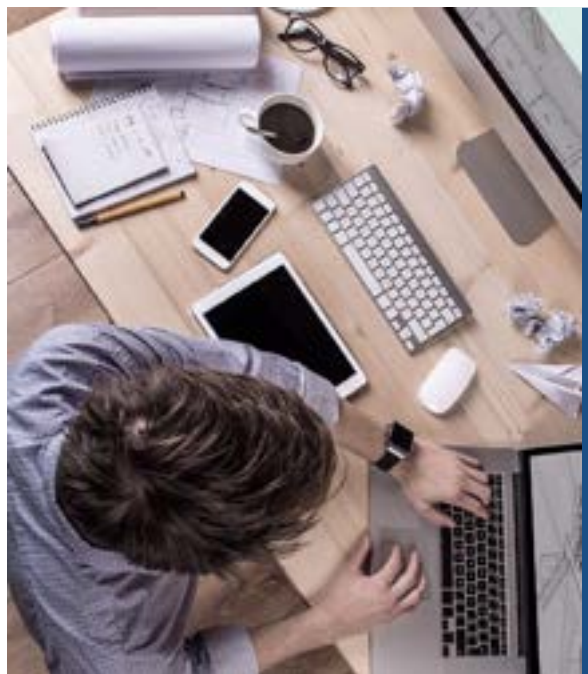




SANGFOR NGAF V8.0.47 Professional

Endpoint Protection





- 1 Endpoint Secure Correlation
- 2 Endpoint Correlation Options
- 3 Application Scenario

