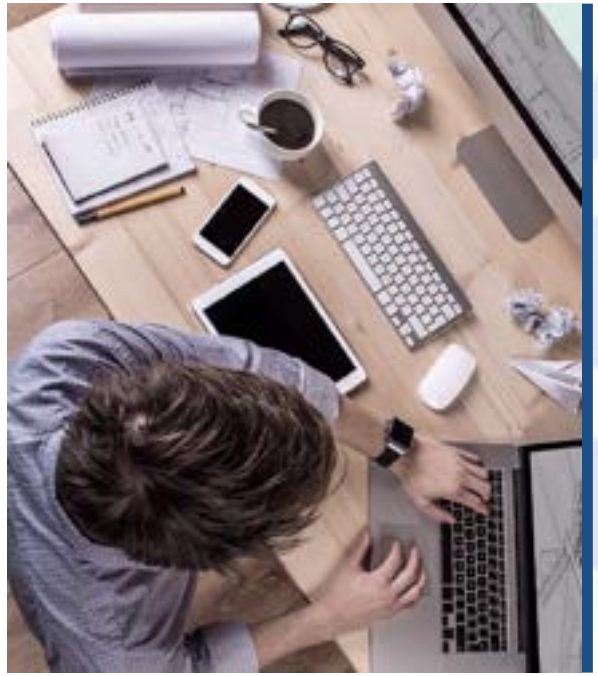
SANGFOR

SANGFOR NGAF V8.0.47 Professional

Endpoint Protection



1 Endpoint Secure Correlation

2 Endpoint Correlation Options

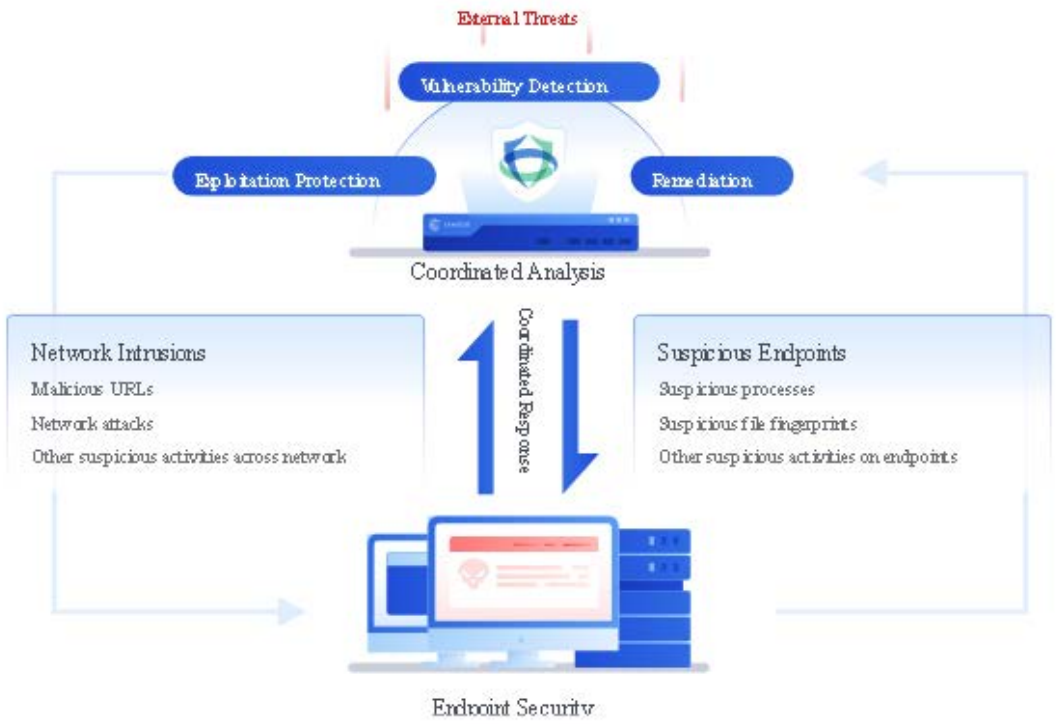
3 Application Scenario

1. Introduction

