



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

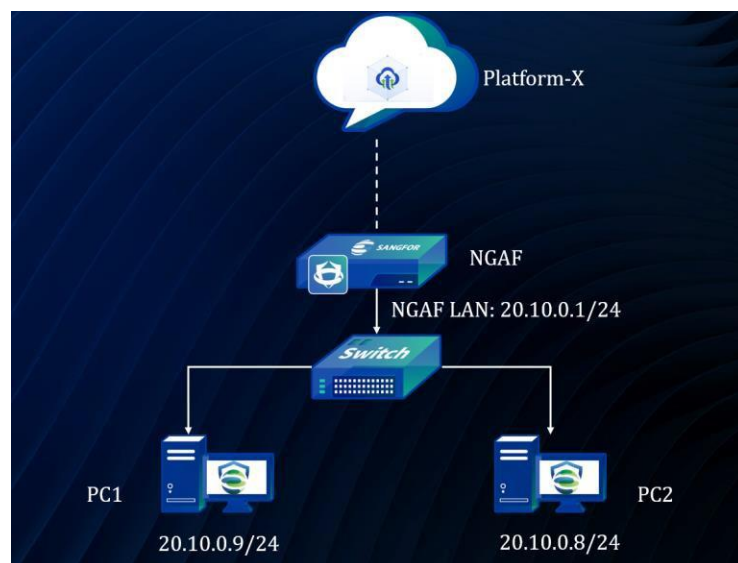
| | |
|---|----|
| Bab 1 Skenario | 1 |
| 1.1 Skenario..... | 1 |
| 1.2 Topologi | 1 |
| 1.3 Pengenalan Tes..... | 1 |
| 1.3.1 Kondisi Tes | 2 |
| Bab 2 Login ke Platform-X dan Buat branch | 2 |
| 2.1 Login Platform-X | 2 |
| 2.2 Buat perangkat branch di Platform-X..... | 3 |
| 2.3 Connect NGAF ke Sangfor Platform-X..... | 5 |
| 2.4 Activate Endpoint Secure di NGAF | 6 |
| Bab 3 Instal Agent dan Konfigurasi Policy | 6 |
| Bab 4 Anti Virus | 10 |
| 4.1 Realtime Detection dari Ransomware | 10 |
| 4.2 Korelasi dengan NAGF ke Anti Botnet | 12 |

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 ingin 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 |

Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network

1.3 Pengenalan Tes

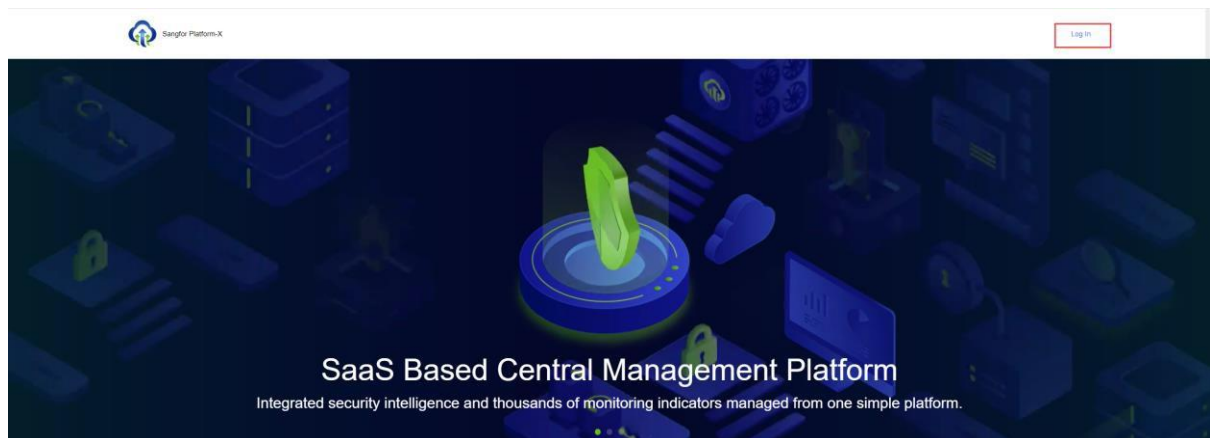
1.3.1 Kondisi Tes

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

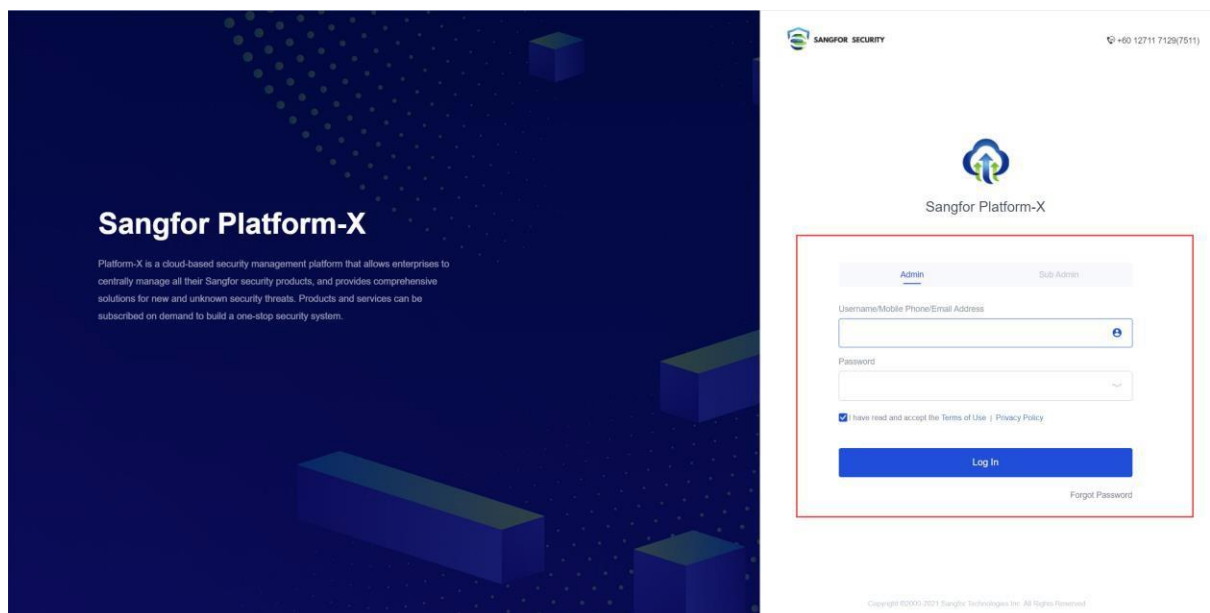
Bab 2 Login ke Platform-X dan Buat branch

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.