1. Introduction

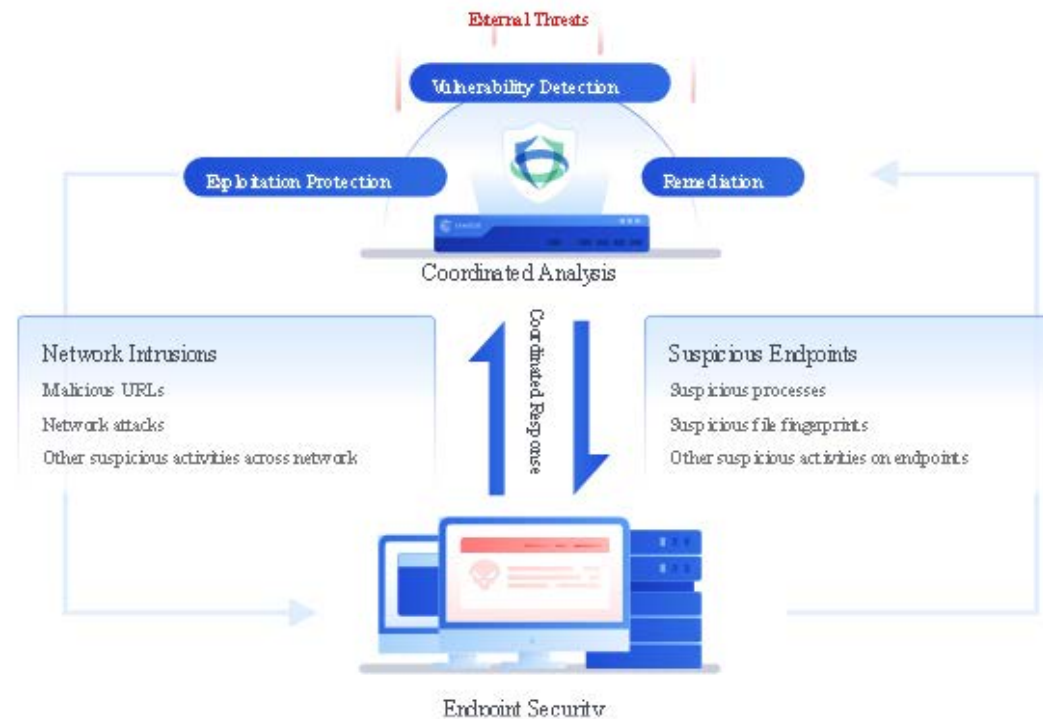


SANGFOR
深信服科技

Introduction



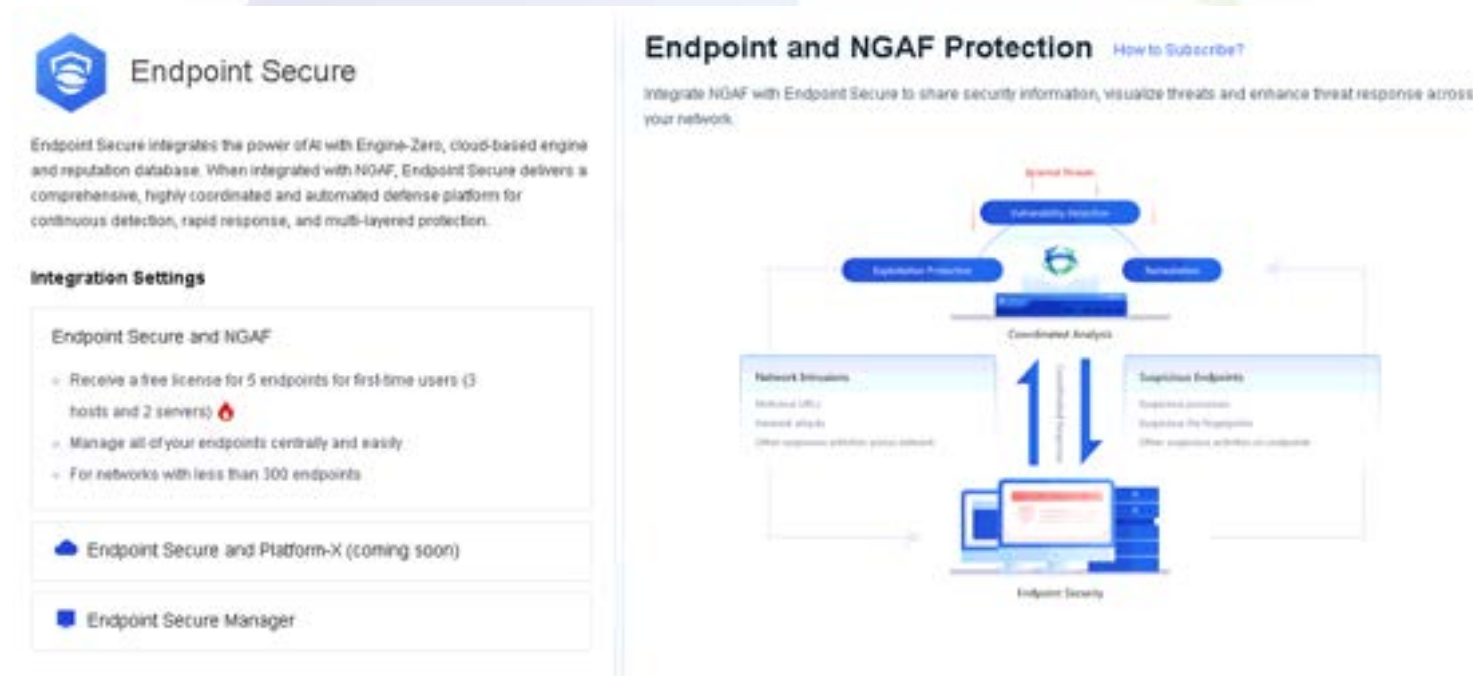
Endpoint and NGAF Protection enables the ES to share security information with the NGAF, thus implementing the association of network and endpoint security information, which can make threats more detectable and easier to handle.



Introduction



Endpoint protection options can be configured to realize the correlation between Endpoint Secure and NGAF. Sangfor Endpoint Secure (ES) is equipped with the Engine Zero engine, behavioral engine, cloud engine, and reputation library, which continuously performs detection and responds and deals with threats in a quick manner, building a comprehensive and effective terminal threat handling platform. NGAF can cooperate with ES to automatically deal with threats, forming a multilevel and multidimensional threat defense system. Endpoint Protection Options include three connection methods: Endpoint Secure and NGAF, Endpoint Secure and Platform X, and Endpoint Secure Manager.



2. Endpoint Correlation Options



SANGFOR
深信服科技

Endpoint Correlation Options



2.1. Endpoint Secure and NGAF

After subscribing to the Endpoint Secure and NGAF in Platform-X -Services, NGAF implements the cooperation with ES by connecting to Platform-X, and can quickly deploy the ES without using additional server resources. At the same time, the endpoint ES management policy can be quickly configured in the NGAF without switching platforms.

The screenshot displays the 'Endpoint Secure' configuration page. On the left, under 'Integration Settings', the 'Connection Method' is set to 'Endpoint Secure and NGAF'. The status is 'Waiting for connection', with a note that Platform-X is connected and the Endpoint Secure Manager is found. A 'Connect' button is visible. The main content area is titled 'Endpoint and NGAF Protection' and includes a 'Benefits' section, an 'Apply for Free Trial' section with a 3-step process, and a 'Steps' section with 3 numbered instructions. A diagram on the right shows the data flow between NGAF and Endpoint Secure, with a legend indicating green arrows for Endpoint Secure data transmission and blue arrows for NGAF data transmission.

Endpoint Correlation Options



2.2. Endpoint Secure and Platform-X

Endpoint Secure and Platform-X connection deploy the ES management platform on Platform-X. NGAF can cooperate with ES after both of them being bound to Platform-X.



Endpoint Secure

Endpoint Secure integrates the power of AI with Engine-Zero, cloud-based engine and reputation database. When integrated with NGAF, Endpoint Secure delivers a comprehensive, highly coordinated and automated defense platform for continuous detection, rapid response, and multi-layered protection.

Integration Settings

Connection Method: Endpoint Secure and Platform-X

Status: Waiting for connection

No cloud-based Endpoint Secure subscription was found.

[Back](#)

Endpoint and NGAF Protection How to Subscribe?