SANGFOR
深信服科技

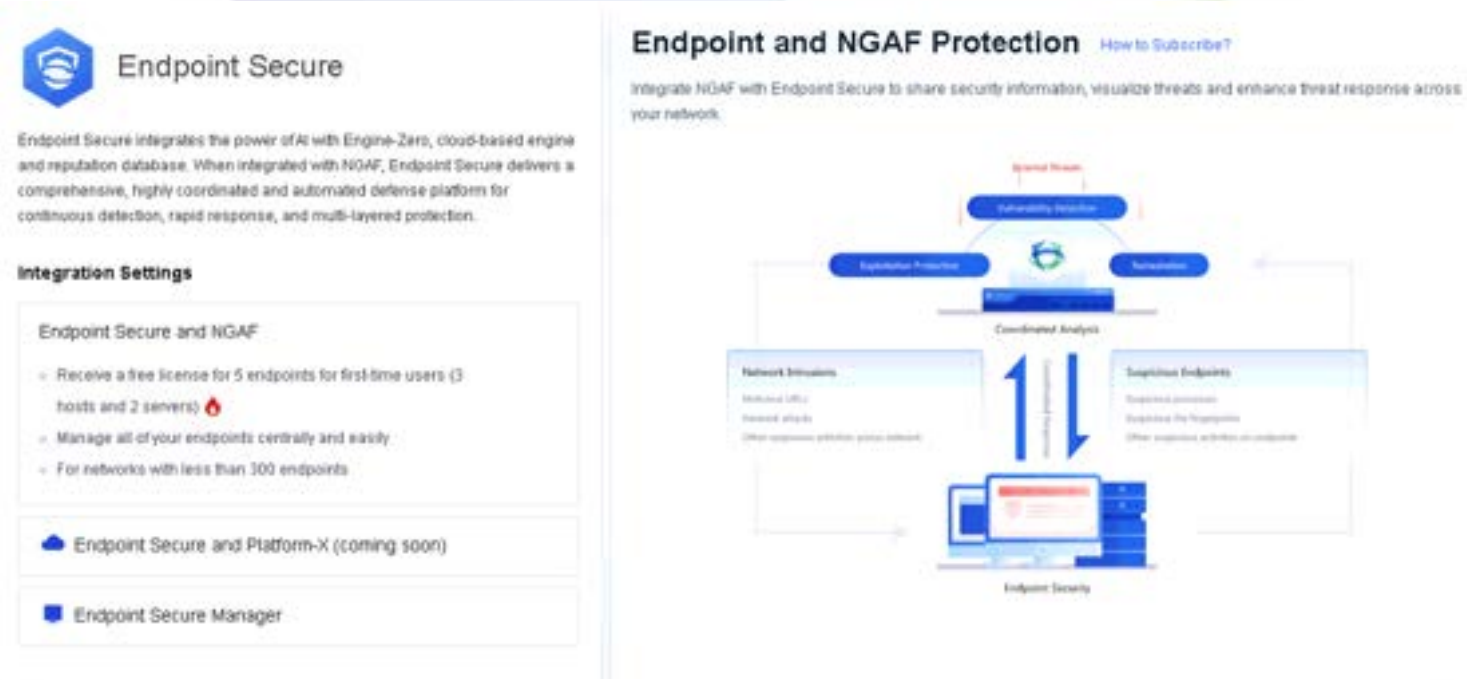
Introduction

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.



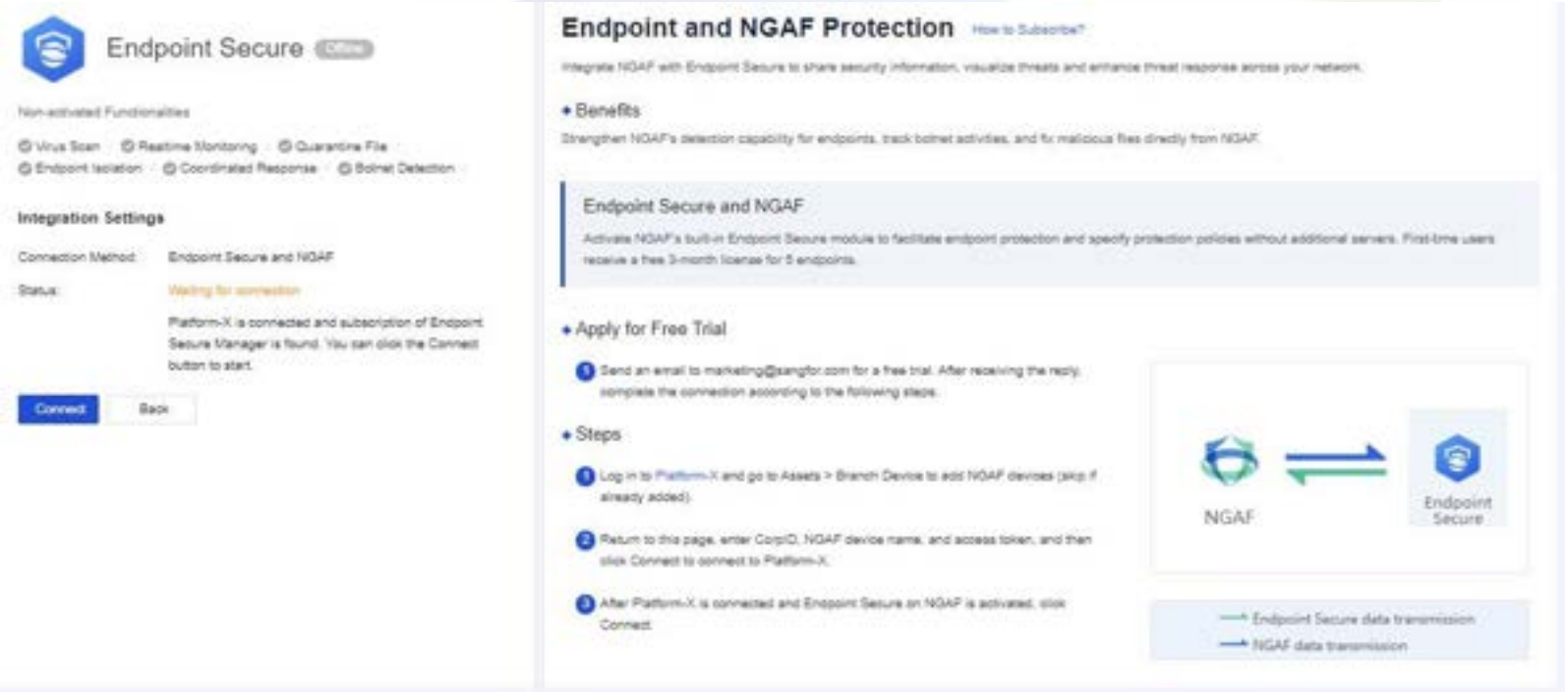
2. Endpoint Correlation Options

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.



