SANGFOR

Endpoint Secure

Best Practices for Scenarios_Correlate with IAM to Prevent Network Threat

Version 3.2.22

Change Log

Date	Change Description
Feb 25, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario

1.1 Scenario

Current problems faced by customers

The Internet has become an indispensable production tool for employees. However, due to the complexity of the network environment and the threat of various viruses, there are endless levels of Internet management and terminal security issues.

Network side:

1. High-bandwidth applications such as video take up a lot of bandwidth resources, employees are slow to surf the Internet, and internal complaints increased.

2. When employees go to work, they use Internet to surf entertainment website, which seriously affects work efficiency.

3. There are many outgoing file applications and channels such as mail, web disk and QQ WeChat, and the risk of important data leakage is getting higher and higher, and there is a lack of traceability methods;

Endpoint side:

1. The Endpoint assets are not clearly sorted out, the terminal assets that need to be protected cannot be clarified, and the terminal responsible person cannot be clarified.

2. Endpoint are often plagued by viruses, and their internal unrestricted and rapid spreading poses a major threat to Local Area network.

3. The employees have weak security awareness, and the risk of operating system vulnerabilities is significant, which can easily cause threats to invade;

IAM and Endpoint Secure products are deeply integrated to help customers build a green, safe, efficient and easy-to-use Internet environment;

User access authentication to ensure the security of access identity

To achieved wired and wireless network access authentication, IAM supports multiple access authentication methods such as 802.1x, bypass non-sensing, and wireless Portal;

Support 29 authentication methods such as AD domain, SMS, WeChat, etc., which can be flexibly selected according to the Internet scenario;

Accurate Internet control and flow control to ensure Internet experience and work efficiency

IAM has a leading application identification feature library and URL library, supports application segmentation function management and control, blocks irrelevant applications, and allows employees to surf the Internet more efficiently.

IAM has accumulated professional traffic management technology for ten years to ensure the Internet experience of normal applications, limit the traffic of entertainment applications such as audio and video downloads, and increase bandwidth utilization by more than 30%.

Full outgoing audit, discovering the risk of leakage

Sangfor IAM has professional content identification and auditing technology in the industry, and can effectively audit various online behaviors and various outgoing data, including outgoing content audits such as web pages, mailboxes, online disks, WeChat, and QQ.

Through various outsourced audits and analysis, we found out the abnormal behavior of leaks, early warning the risks of leaks and quickly locating leaks.

Endpoint security access to ensure the security of access terminals

The Endpoint security software is installed uniformly, and the terminal Endpoint Secure software can be forcibly installed after IAM certification;

Endpoint security access inspection, including system vulnerability scanning, anti-virus installation, open interfaces, etc., only allow endpoints that meet the security requirements to access the network;

Regular endpoint vulnerability scanning, after vulnerability scanning, it can be automatically repaired and reported;

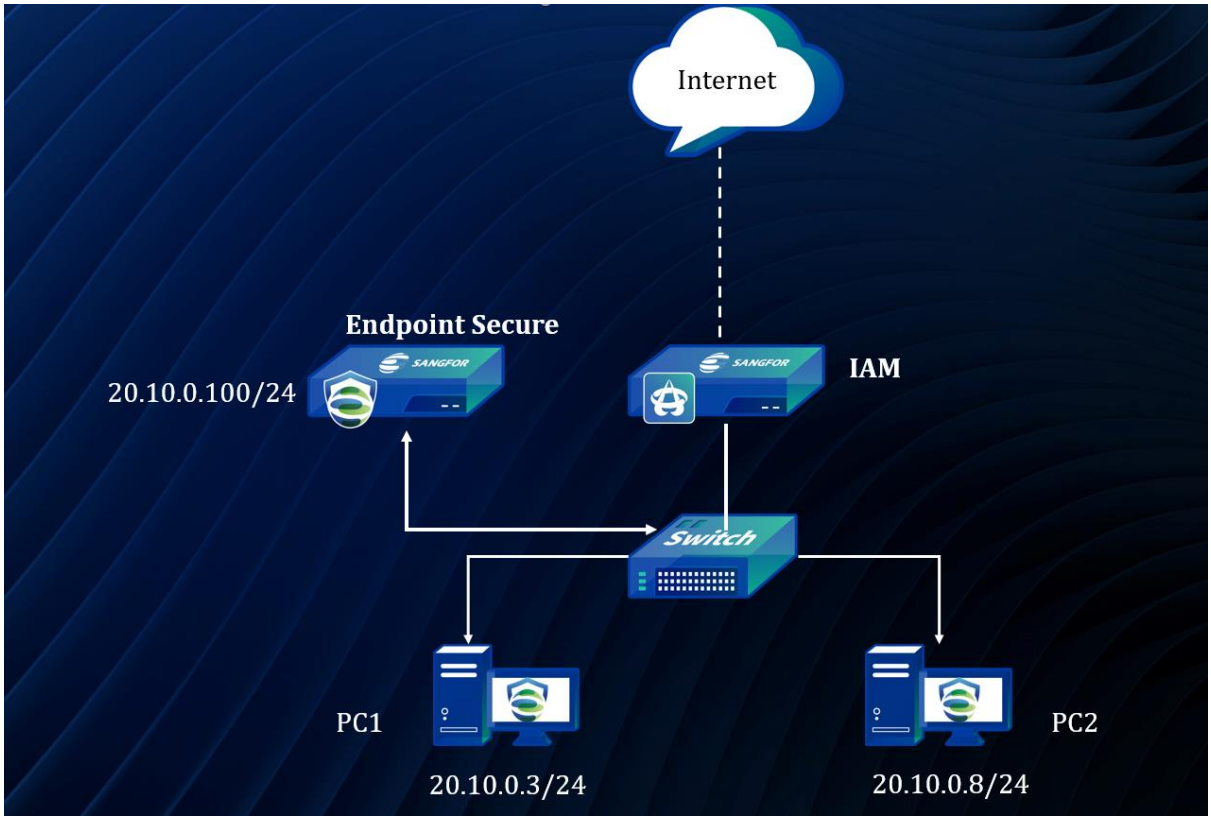
Network terminal intelligent linkage to strengthen threat protection capabilities