Integrate NGAF with Endpoint Secure to share security information, visualize threats and enhance threat response across your network.

- **Benefits**

Strengthen NGAF's detection capability for endpoints, track botnet activities, and fix malicious files directly from NGAF.

Endpoint Secure and Platform-X

Integrate NGAF with Endpoint Secure by connecting to Platform-X.

- **Steps**

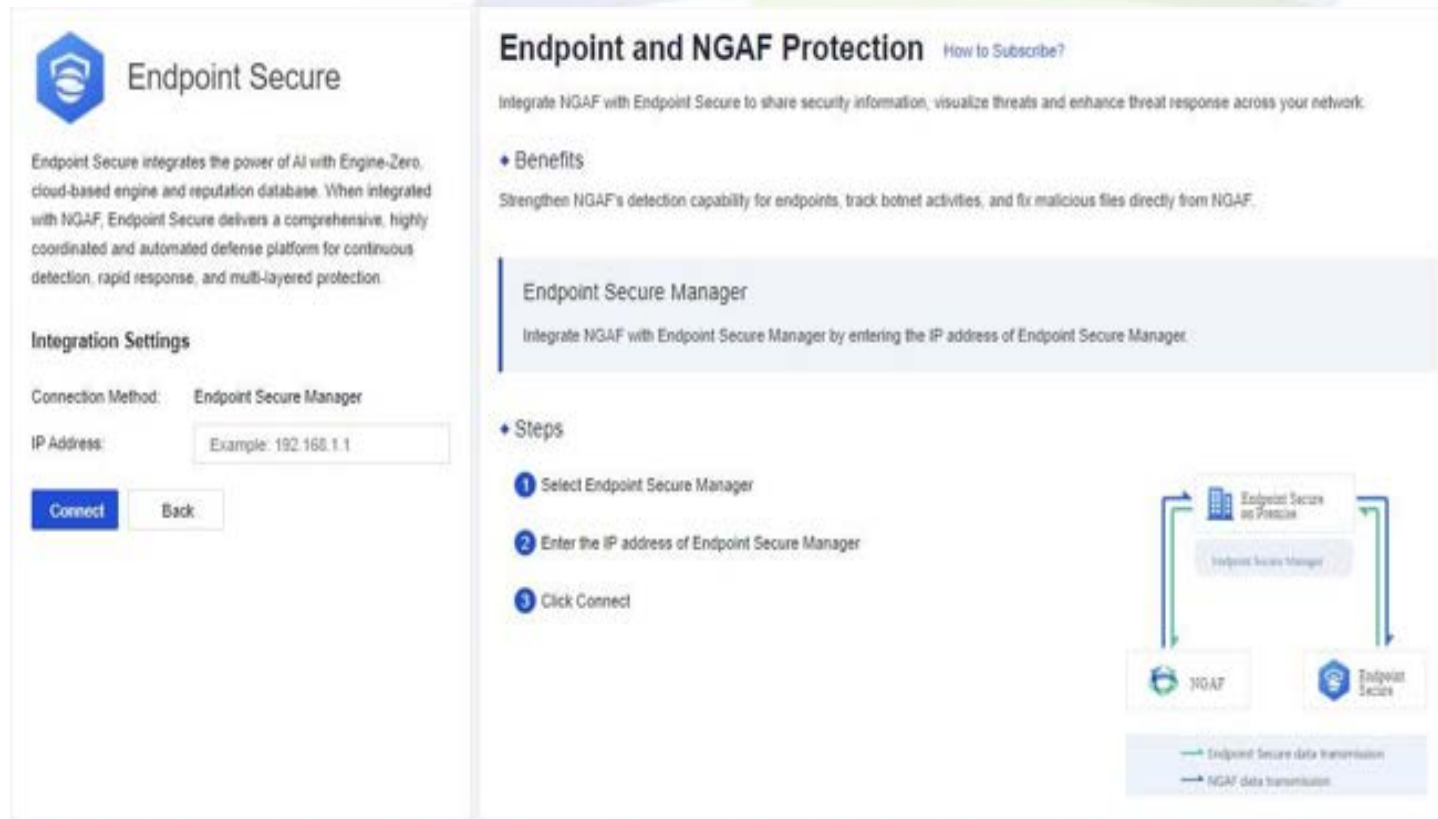
- 1 Select Endpoint Secure and Platform-X
- 2 Connect NGAF to Platform-X
Enter CorpID, NGAF device name, and access token.
- 3 Integrate NGAF with Endpoint Secure subscribed to in Platform-X
Click Connect and Start to connect NGAF to Endpoint Secure Manager.



Endpoint Correlation Options

2.3. Endpoint Secure Manager

Endpoint Secure Manager connection deploys the ES management platform locally. Enter the IP address of Endpoint Secure Manager to establish the connection and implement the cooperation between NGAF and ES.