Endpoint Correlation Options

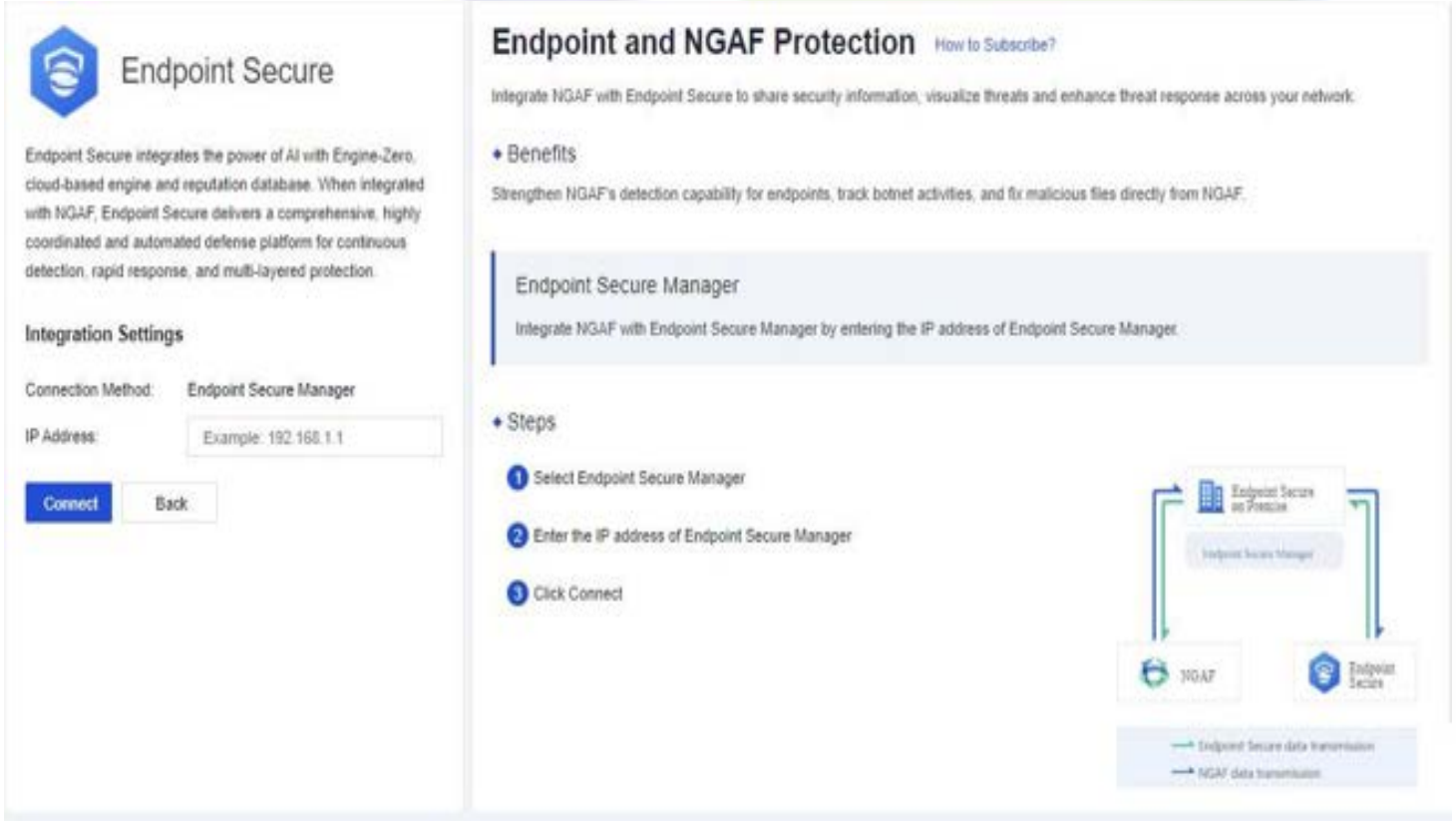
2.2. Endpoint Secure and Platform-X

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 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.



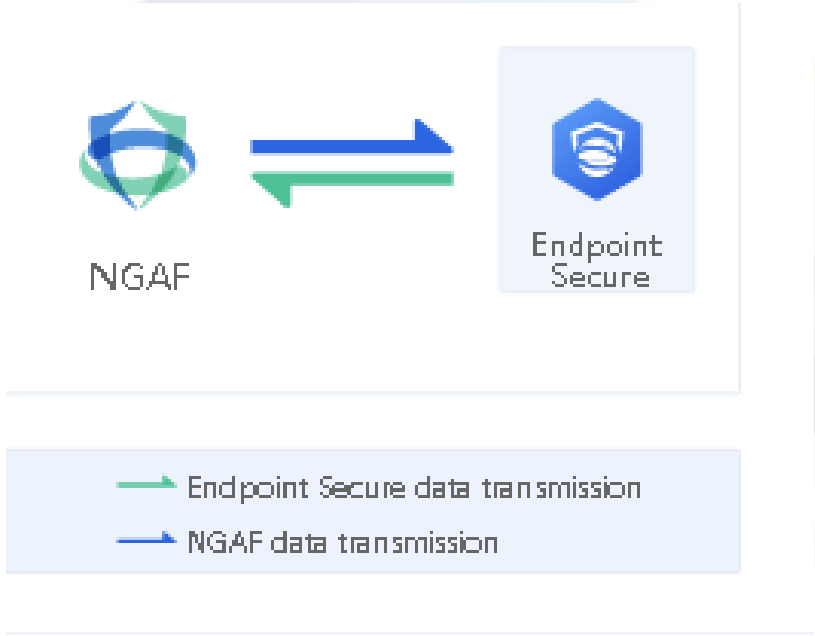
3. Application Scenario

SANGFOR
深信服科技

Application Scenario

3.1. Application Scenario

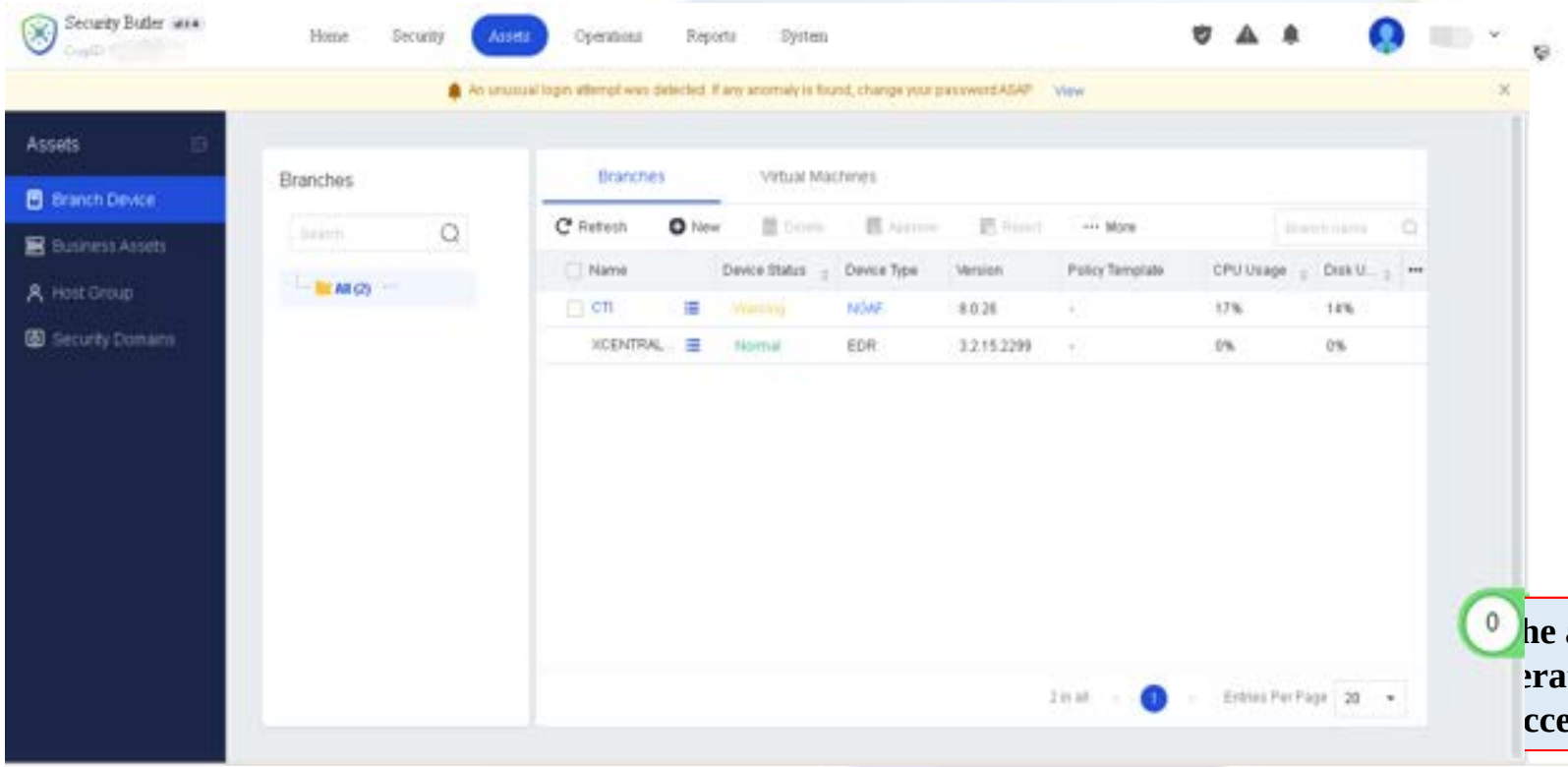
Starting from the NGAF8.0.26 version, NGAF added an Endpoint Secure on NGAF. This enhancement enhances the way by having an MGR cloud image and combining MGR's management interface into the NGAF management interface. This enhancement allows the administrator to manage both MGR and NGAF at the same time.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