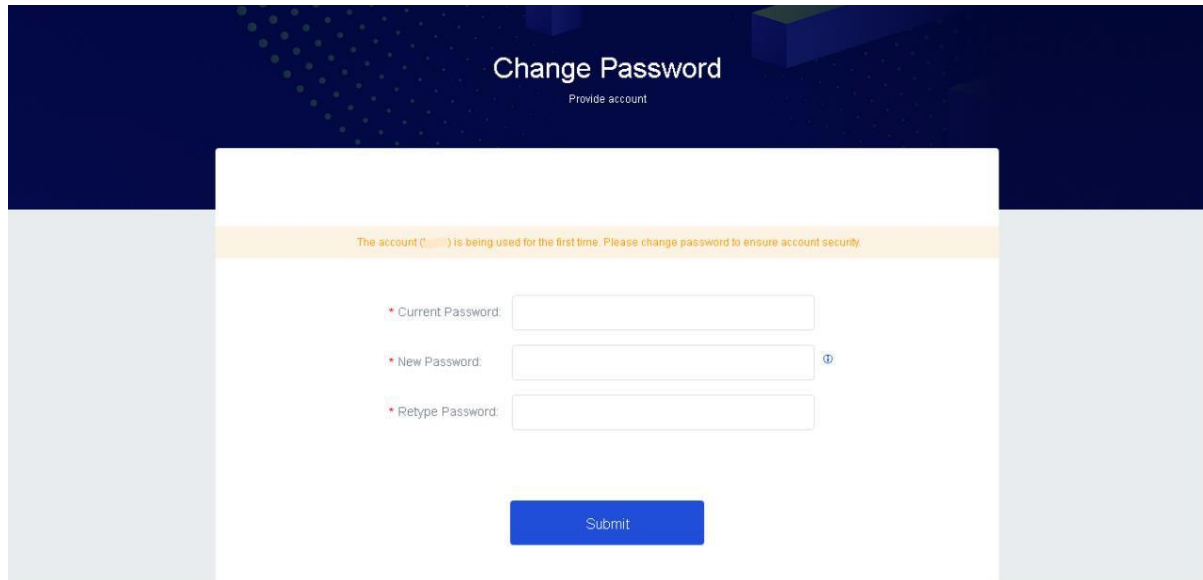


2. Setelah Anda klik log in, Anda akan mengarahkan ke halaman berikut. Anda dapat input akun name dan password untuk login.

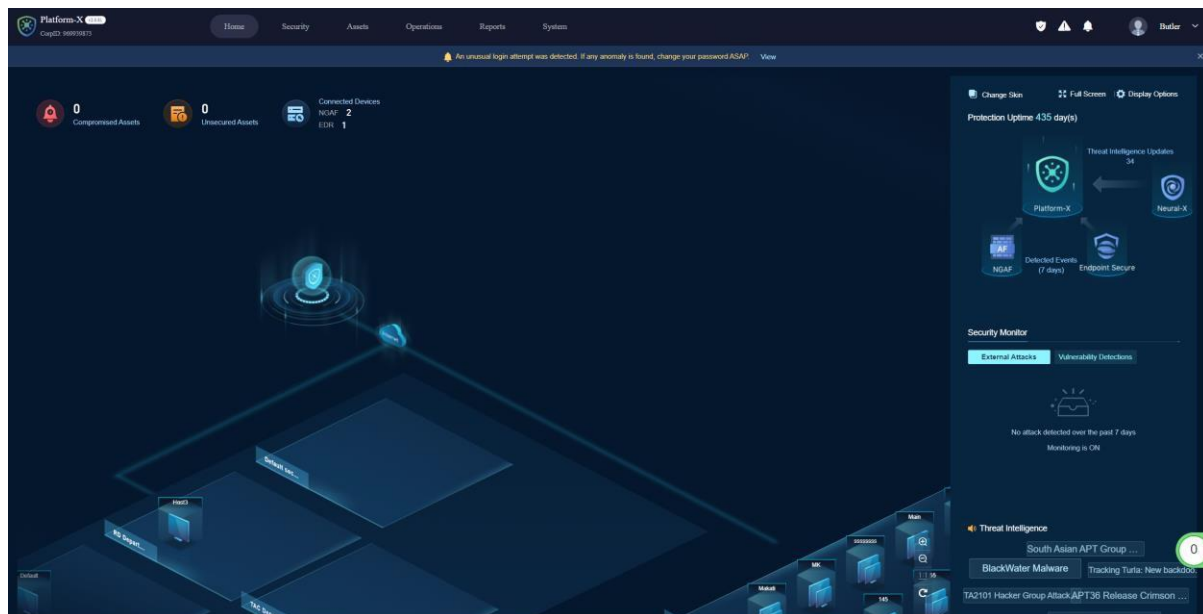


Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network

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



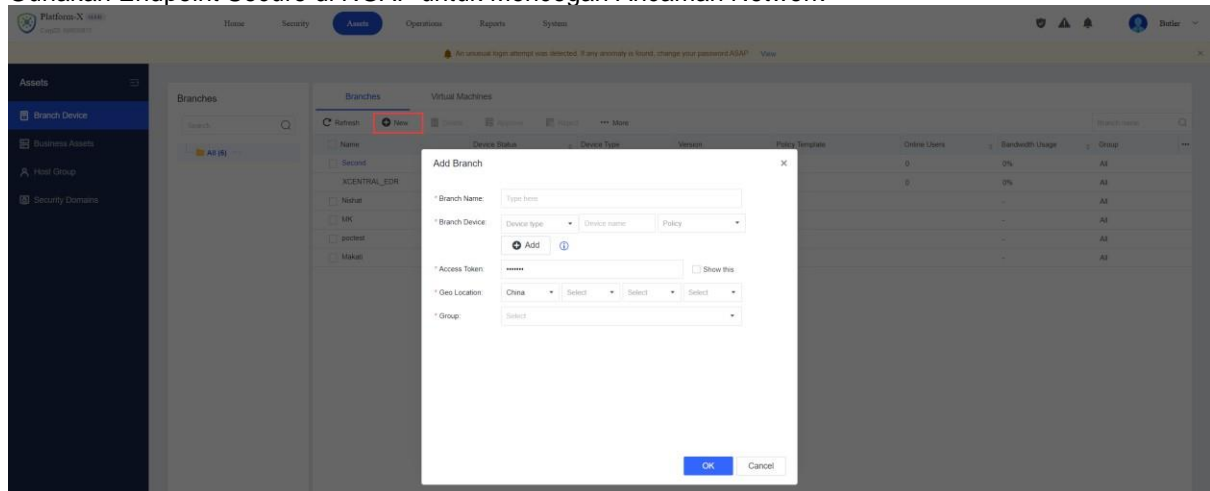
4. Halaman berikut adalah homepage dari Platform-X.