The screenshot displays the 'Endpoint Secure' integration settings page. On the left, the 'Endpoint Secure' logo is shown above a description of its AI-powered Engine-Zero. Below this, the 'Integration Settings' section shows the 'Connection Method' set to 'Endpoint Secure Manager'. An 'IP Address' field contains the example '192.168.1.1'. 'Connect' and 'Back' buttons are at the bottom of this section. The right side of the page, titled 'Endpoint and NGAF Protection', explains the integration's purpose and lists benefits. It includes a 'Steps' section with three numbered instructions: 1. Select Endpoint Secure Manager, 2. Enter the IP address of Endpoint Secure Manager, and 3. Click Connect. A diagram at the bottom right illustrates the data flow between NGAF, Endpoint Secure Manager, and Endpoint Secure, with green arrows indicating data transmission from Endpoint Secure to NGAF and blue arrows indicating data transmission from NGAF to Endpoint Secure.

3. Application Scenario

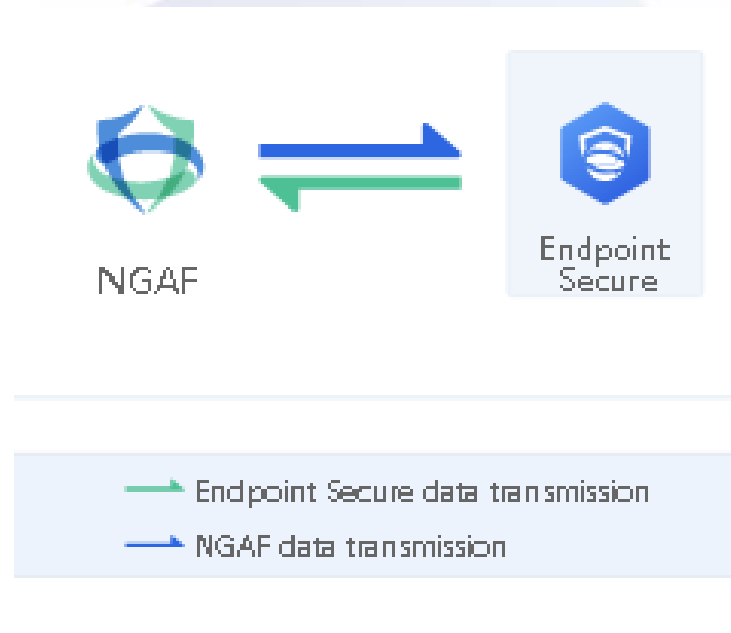


SANGFOR
深信服科技

Application Scenario

3.1. Application Scenario

Starting from the NGAF8.0.26 version, NGAF added an Endpoint Secure on NGAF. This enhancement enhances the way by having an MGR cloud image and combining MGR's management interface into the NGAF management interface. This enhancement allows the administrator to manage both MGR and NGAF at the same time. ES was added into NGAF to correlate.