Endpoint Secure and NGAF

4.1. Configuration Guide

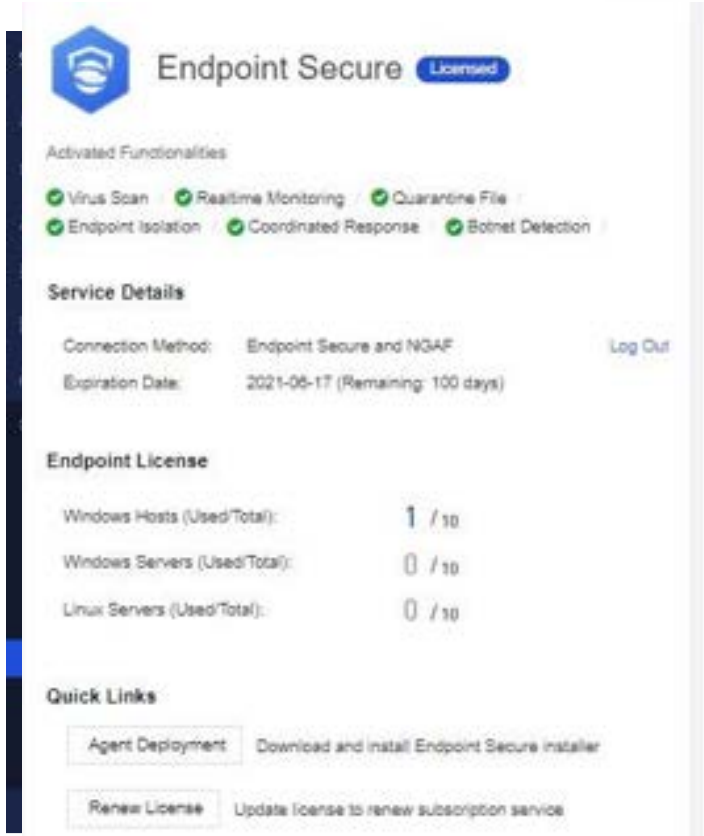
4.1.1. Configuring Platform-X

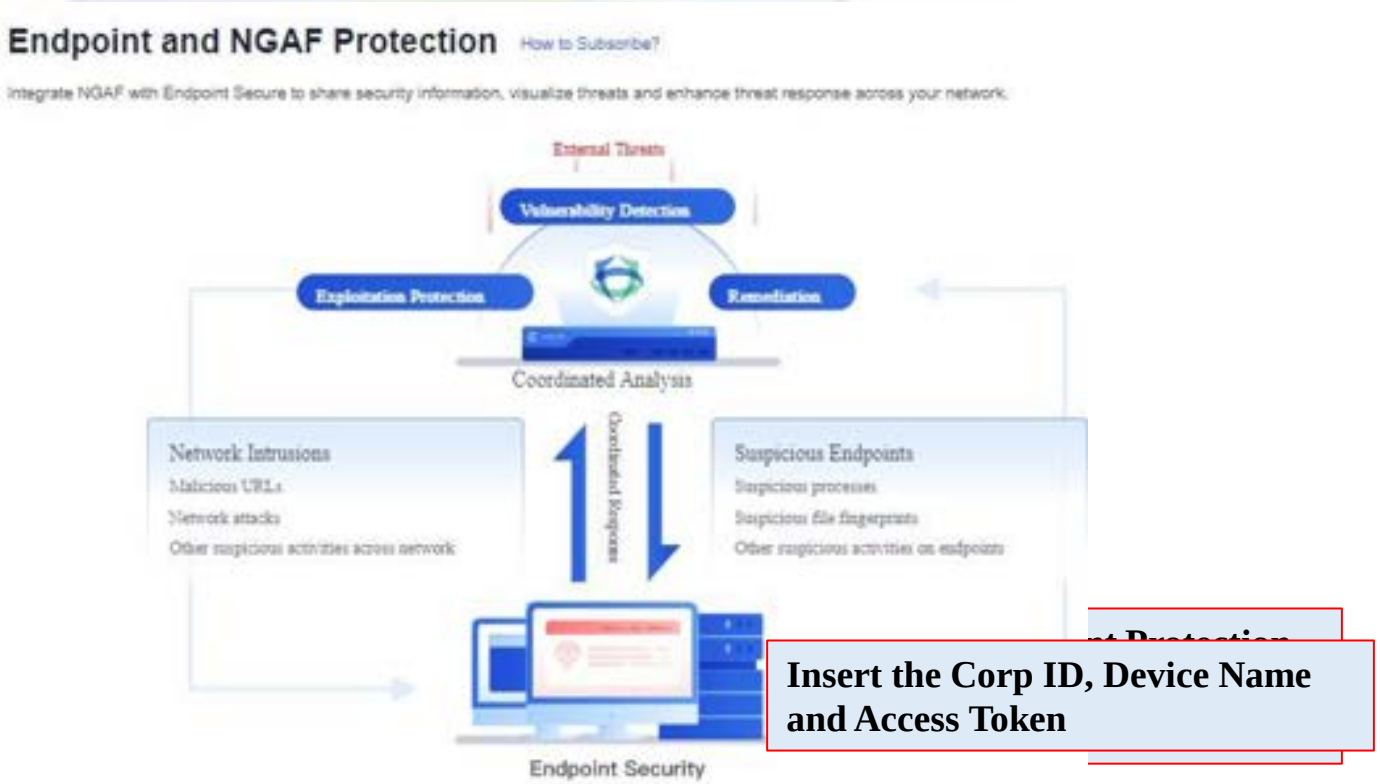


Endpoint Secure and NGAF

4.1. Configuration Guide

4.1.2. Configuring Endpoint Secure and NGAF



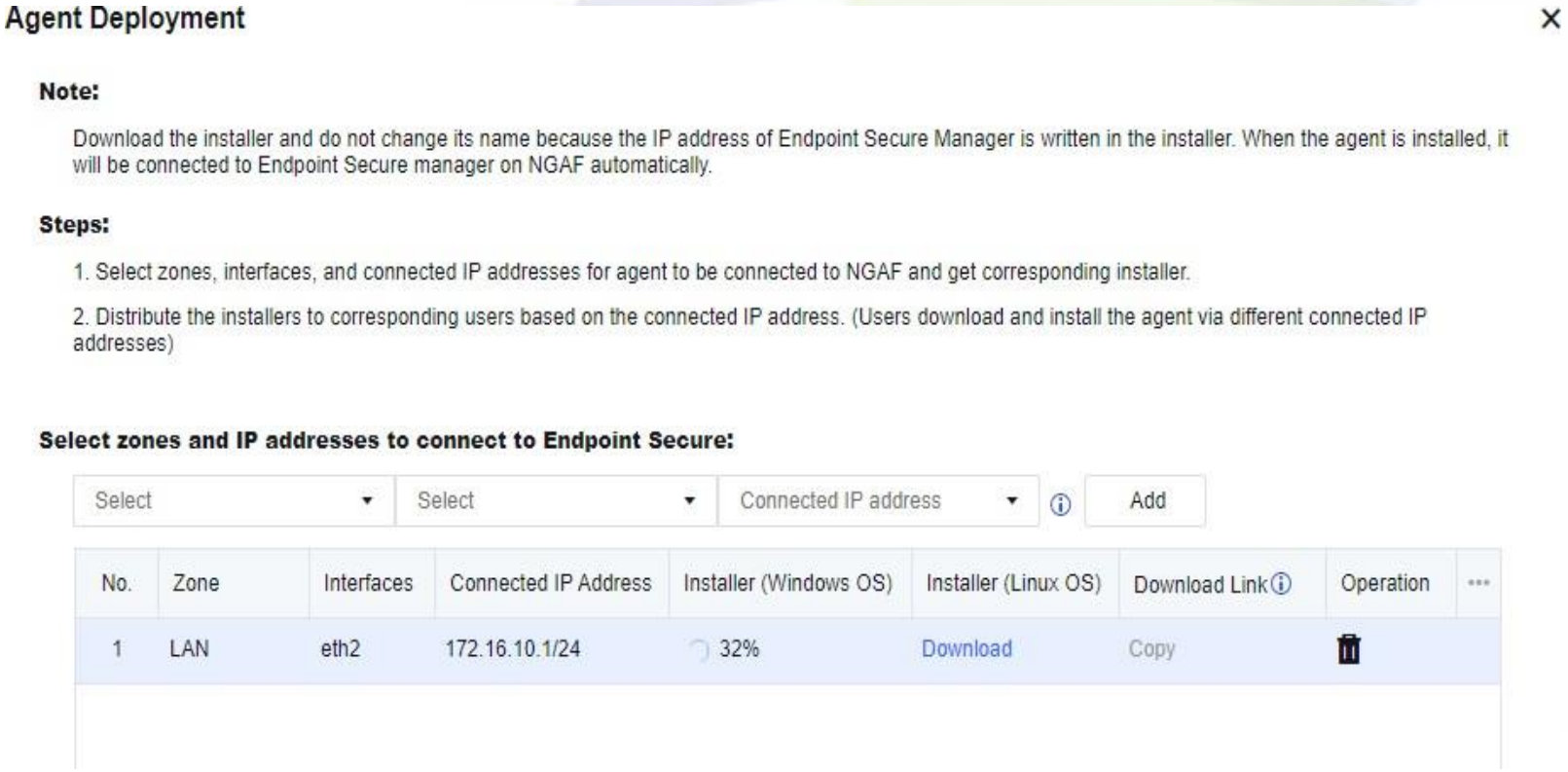


Insert the Corp ID, Device Name and Access Token