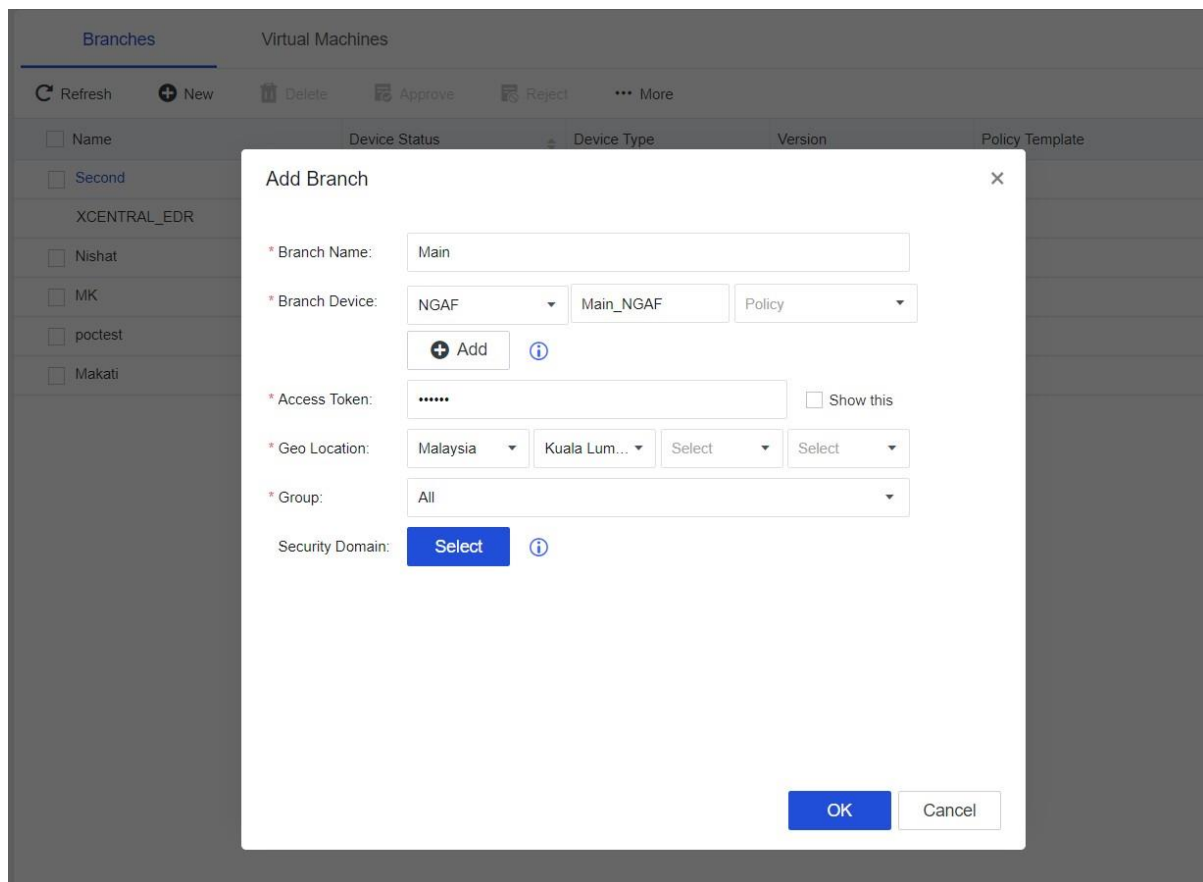
2.2 Buat perangkat branch di Platform-X

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

Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network



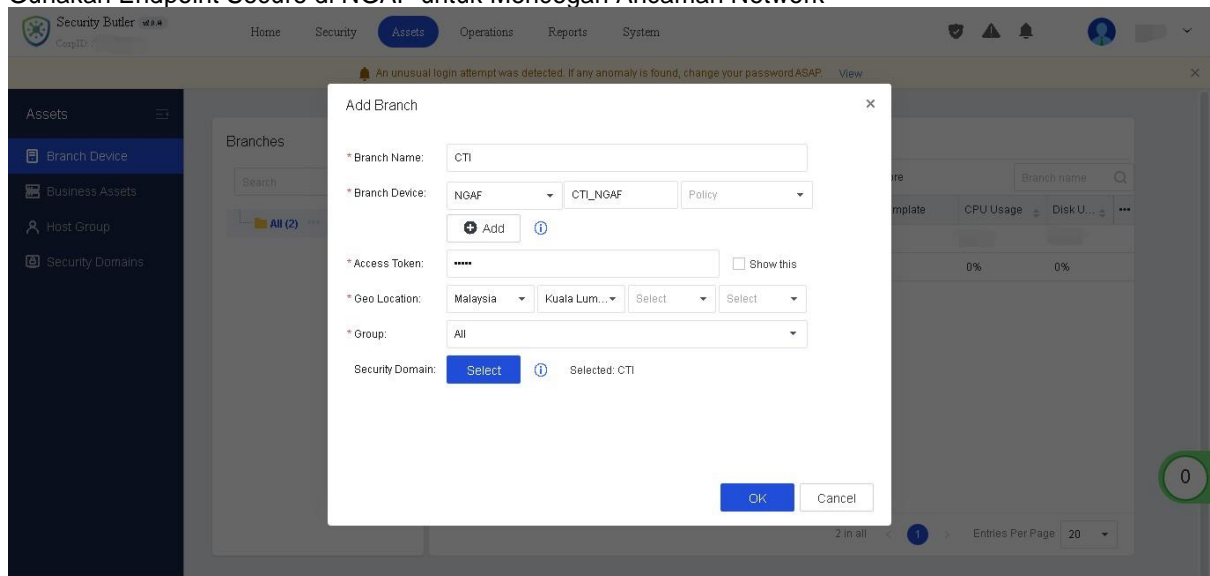
2. Input branch name, branch device type, access token, pilih lokasi perangkat dan pilih group.



