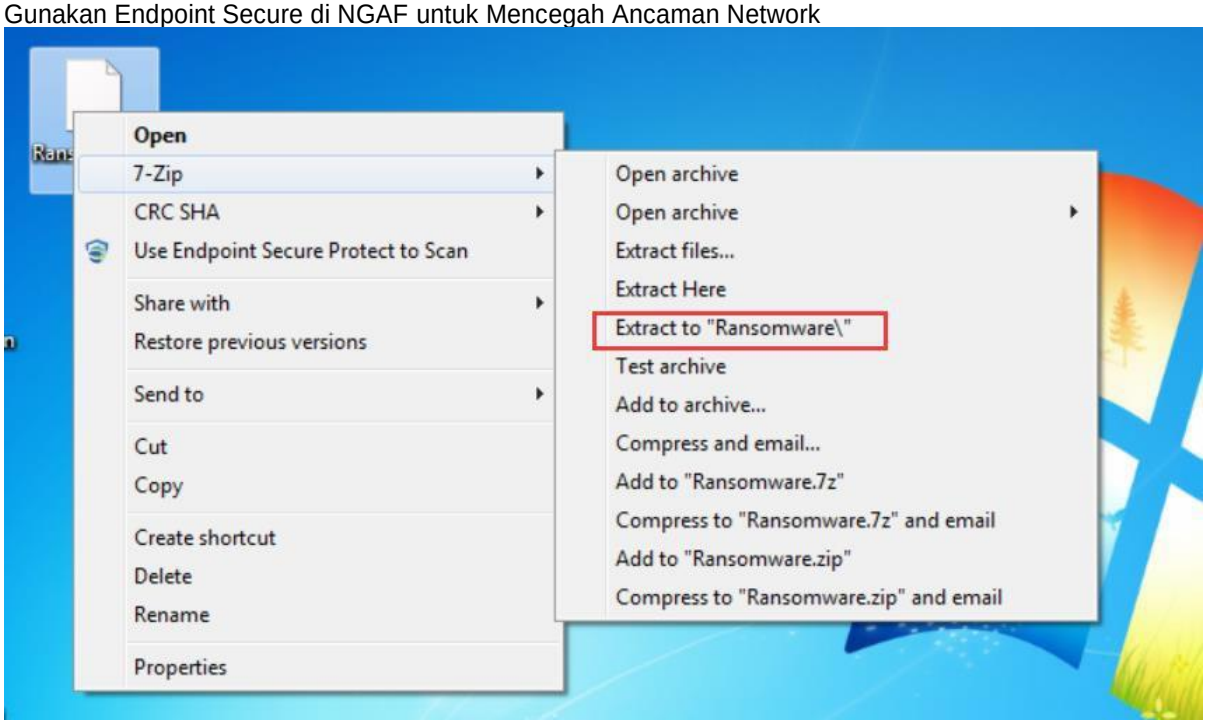
Bab 4 Anti Virus

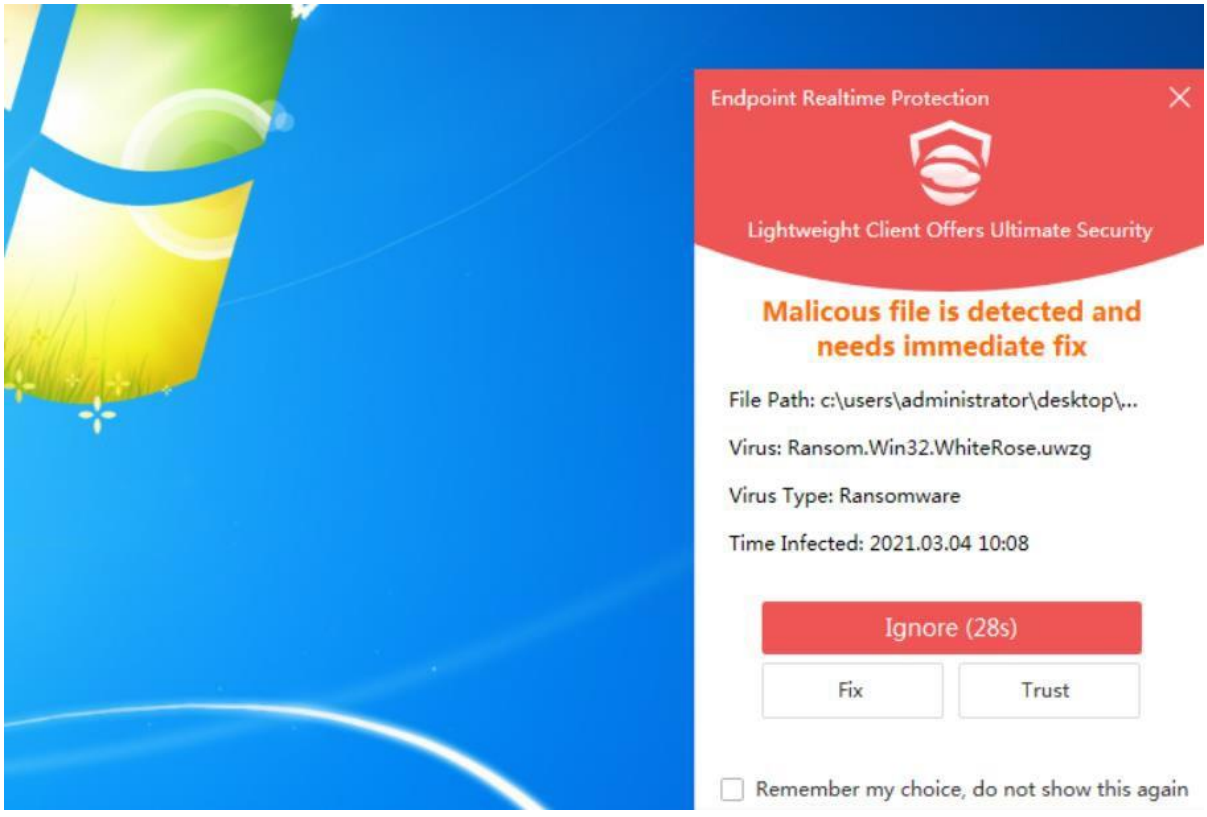
4.1 Realtime Detection dari Ransomware

1. Jika Anda ingin anti ransomware, Harap enable real-time