Endpoint Secure and NGAF

4.2. Agent Deployment

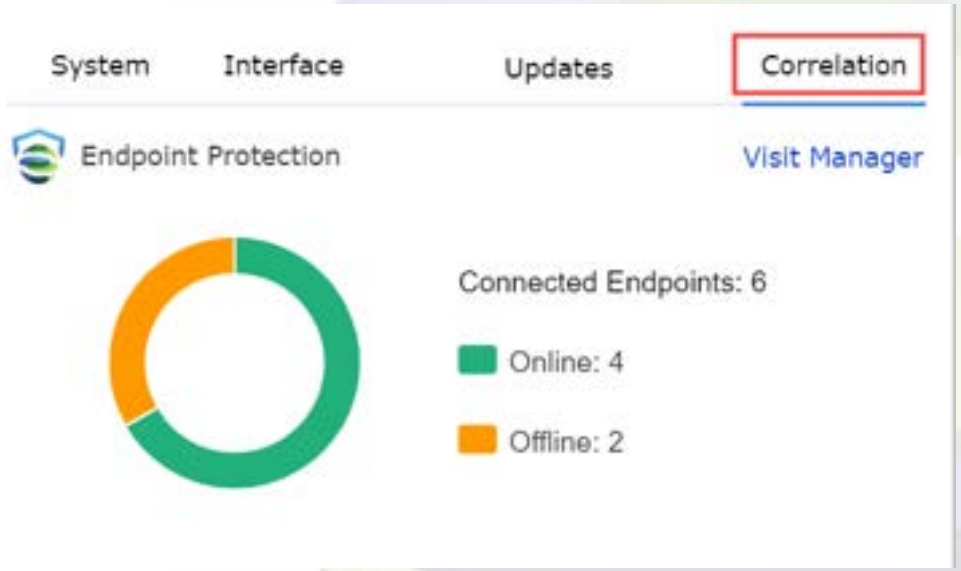
Click **Agent Deployment** to open the **Agent Deployment** page, manage ES clients downloading and deployment via different IP addresses associated with different zones by selecting zones and connected IP addresses respectively.