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

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

Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network



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

Branches

Virtual Machines

Refresh

New

Delete

Approve

Reject

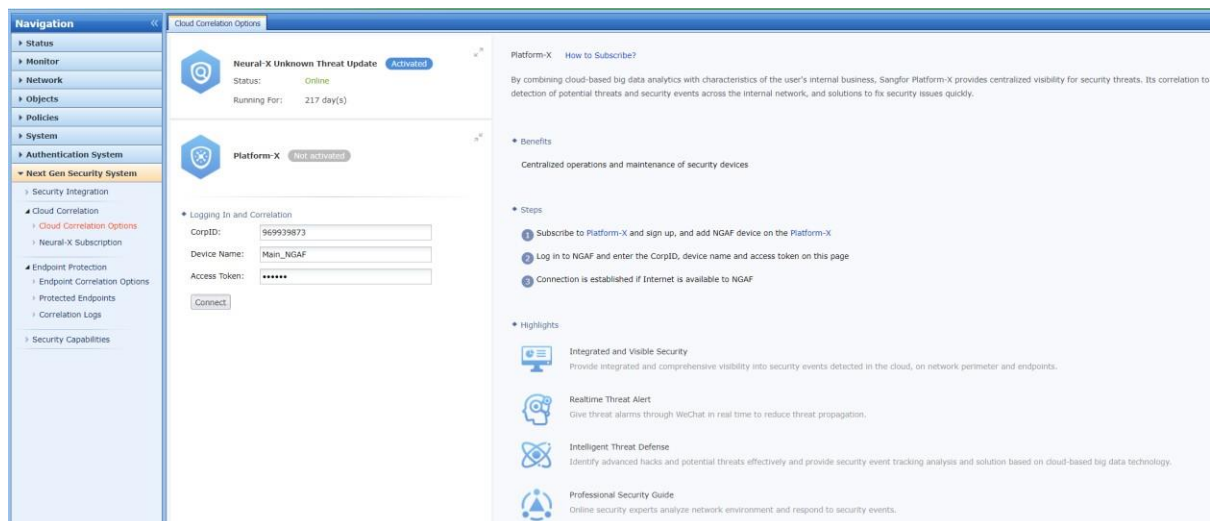
More

| <div><input type="checkbox"/></div> <div>Name</div> | <div><div></div></div> <div>Device Status</div> | <div><div></div></div> <div>Device Type</div> | Version | Policy Template | Online Users |
|--|---|---|-------------|-----------------|--------------|
| <div><input type="checkbox"/></div> <div>Second</div> | <div><div></div></div> <div>Normal</div> | <div>NGAF</div> | 8.0.26 | - | 0 |
| <div></div> <div>XCENTRAL_EDR</div> | <div><div></div></div> <div>Normal</div> | EDR | 3.2.15.2208 | - | 0 |
| <div><input type="checkbox"/></div> <div>Nishat</div> | <div><div></div></div> <div>Inactivated</div> | NGAF | - | - | |
| <div><input type="checkbox"/></div> <div>MK</div> | <div><div></div></div> <div>Inactivated</div> | NGAF | - | - | |
| <div><input type="checkbox"/></div> <div>pocrest</div> | <div><div></div></div> <div>Inactivated</div> | NGAF | - | - | |
| <div><input type="checkbox"/></div> <div>Makati</div> | <div><div></div></div> <div>Inactivated</div> | NGAF | - | - | |
| <div><input type="checkbox"/></div> <div>Main</div> | <div><div></div></div> <div>Inactivated</div> | NGAF | - | - | |

2.3 Connect NGAF ke Sangfor Platform-X

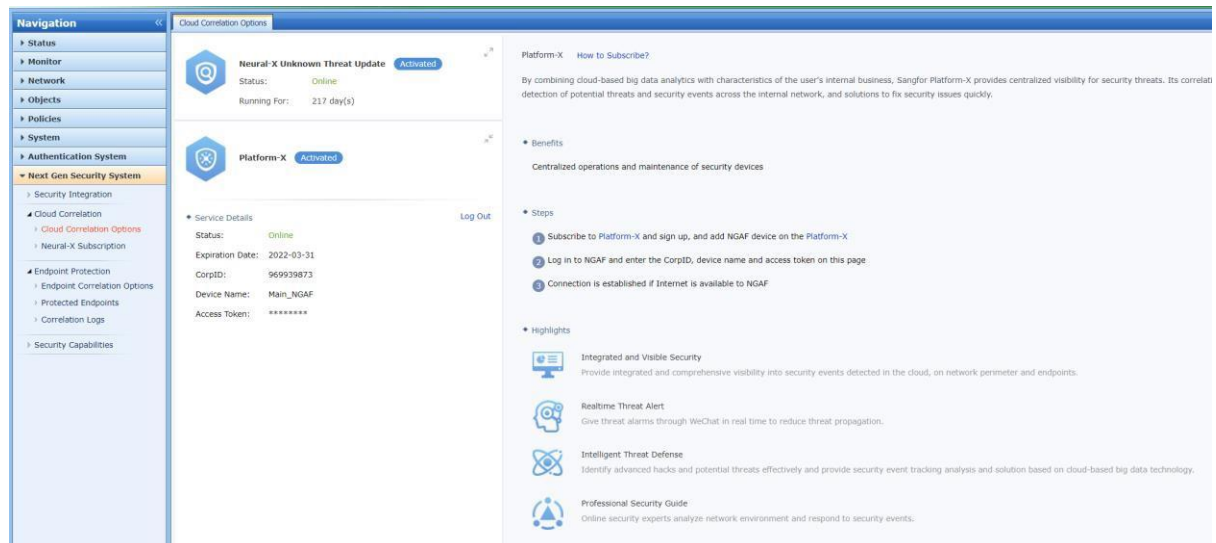
Akses NGAF Web console, pergi ke Next Gen Security System -> Cloud Correlation -> Cloud Correlation Options, pilih Platform-X.

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.

Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network



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.

Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network

Navigation

- Status
- Monitor
- Network
- Objects
- Policies
- System
- Authentication System
- Next Gen Security System**
 - Security Integration
 - Cloud Correlation
 - Endpoint Protection**
 - Endpoint Correlation Options**
 - Security Protection
 - Protected Endpoints
 - Correlation Logs
 - Update
 - Security Capabilities

Endpoint Correlation Options System

Endpoint Secure **Activated**

Licensed Functionality

- Virus Scan / Realtime Monitoring / Quarantine File /
- Endpoint Isolation / Intelligent Correlated Response /
- APT Detection /

Service Details

Connection Method: Endpoint Secure on NGAF [Log Out](#)

Expiration Date: 2021-06-17 (Remaining: 112 days)

Endpoint License

Windows Hosts (Used/Total): 1 / 10

Windows Servers (Used/Total): 0 / 10

Linux Servers (Used/Total): 0 / 10

Quick Widgets

[Agent Deployment](#) Get Endpoint Secure installer and deploy

[Renew License](#) Update license to renew subscription service

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

Endpoint Secure Integration [How to Subscribe?](#)

Correlate NGAF with Endpoint Secure to share security information, visualize threats and take action across platforms.

Agent Deployment

Notes:

Download the installer and do not change its name because the Endpoint Secure manager IP address is written in the installer. When the agent is installed, it will be connected to Endpoint Secure manager on NGAF automatically.

Steps:

1. Select zones, interfaces and connected IP addresses for agent to be connected to NGAF and get corresponding installer.
2. Distribute the installers to corresponding users based on the connected IP address. (Users download and install the agent via different connected IP addresses)

Select zones and IP addresses to connect to Endpoint Secure:

Select zone: Select interface: Connected IP address: [Add](#)