protection dan enable detection ransomware.



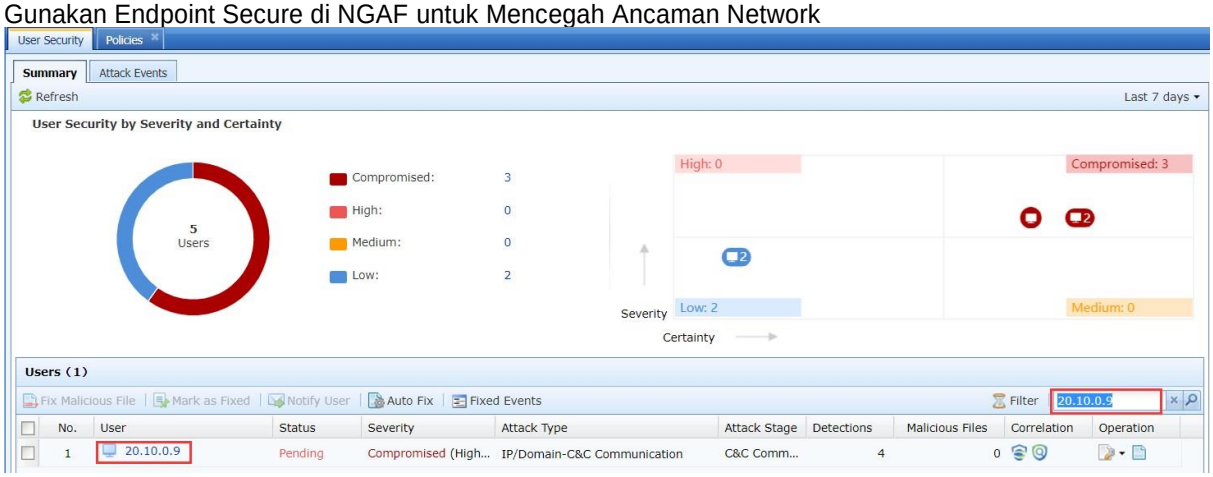
2. Setelah Anda dekompresi file virus, Anda dapat melihat bahwa ES agent telah mendeteksi dan memperingatkan.