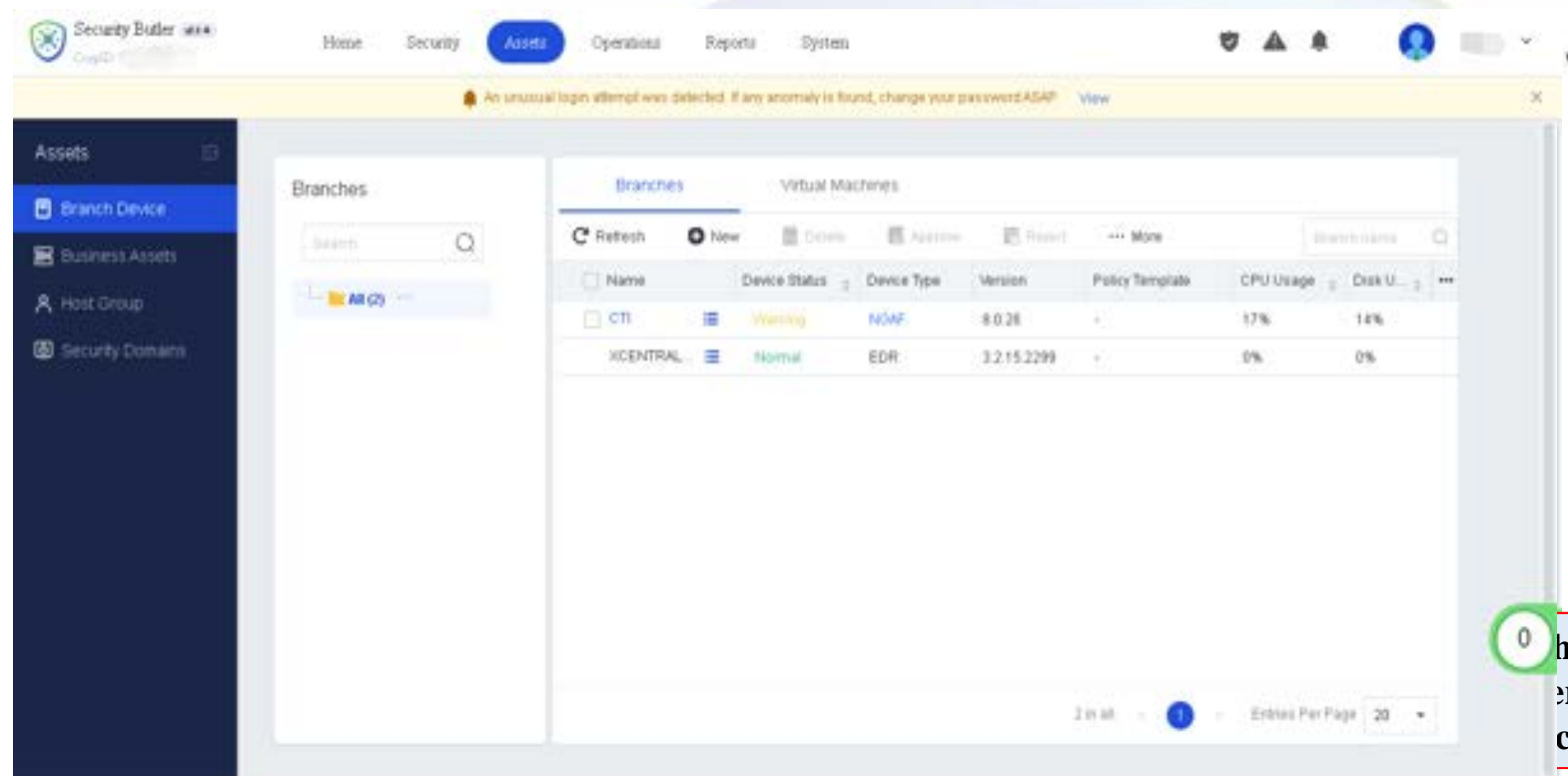


Endpoint Secure and NGAF



4.1. Configuration Guide

4.1.1. Configuring Platform-X



Endpoint Secure and NGAF



4.1. Configuration Guide

4.1.2. Configuring Endpoint Secure and NGAF

Endpoint Secure Licensed

Activated Functionalities

- ✓ Virus Scan
- ✓ Realtime Monitoring
- ✓ Quarantine File
- ✓ Endpoint Isolation
- ✓ Coordinated Response
- ✓ Botnet Detection

Service Details

Connection Method: Endpoint Secure and NGAF Log Out

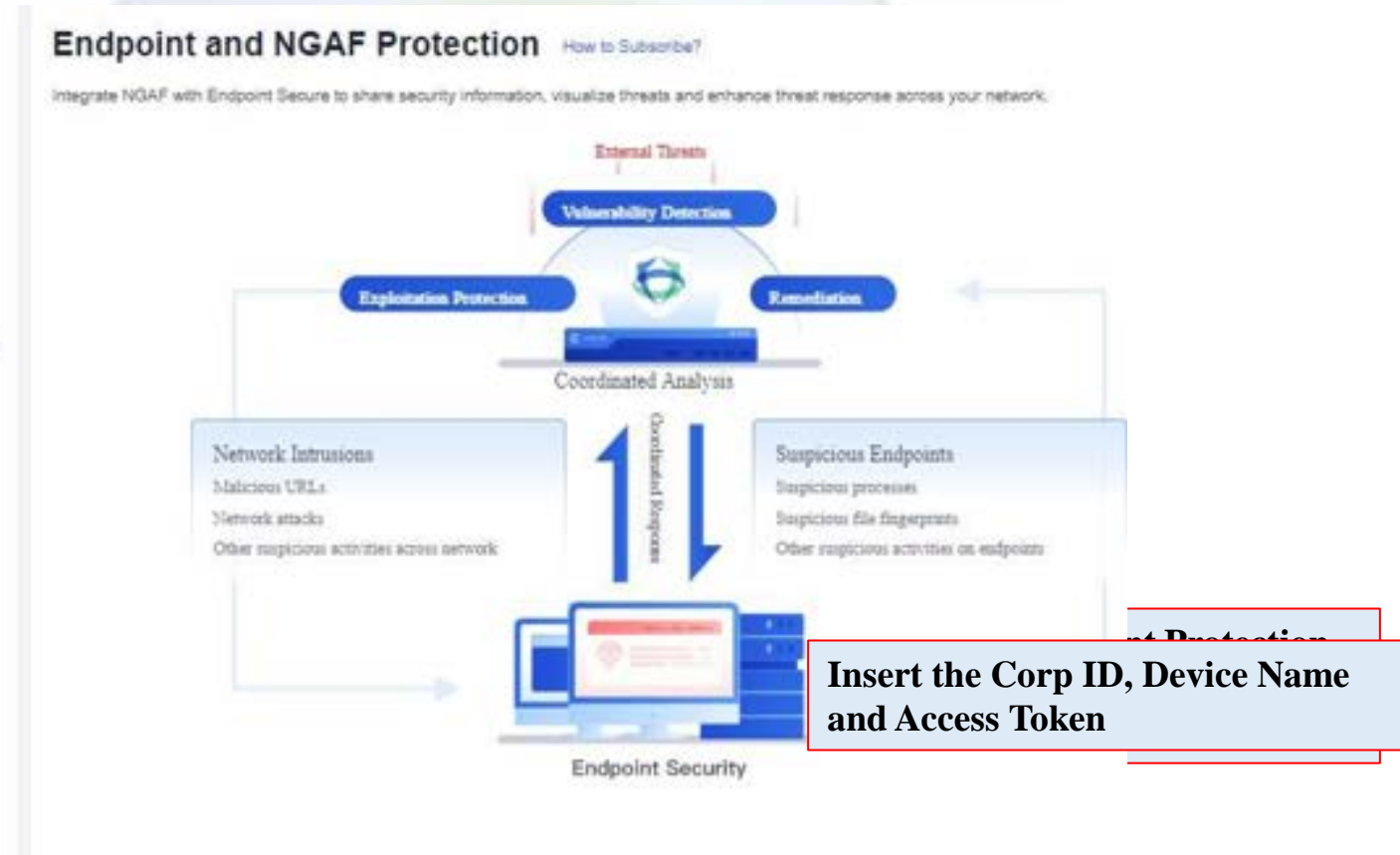
Expiration Date: 2021-06-17 (Remaining: 100 days)