Endpoint Secure and NGAF

4.3. Confirm Correlation Status

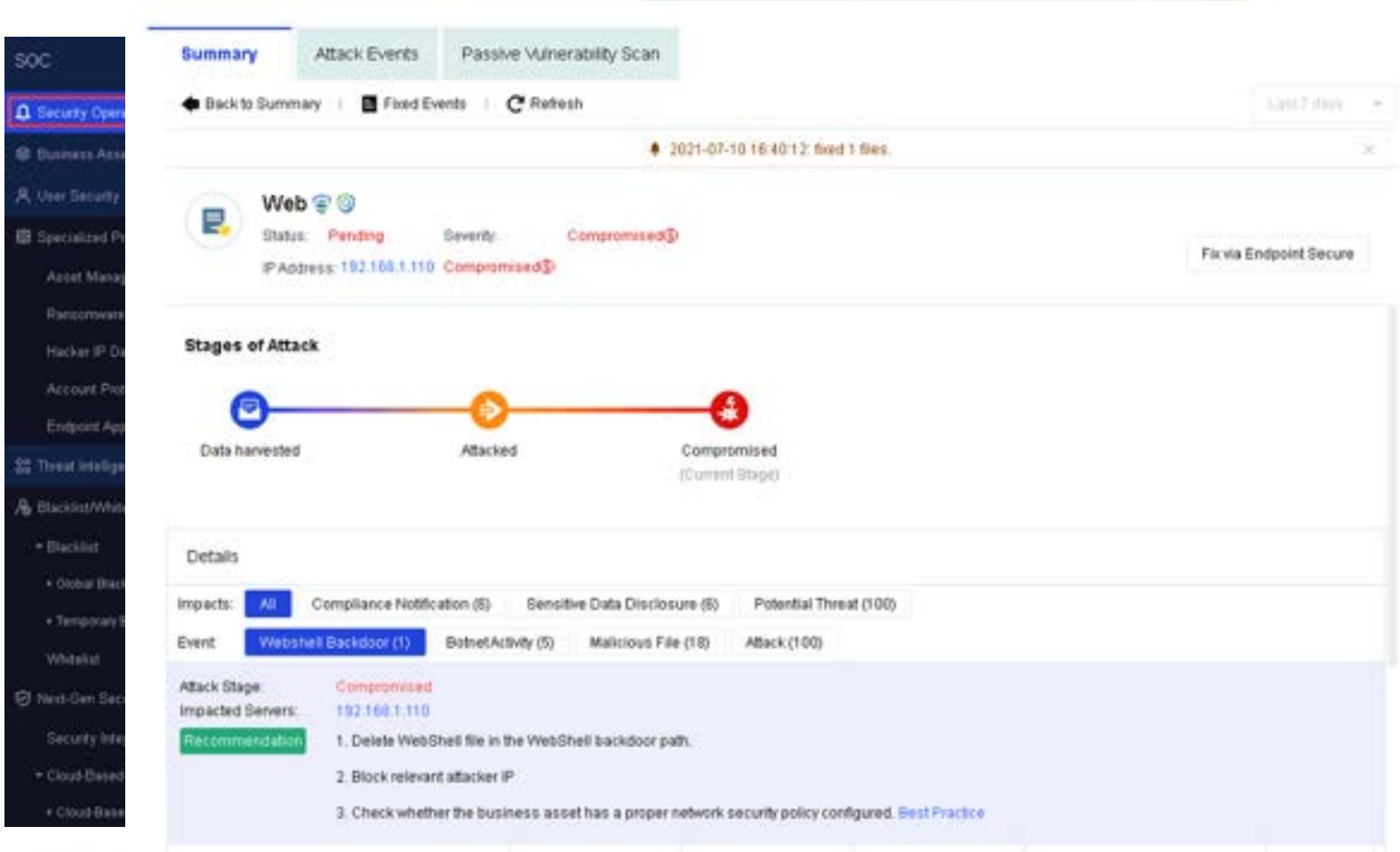
Go to **Status > Dashboard** confirm correlation status, you can see the connected endpoints of endpoint, as shown below.