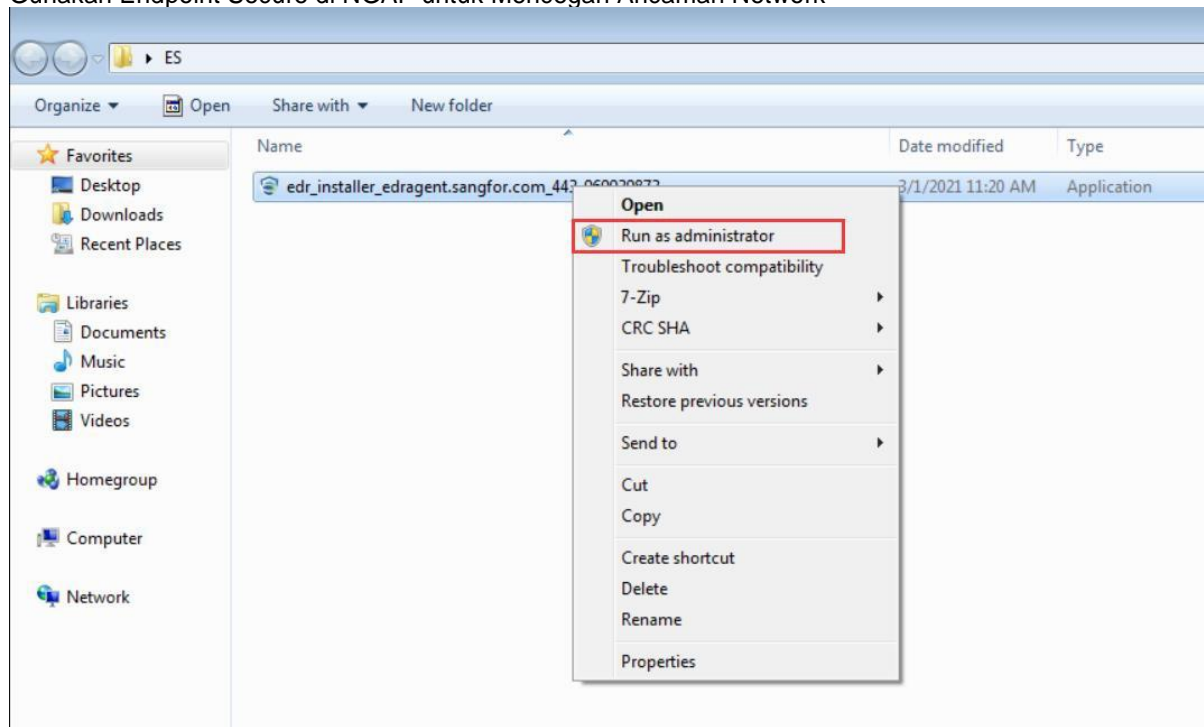
| No. | Zone | Interfaces | Connected IP Address | Installer (Windows OS) | Installer (Linux OS) | Download Link | Open |
|-----|------|------------|----------------------|------------------------|----------------------|---------------|------|
| 1 | lan | eth2 | 192.168.11.1/24 | Download | Download | Copy | X |

[Agent Deployment](#) Get Endpoint Secure installer and deploy

[Renew License](#) Update license to renew subscription service

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

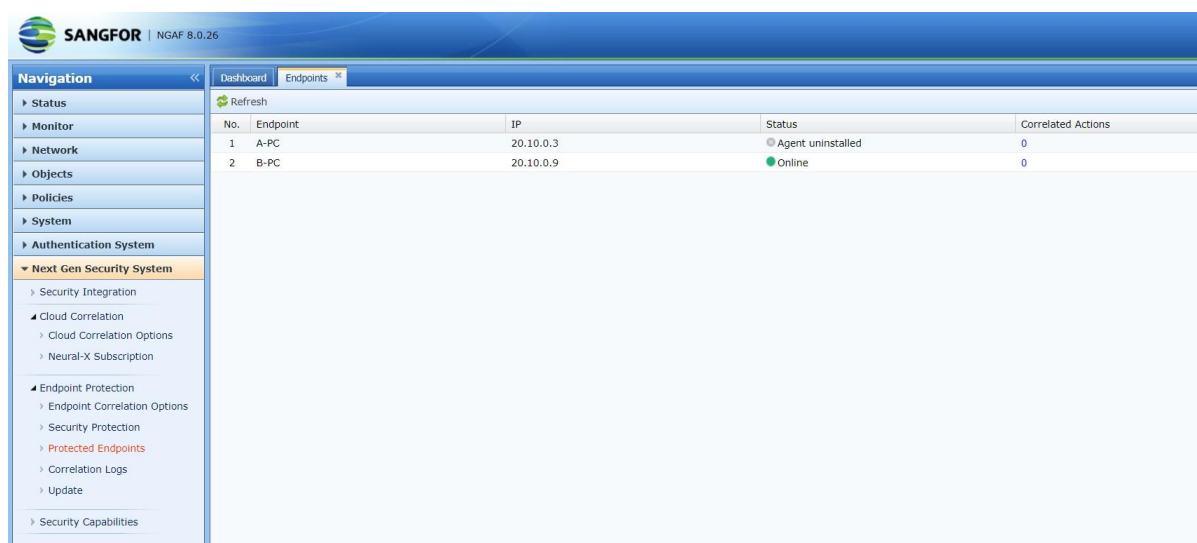
Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network