Endpoint License

Device Type	Used	Total
Windows Hosts	1	10
Windows Servers	0	10
Linux Servers	0	10

Quick Links

- [Agent Deployment](#) Download and install Endpoint Secure installer
- [Renew License](#) Update license to renew subscription service



Endpoint Secure and NGAF



4.2. Agent Deployment

Click **Agent Deployment** to open the **Agent Deployment** page, manage ES clients downloading and deployment via different IP addresses associated with different zones by selecting zones and connected IP addresses respectively.

Agent Deployment



Note:

Download the installer and do not change its name because the IP address of Endpoint Secure Manager 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

Select

Connected IP address

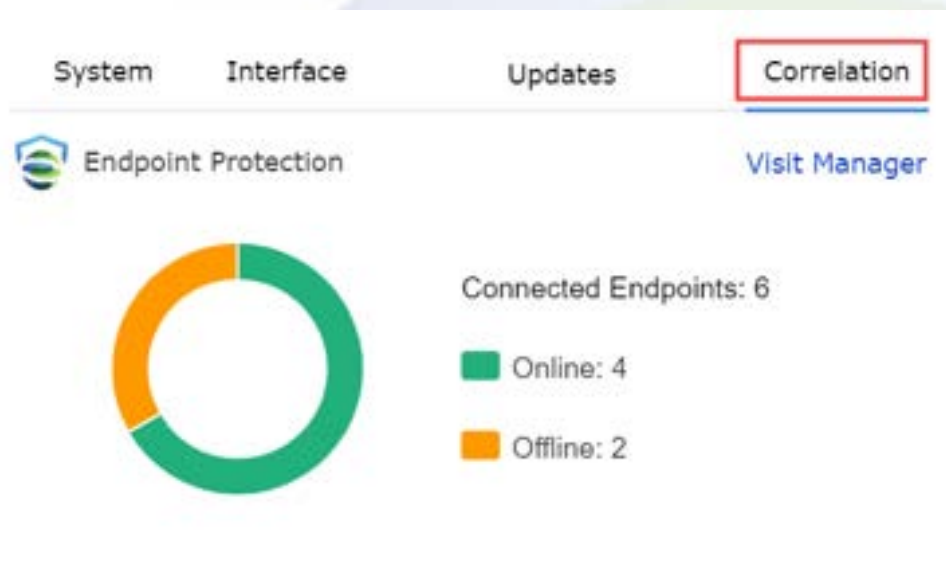
Add

No.	Zone	Interfaces	Connected IP Address	Installer (Windows OS)	Installer (Linux OS)	Download Link	Operation
1	LAN	eth2	172.16.10.1/24	32%	Download	Copy	

Endpoint Secure and NGAF

4.3. Confirm Correlation Status

Go to **Status > Dashboard** confirm correlation status, you can see the connected endpoints of endpoint, as shown below.