Endpoint Secure and NGAF

4.4. Security Operations

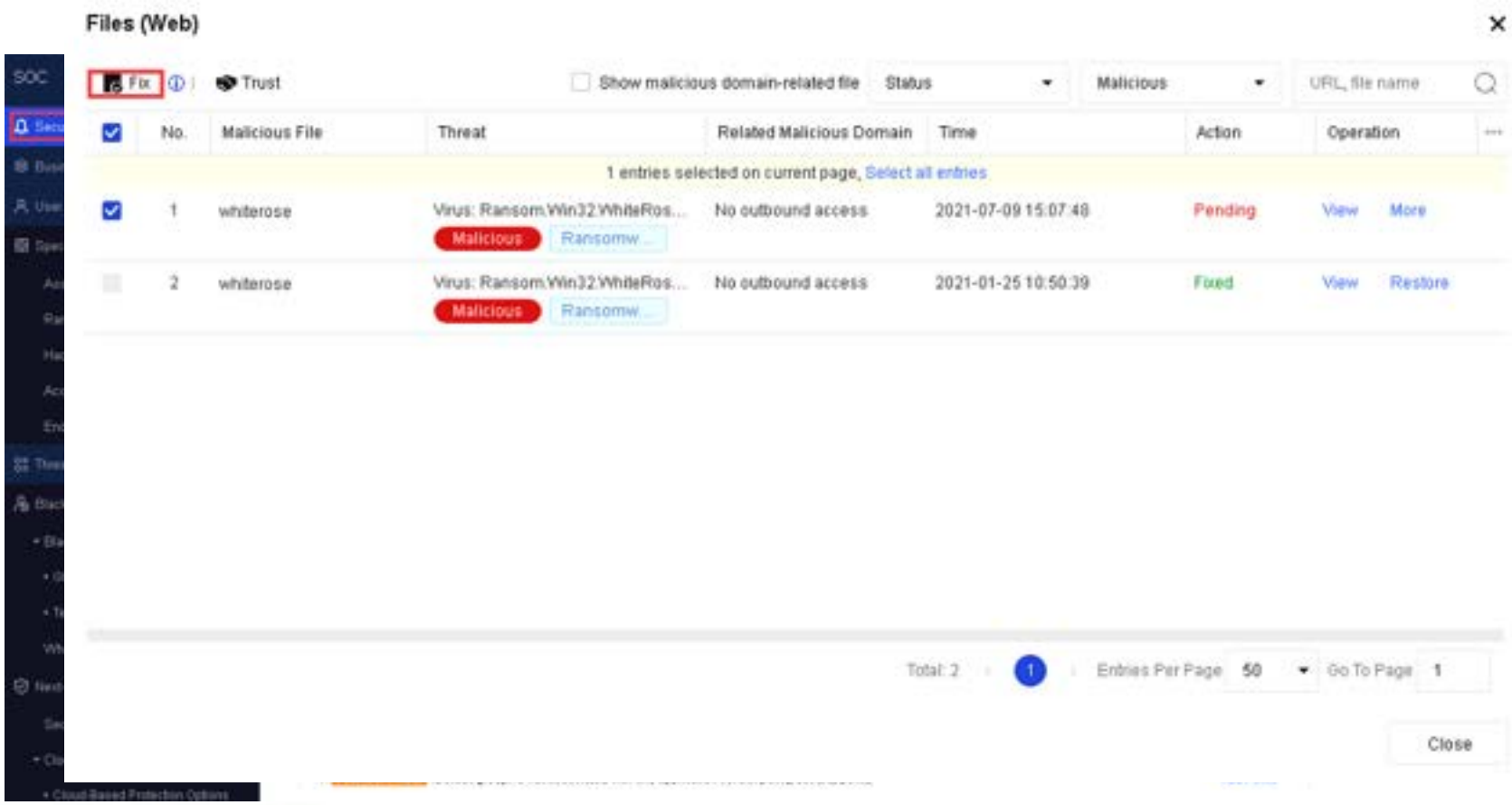
In the analysis of high threats, in addition to the protocol resolution of NGAF itself, the Neural-X is further linked to further analyze the behavior of the host.



Endpoint Secure and NGAF

4.5. Security Operations

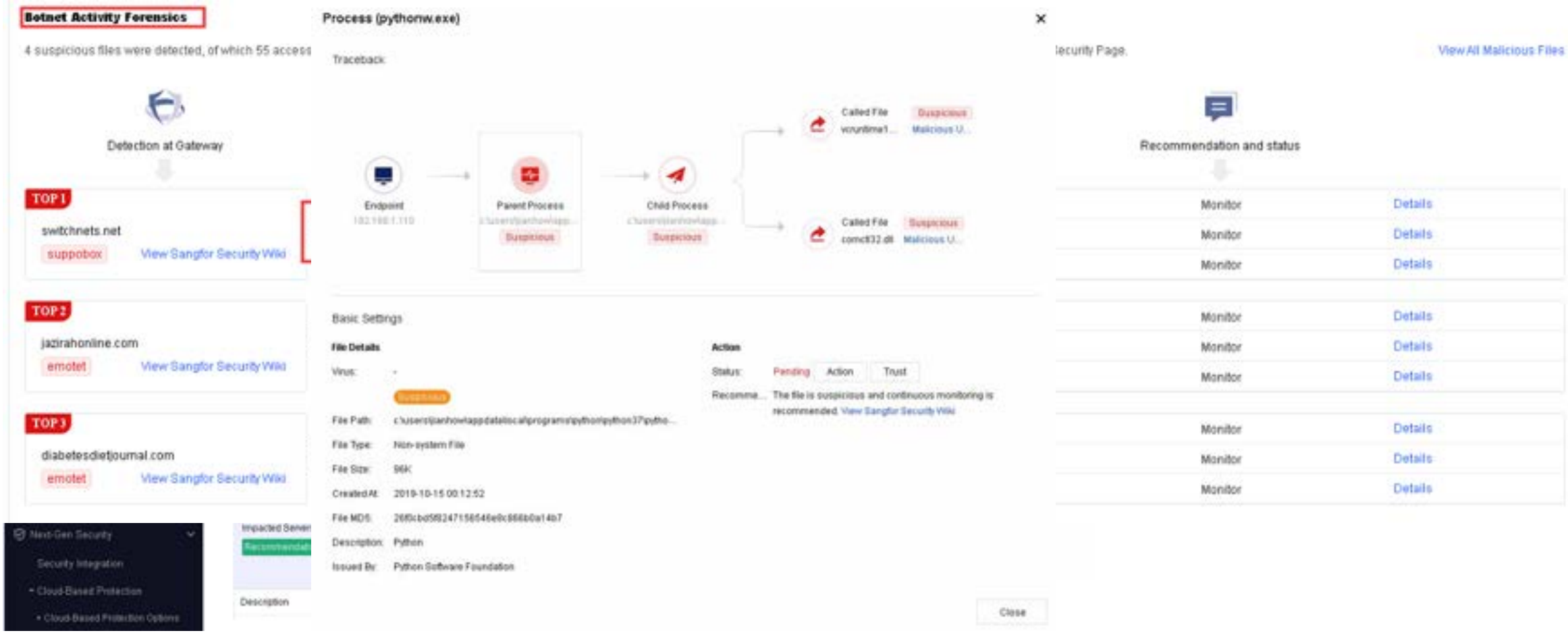
If a malicious file is detected, the corresponding file can be quarantined by viewing the details. NGAF only issues the quarantine task to the Endpoint Secure Server. Then the Endpoint software quarantine the corresponding files in computer.