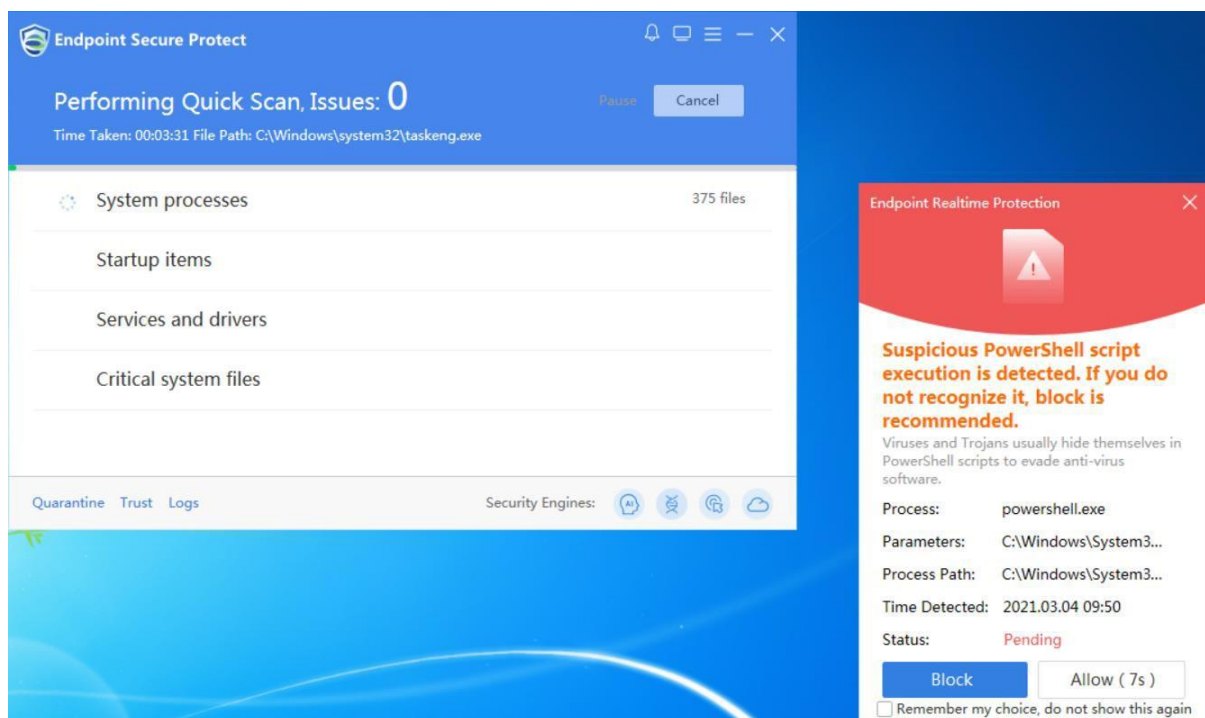
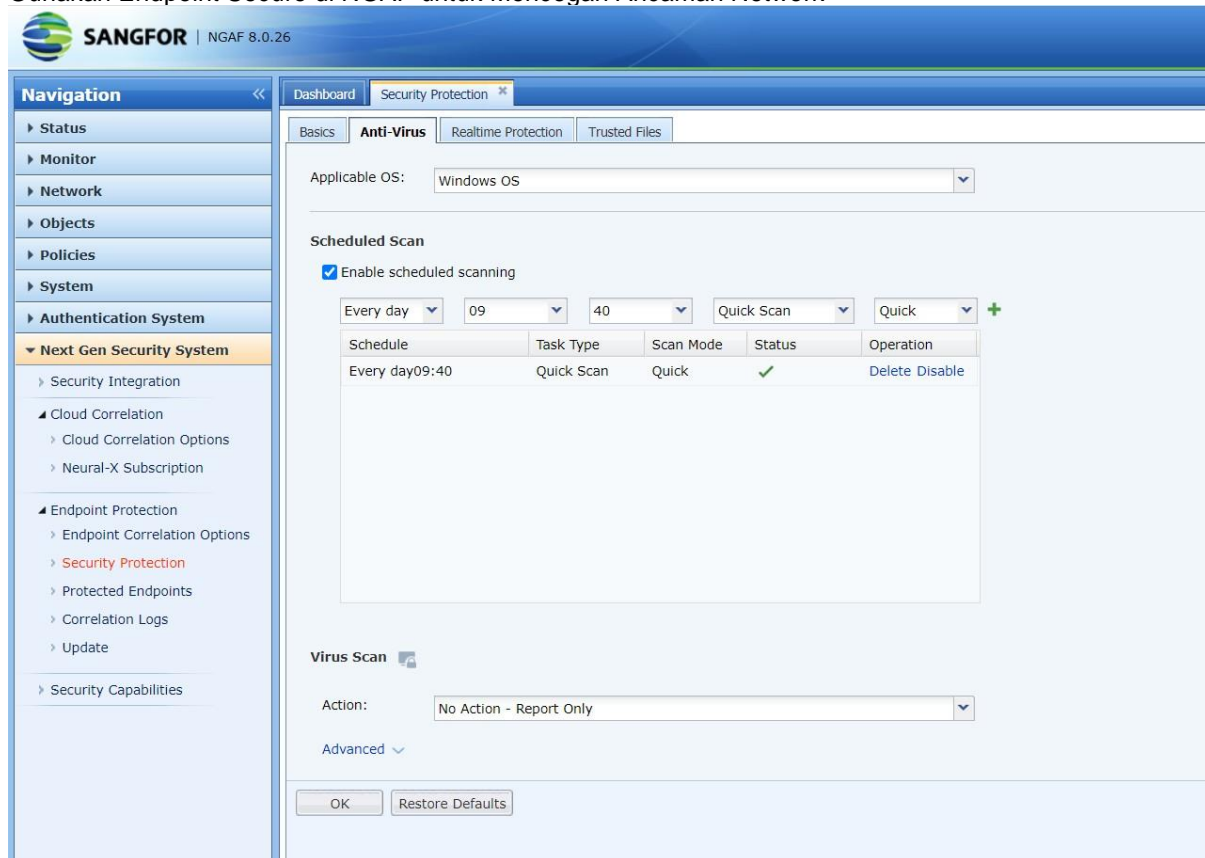
Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network



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.

SANGFOR | NGAF 8.0.26

Navigation

- Status
- Monitor
- ▼ **Network**
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - SSLVPN
 - IPSecVPN
- Objects
- Policies
- System
- Authentication System
- Next Gen Security System

Dashboard | **Security Protection** x

Basics | Anti-Virus | **Realtime Protection** | Trusted Files

Applicable OS: Windows OS ⓘ

Realtime Protection ⓘ

☒ Enable realtime protection

Action: No Action - Report Only ▼

Protection Level: ☐ High ☒ Medium ☐ Low

Monitor execution and write actions on files, preventing virus intrusion and execution. Low performance impact.

File Type: ☒ Documents ☒ Script
☒ Executable ☒ Compressed ⓘ

File Scan: Skip files larger than 50 MB
 Scan compressed files up to 3 layers deep

Engine: ☒ Sangfor Engine Zero ☒ Gene Engine ⓘ
☒ Cloud-Based Engine

Tip: Enable more engines to improve virus detection but it may impact system performance.