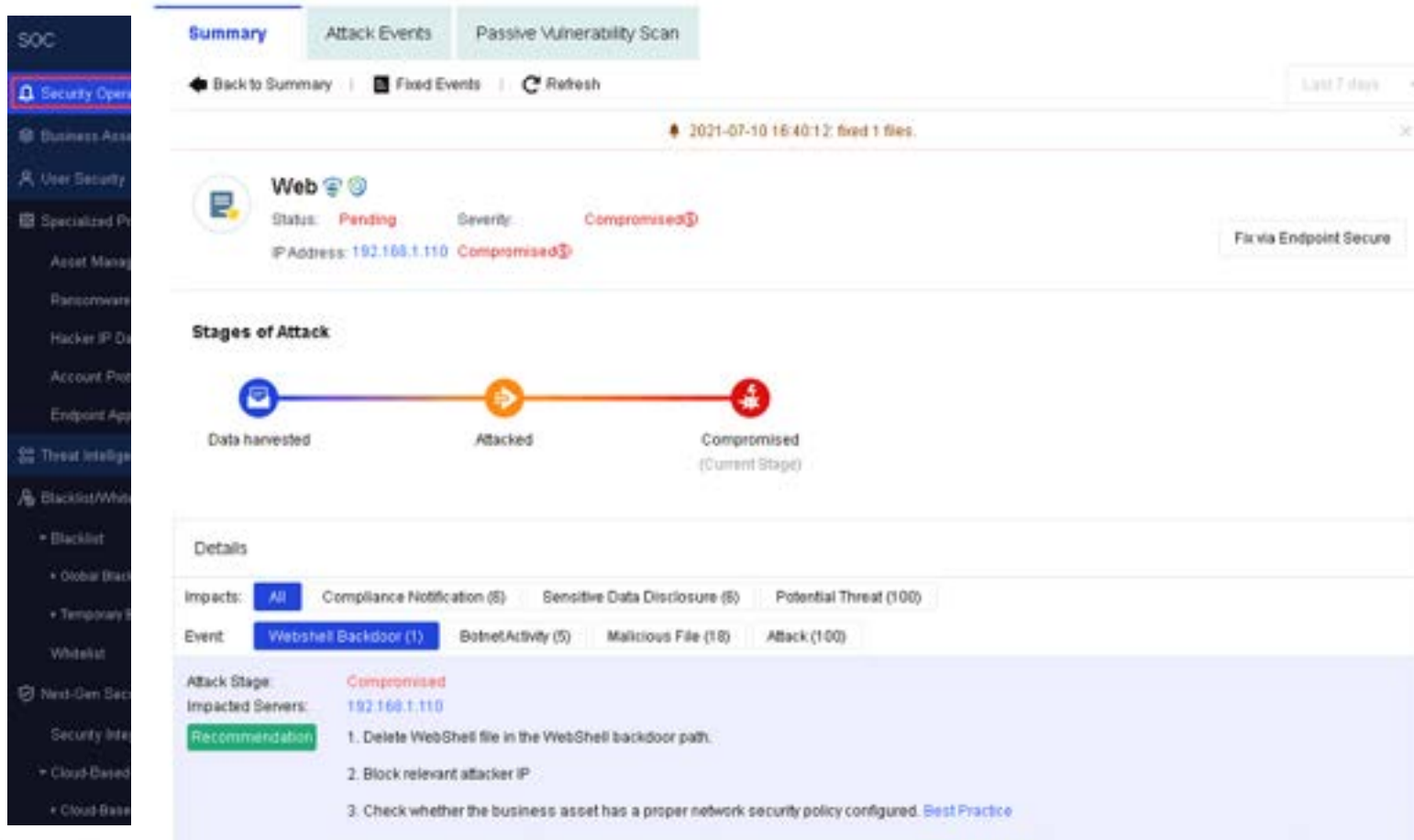


Endpoint Secure and NGAF



4.4. Security Operations

In the analysis of high threats, in addition to the protocol resolution of NGAF itself, the Neural-X is further linked to further analyze the behavior of the host.



Endpoint Secure and NGAF



4.5. Security Operations

If a malicious file is detected, the corresponding file can be quarantined by viewing the details. NGAF only issues the quarantine task to the Endpoint Secure Server. Then the Endpoint software quarantine the corresponding files in computer.

Files (Web) [X]

[Fix] [Trust] ☐ Show malicious domain-related file Status: [Malicious] URL, file name [Search]

<input checked="" type="checkbox"/>	No.	Malicious File	Threat	Related Malicious Domain	Time	Action	Operation
1 entries selected on current page, Select all entries							
<input checked="" type="checkbox"/>	1	whiterose	Virus: Ransom.Win32.WhiteRos... Malicious Ransomw...	No outbound access	2021-07-09 15:07:48	Pending	View More
<input type="checkbox"/>	2	whiterose	Virus: Ransom.Win32.WhiteRos... Malicious Ransomw...	No outbound access	2021-01-25 10:50:39	Fixed	View Restore

Total: 2 | 1 | Entries Per Page: 50 | Go To Page: 1

[Close](#)

Endpoint Secure and NGAF



4.6. Business System Security

Botnet activity tracking can be achieved through correlation. The botnet activity tracking can locate specific malicious process names and storage paths.

The screenshot displays the 'Botnet Activity Forensics' section of the Sangfor Endpoint Security interface. It shows a process (pythonw.exe) being analyzed, with a traceback diagram illustrating the flow from the Endpoint (192.168.1.110) to the Parent Process (C:\Users\janzhowapp\pythonw.exe) and then to the Child Process (C:\Users\janzhowapp\pythonw.exe). The Child Process is shown calling two files: 'vounfma1...' and 'comc832.dll', both marked as 'Suspicious' and 'Malicious U...'. The interface also lists 'TOP 1' suspicious files: switchnets.net, suppbobx, and View Sangfor Security Wiki. 'TOP 2' includes jazirahonline.com, emotet, and View Sangfor Security Wiki. 'TOP 3' includes diabetesdietjournal.com, emotet, and View Sangfor Security Wiki. The 'Basic Settings' section shows file details for a Python file, including File Path, File Type, File Size, Created At, File MD5, Description, and Issued By. The 'Action' section shows the file status as 'Pending' and a recommendation to monitor it. The 'Recommendation and status' section shows a table with 'Monitor' and 'Details' links for each suspicious file.