Endpoint Secure and NGAF

4.6. Business System Security

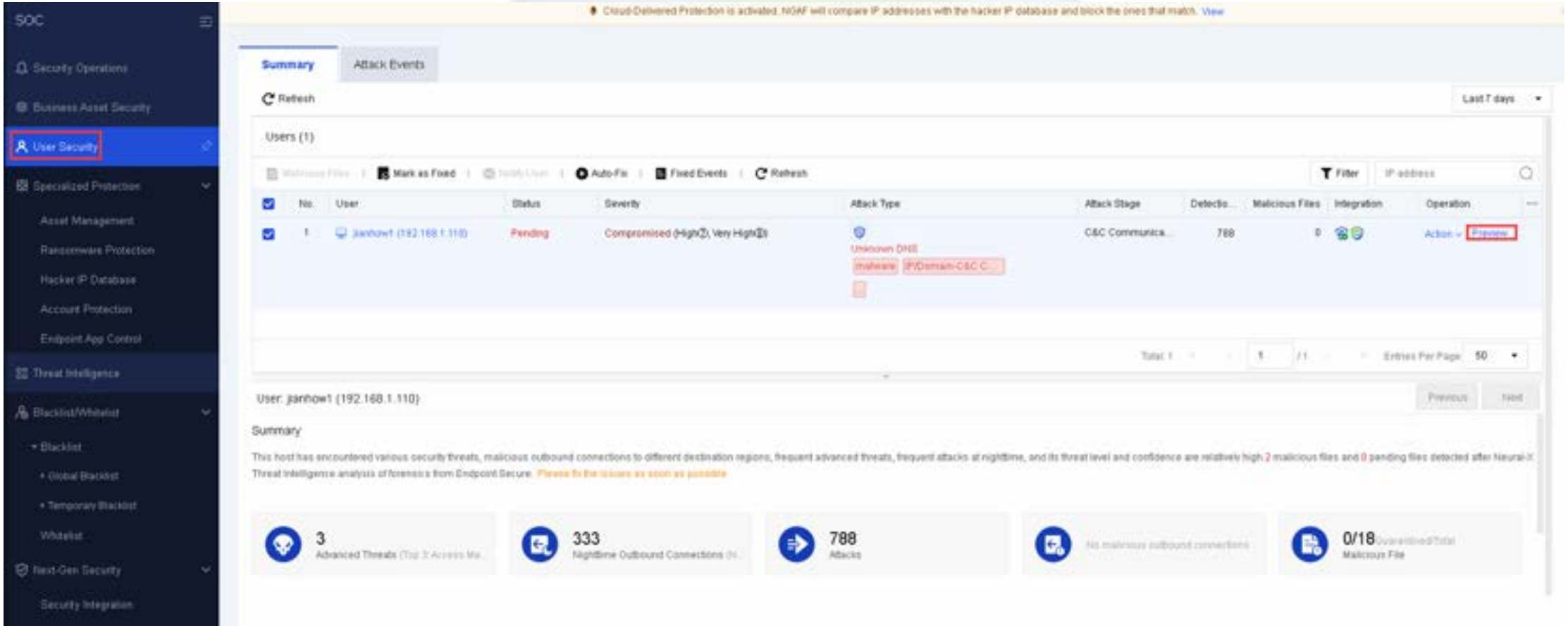
Botnet activity tracking can be achieved through correlation. The botnet activity tracking can locate specific malicious process names and storage paths.



Endpoint Secure and NGAF

4.7. User Security

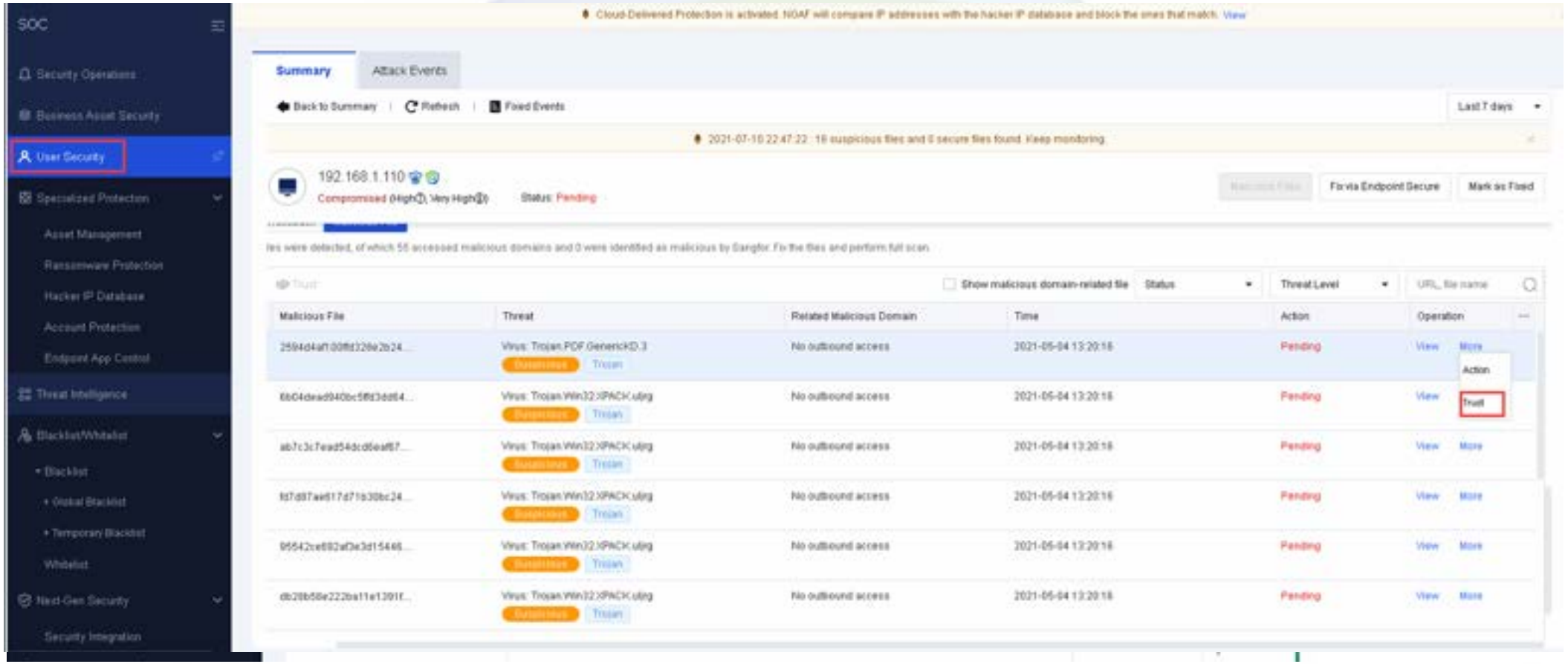
Analysis of suspicious files through correlation. There are three types of analysis results: “malicious” , “suspicious” and “Security Issue”.



Endpoint Secure Correlation

4.8. User Security

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



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)