Collapse ^

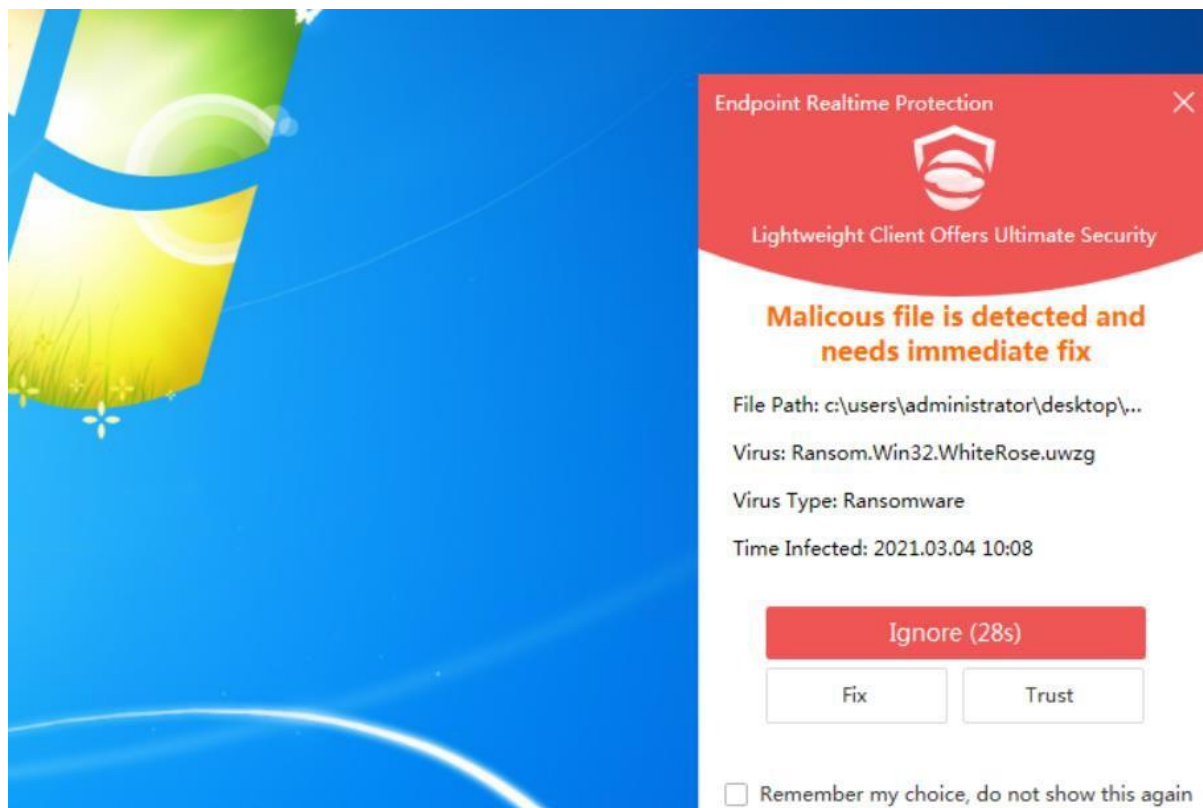
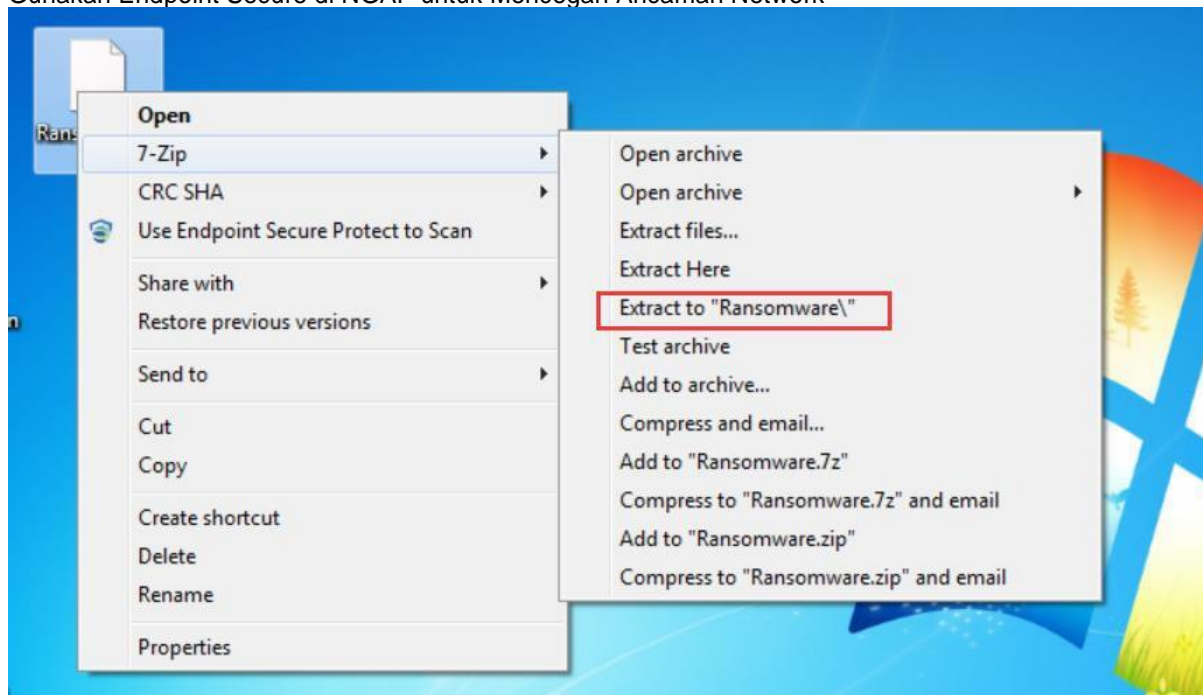
Ransomware Detection ⓘ

☒ Enable detection

Action: Manual ▼

OK Restore Defaults

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



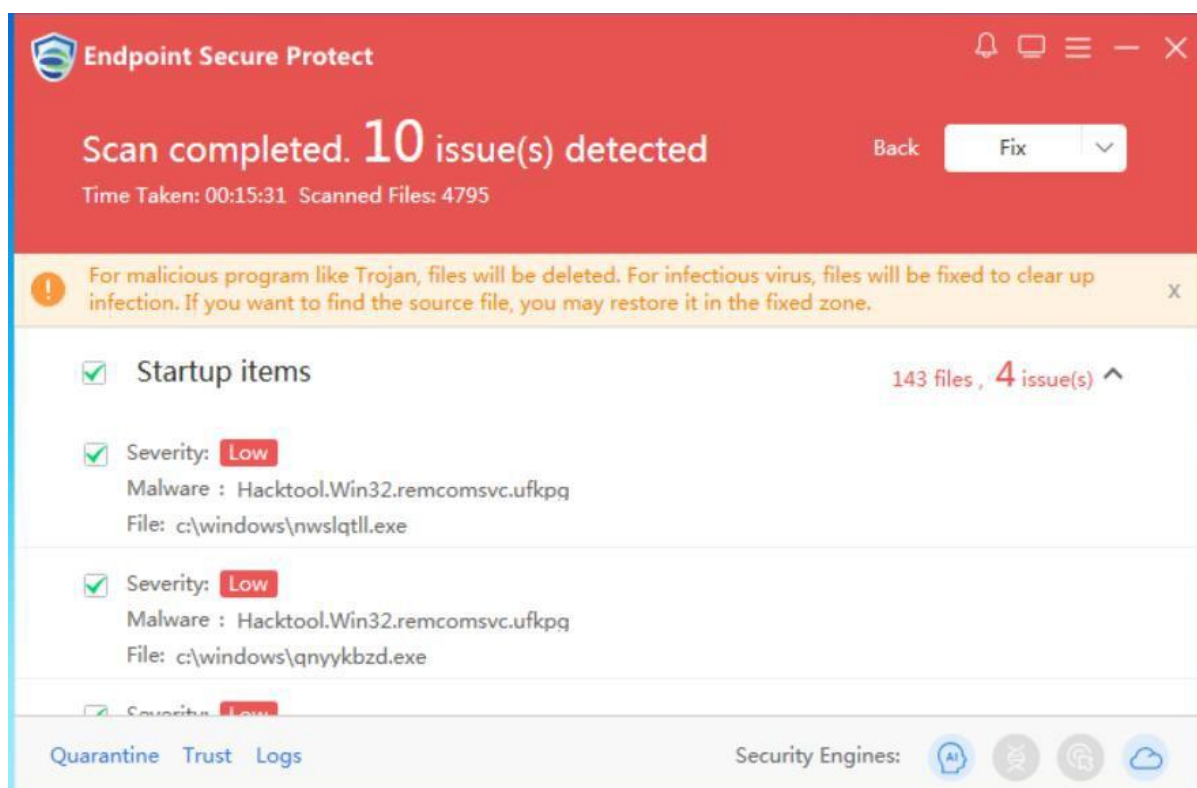
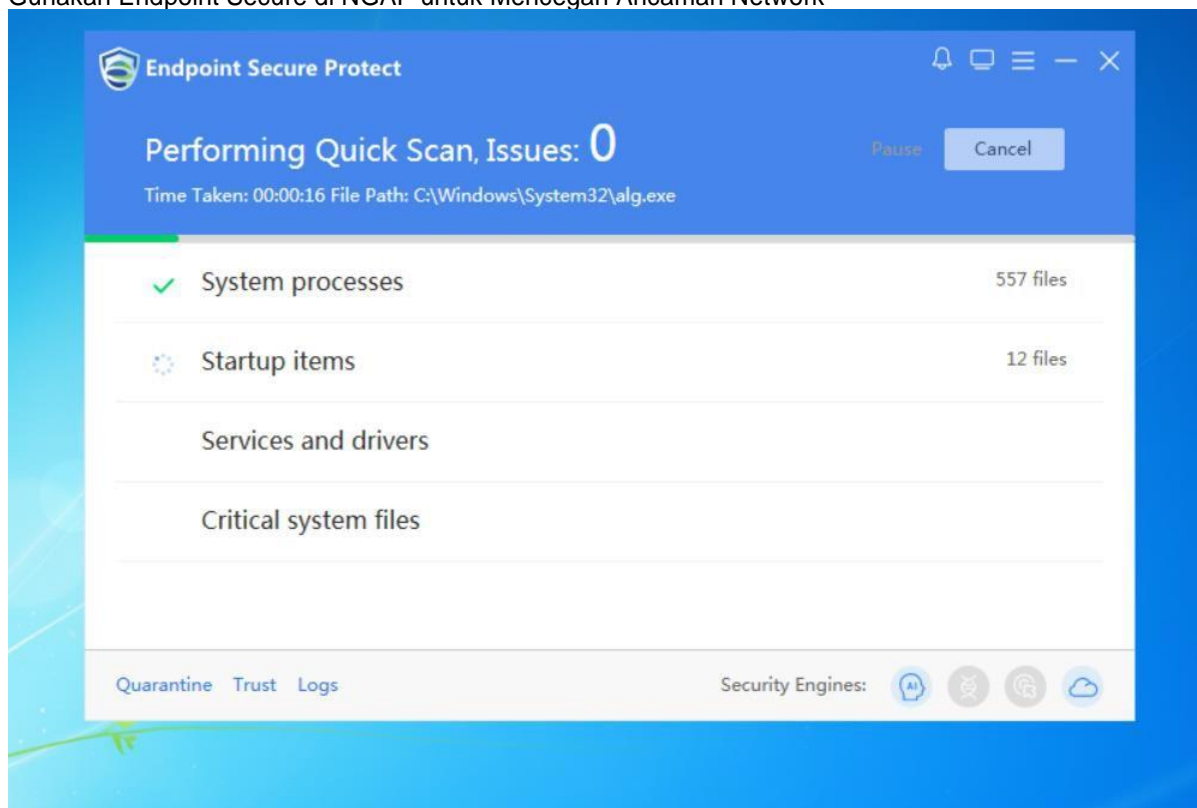
4.2 Korelasi dengan NAGF ke Anti Botnet