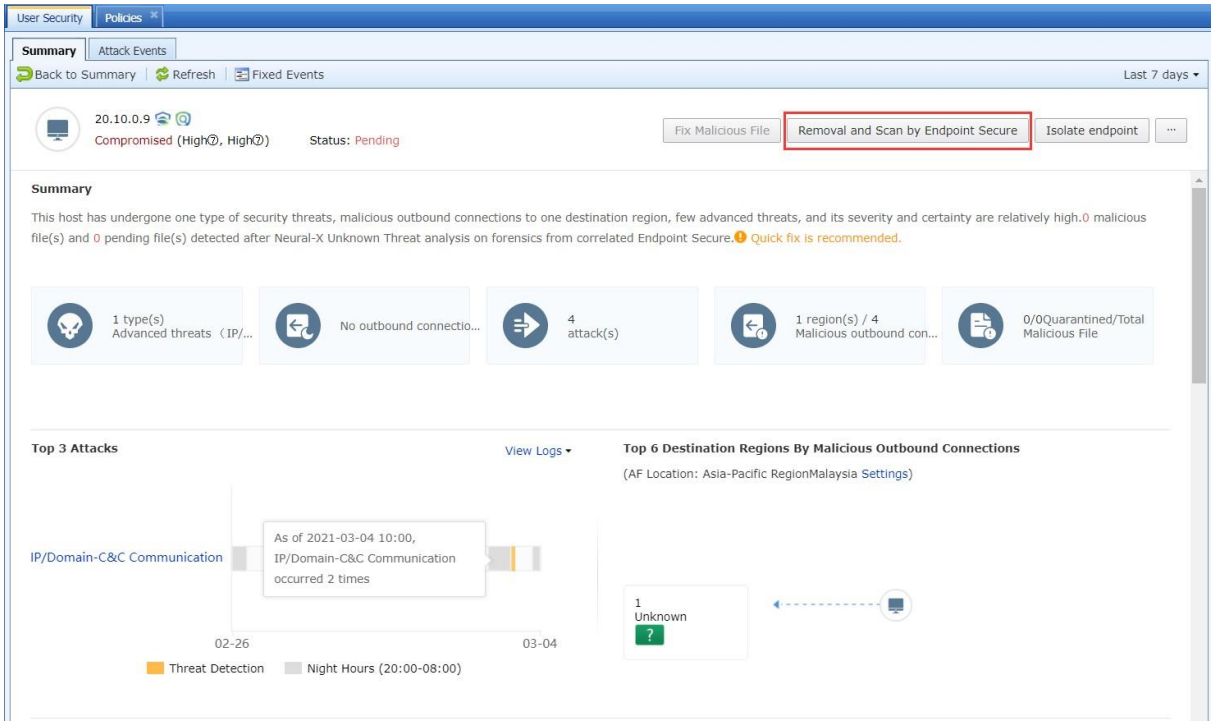




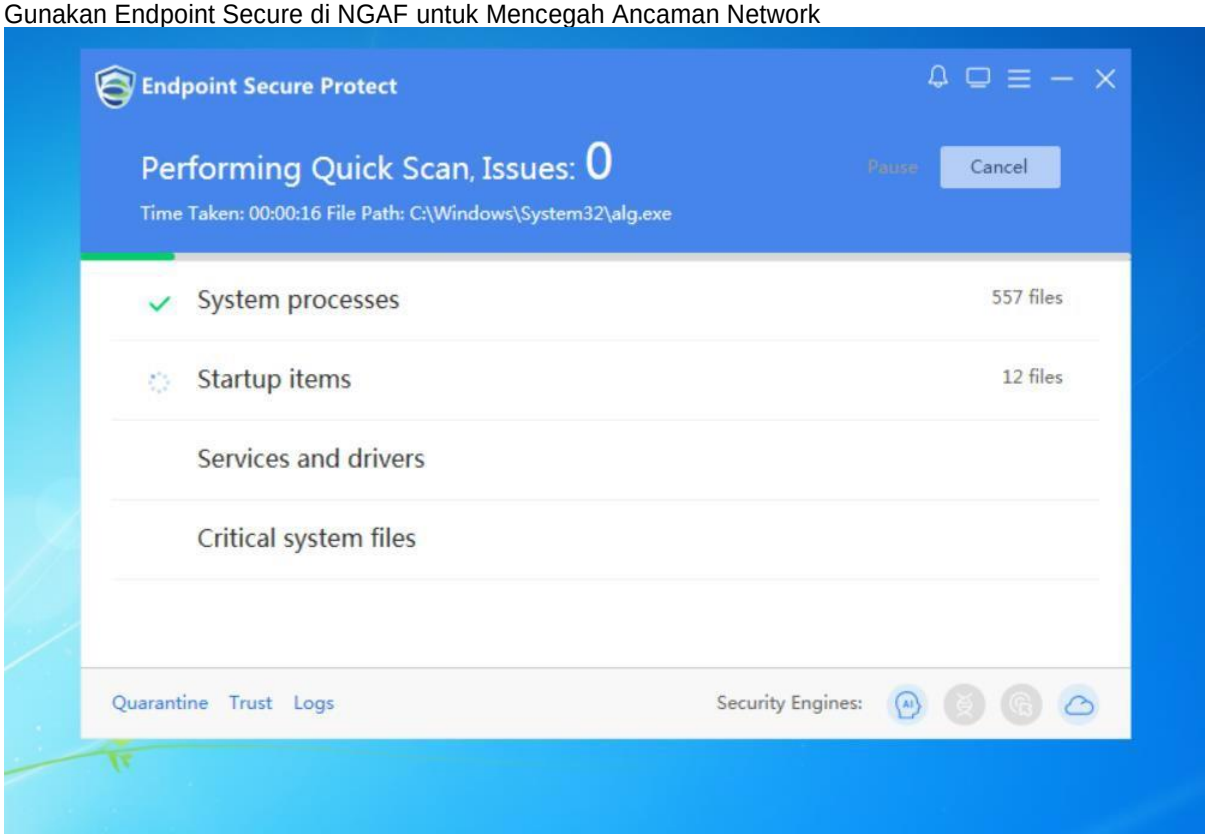
4.2 Korelasi dengan NAGF ke Anti Botnet

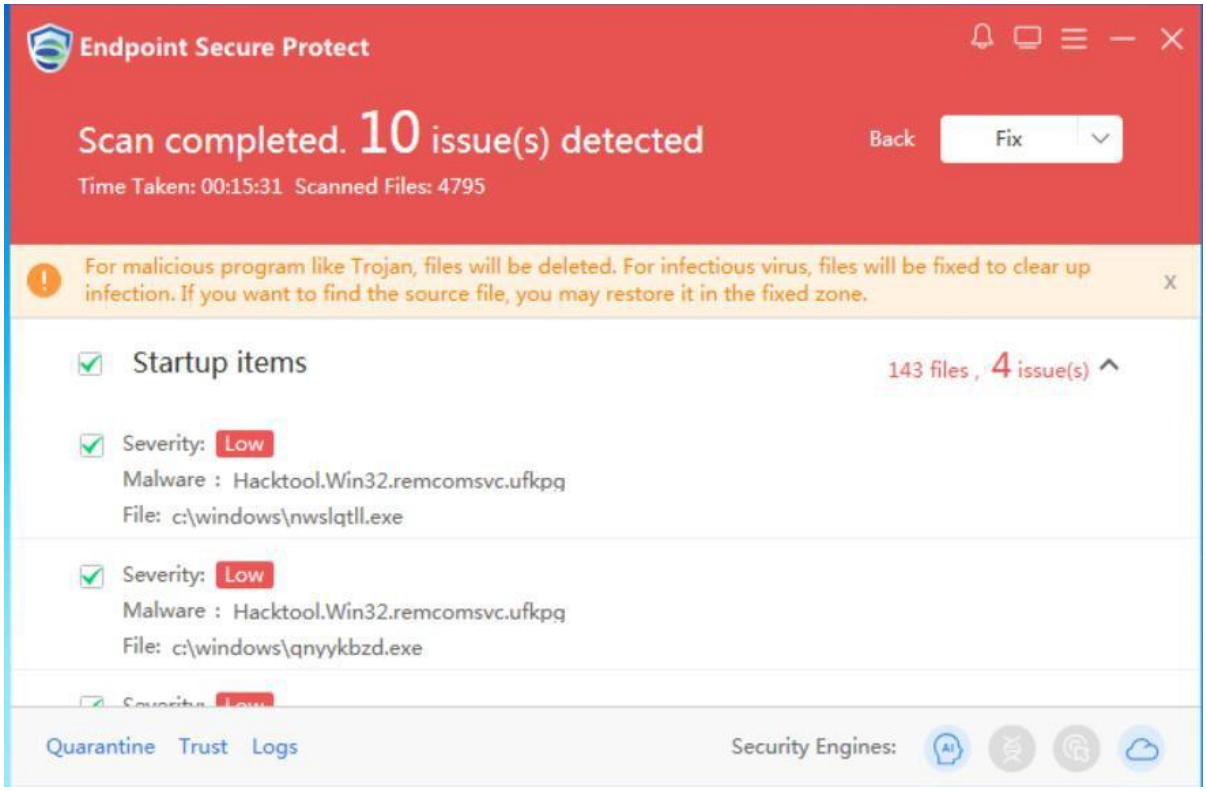
1. Jika PC terinfeksi oleh botnet dan NGAF mendeteksi aktivitas botnet, Anda dapat korelasi ke ES untuk scan seluruh disk pada NGAF.