Recommendation	Status
Monitor	Details
Monitor	Details
Monitor	Details
Monitor	Details
Monitor	Details
Monitor	Details
Monitor	Details
Monitor	Details

Endpoint Secure and NGAF



4.7. User Security

Analysis of suspicious files through correlation. There are three types of analysis results: “malicious”, “suspicious” and “Security Issue”.

The screenshot displays the Sangfor SOC interface, specifically the 'User Security' section. The left sidebar shows the navigation menu with 'User Security' highlighted. The main content area shows a summary of attack events for the user 'janhw1' (IP: 192.168.1.110). The interface includes a 'Summary' tab, a 'Refresh' button, and a 'Last 7 days' filter. A table lists the attack events, with one entry for 'janhw1' (192.168.1.110) showing a 'Pending' status, 'Compromised (High)' severity, and 'C&C Communication' attack type. The table also shows 788 detections, 0 malicious files, and 0 integration events. The 'Action' column for this entry has a 'Preview' button. Below the table, there is a section for 'User: janhw1 (192.168.1.110)' with a 'Summary' of security threats. At the bottom, there are five summary cards: '3 Advanced Threats (Top 3 Access Ma)', '333 Nighttime Outbound Connections (N)', '788 Attacks', 'No malicious outbound connections', and '0/18 Quarantined/Total Malicious File'.

No.	User	Status	Severity	Attack Type	Attack Stage	Detectio...	Malicious Files	Integration	Operation
1	janhw1 (192.168.1.110)	Pending	Compromised (High), Very High	Unknown DNS malware, IPDomain-C&C C...	C&C Communica...	788	0		Action - Preview

Total: 1 / 1 Entries Per Page: 50

User: janhw1 (192.168.1.110)

Summary

This host has encountered various security threats, malicious outbound connections to different destination regions, frequent advanced threats, frequent attacks at nighttime, and its threat level and confidence are relatively high. 2 malicious files and 0 pending files detected after Neural-X Threat Intelligence analysis of forensics from Endpoint Secure. Please fix the issues as soon as possible.

3 Advanced Threats (Top 3 Access Ma)

333 Nighttime Outbound Connections (N)

788 Attacks

No malicious outbound connections

0/18 Quarantined/Total Malicious File

Endpoint Secure Correlation



4.8. User Security

User Security can display Fixed Event and set trust for quarantined files.

The screenshot displays the SANGFOR User Security interface. On the left is a dark sidebar with navigation options: SOC, Security Operations, Business Asset Security, **User Security** (highlighted), Specialized Protection, Asset Management, Ransomware Protection, Hacker IP Database, Account Protection, Endpoint App Control, Threat Intelligence, Blacklist/Whitelist, and Next-Gen Security. The main panel shows a 'Summary' tab with a status bar indicating '2021-07-10 22:47:22: 16 suspicious files and 5 secure files found. Keep monitoring.' Below this, a card for IP 192.168.1.110 shows a 'Compromised (High, Very High)' status and 'Pending' action. A table lists detected malicious files with columns for Malicious File, Threat, Related Malicious Domain, Time, Action, and Operation. The 'Operation' column includes a 'Trust' button for the second file.

Malicious File	Threat	Related Malicious Domain	Time	Action	Operation
2594d4a1f00f1d20e2b24...	Virus: Trojan.PDF.GenericKD.3 Quarantine Trojan	No outbound access	2021-05-04 13:20:16	Pending	View More
6b04dead940bc5f93d064...	Virus: Trojan.Win32.XPACK.ulg Quarantine Trojan	No outbound access	2021-05-04 13:20:16	Pending	View Trust
ab7c3c7ead54cd05eaf57...	Virus: Trojan.Win32.XPACK.ulg Quarantine Trojan	No outbound access	2021-05-04 13:20:16	Pending	View More
1d7d87aef17d71b30bc24...	Virus: Trojan.Win32.XPACK.ulg Quarantine Trojan	No outbound access	2021-05-04 13:20:16	Pending	View More
05542ce682af0e3d15446...	Virus: Trojan.Win32.XPACK.ulg Quarantine Trojan	No outbound access	2021-05-04 13:20:16	Pending	View More
db28b58e222ba11e1391E...	Virus: Trojan.Win32.XPACK.ulg Quarantine Trojan	No outbound access	2021-05-04 13:20:16	Pending	View More

Thank you !

tech.support@sangfor.com
community.sangfor.com

Sangfor Technologies (Headquarters)

Block A1, Nanshan iPark, No.1001
Xueyuan Road, Nanshan District,
Shenzhen, Guangdong Province,
P. R. China (518055)