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

Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network

The screenshot displays the 'User Security' interface in Sangfor NGAF. The top section, 'User Security by Severity and Certainty', features a donut chart showing 5 users: 3 Compromised (red), 0 High (orange), 0 Medium (yellow), and 2 Low (blue). A matrix on the right shows counts for severity and certainty levels. Below this, the 'Users (1)' table lists user 20.10.0.9 with a 'Pending' status and 'Compromised (High...)' severity. The interface includes various action buttons like 'Fix Malicious File', 'Mark as Fixed', 'Notify User', 'Auto Fix', and 'Fixed Events'. A filter is set to '20.10.0.9'. The detailed view for user 20.10.0.9 shows a 'Compromised (High, High)' status and a 'Pending' status. It includes a 'Summary' section with a warning: 'This host has undergone one type of security threats, malicious outbound connections to one destination region, few advanced threats, and its severity and certainty are relatively high. 0 malicious file(s) and 0 pending file(s) detected after Neural-X Unknown Threat analysis on forensics from correlated Endpoint Secure. Quick fix is recommended.' Below the summary are five key metrics: 1 type(s) Advanced threats (IP/...), No outbound connectio..., 4 attack(s), 1 region(s) / 4 Malicious outbound con..., and 0/0 Quarantined/Total Malicious File. The 'Top 3 Attacks' section shows 'IP/Domain-C&C Communication' as the top threat. The 'Top 6 Destination Regions By Malicious Outbound Connections' section shows '1 Unknown' as the top region. A timeline at the bottom indicates 'IP/Domain-C&C Communication' occurred 2 times as of 2021-03-04 10:00.

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.

Gunakan Endpoint Secure di NGAF untuk Mencegah Ancaman Network

The screenshot shows the 'User Security' interface with a 'Summary' tab. A notification at the top states: '2021-03-04 10:17:36 : The latest correlation found 1 malicious file(s), 9 suspicious file(s), and 0 secure file(s). You may fix them here.' Below this, a table lists suspicious files and their associated threats.

| No. | Malicious File | Threat | Related Malicious Domain | Time | Action | Operation |
|-----|----------------|---|--------------------------|---------------------|---------|-----------|
| 1 | - | Virus:Worm.Win32.DdDriver.dh Malicious Worm | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 2 | blfzsqy.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 3 | jyqzspcc.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 4 | jrttfcv.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 5 | nswlqtl.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 6 | dsqzpfqg.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |

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

The screenshot shows the 'User Security' interface with the 'Fixed Events' tab selected. A notification at the top states: '2021-03-04 10:17:36 : The latest correlation found 1 malicious file(s), 9 suspicious file(s), and 0 secure file(s). You may fix them here.' Below this, a table lists fixed events.

| No. | Malicious File | Threat | Related Malicious Domain | Time | Action | Operation |
|-----|----------------|---|--------------------------|---------------------|---------|-----------|
| 1 | - | Virus:Worm.Win32.DdDriver.dh Malicious Worm | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 2 | blfzsqy.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 3 | jyqzspcc.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 4 | jrttfcv.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |
| 5 | nswlqtl.exe | Virus:Hacktool.Win32.remcomavc.ufpg Suspicious Other Virus... | No outbound accesses | 2021-03-04 10:22:53 | Pending | |

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

The screenshot shows the 'User Security' interface with the 'Fixed Events' tab selected. A notification at the top states: '2021-03-04 10:48:07 : The latest correlation has fixed 9 file(s).' Below this, a table lists fixed events.

| No. | Time | Host IP | Details | Type | Admin | Remark | Operation |
|-----|---------------------|-----------|-------------------------------------|---------------------------|-------|--------|-----------|
| 1 | 2021-03-04 10:48:07 | 20.10.0.9 | 10 process files have been quara... | Fix | admin | - | |
| 2 | 2021-03-04 10:17:36 | 20.10.0.9 | Perform virus scan and removal o... | Removal and Scan by En... | admin | - | |



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