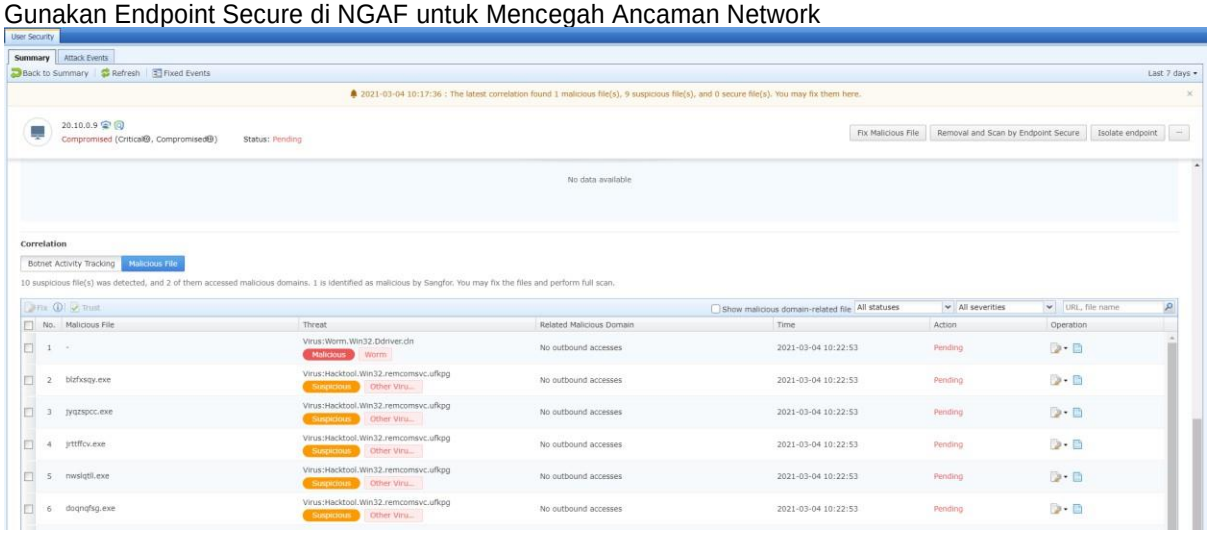


2. Kemudian Anda dapat melihat scan task telah dimulai di ES agent.

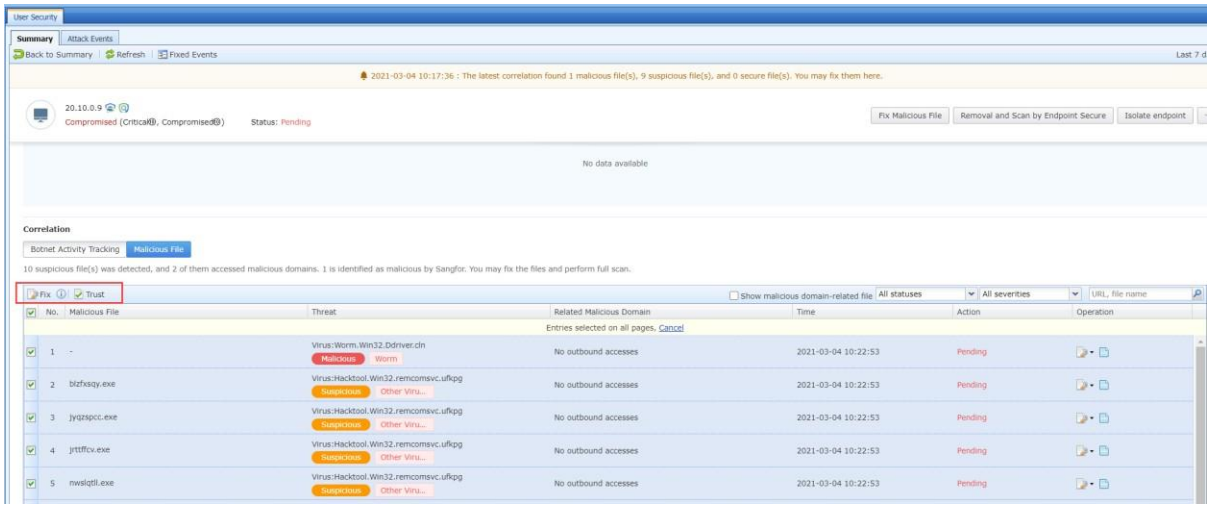




3. Setelah ES Agent selesai scan task, Anda dapat melihat file botnet dan proses informasi di NGAF web console.



4. Anda dapat memilih tindakan yang berbeda untuk proses virus.



5. Setelah memperbaiki semua file virus, Anda dapat melihat event yang diperbaiki.