IAM supports malicious URL filtering, network antivirus detection, zombie host detection, etc. to protect Internet security;

Endpoint Secure takes the artificial intelligence algorithm as the core, greatly improves the terminal virus security check and kill effect, and can check and kill the new virus threat of ransomware in a comprehensive way.

Through the network terminal linkage, the endpoint threats and attacks discovered by IAM can be linked with Endpoint Secure to scan and repair terminal security in time.

1.2 Topology



Device	Account/Password	IP	Description
PC1	administrator/111111	20.10.0.3/24	
PC2	administrator/111111	20.10.0.8/24	
MGR	admin/@sangfor123	20.10.0.100/24	Endpoint Secure MGR
IAM	admin/@sangfor123	LAN: 20.10.0.1/24	IAM

1.3 Test Introduction

1.3.1 Correlation conditions

1. IAM needs to access ES TCP 443 port. IAM requires version 12.0.16 (inclusive) and above.

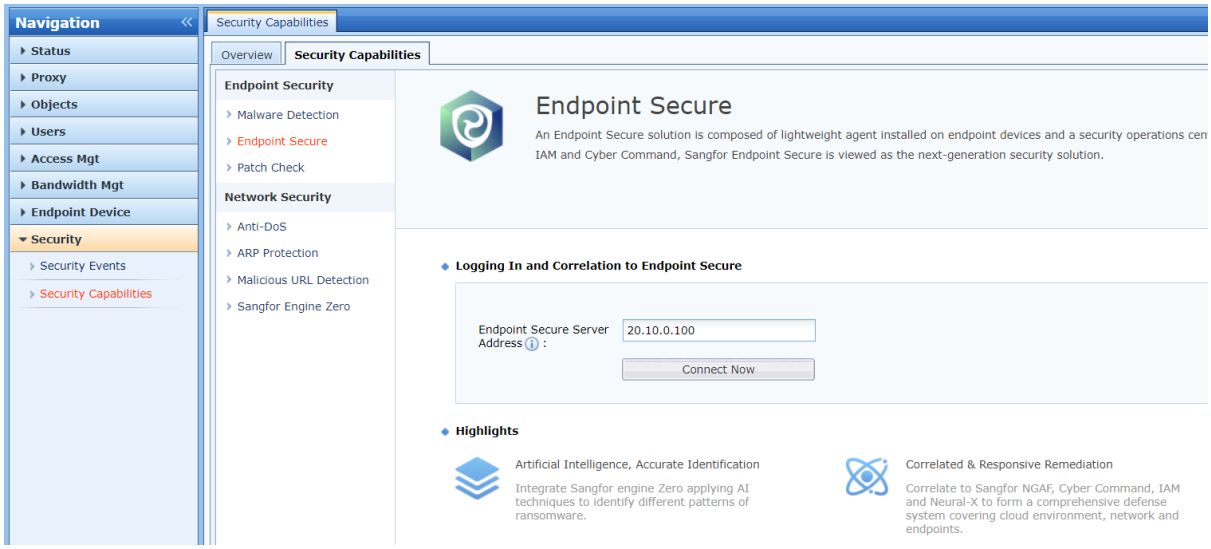
2. Only when the endpoint is recognized as a PC type, IAM/IAG will redirect the terminal's http request to the ES Agent installation page.

In order to allow the terminal to be recognized as a PC type faster, you can download and install QQ and log in.

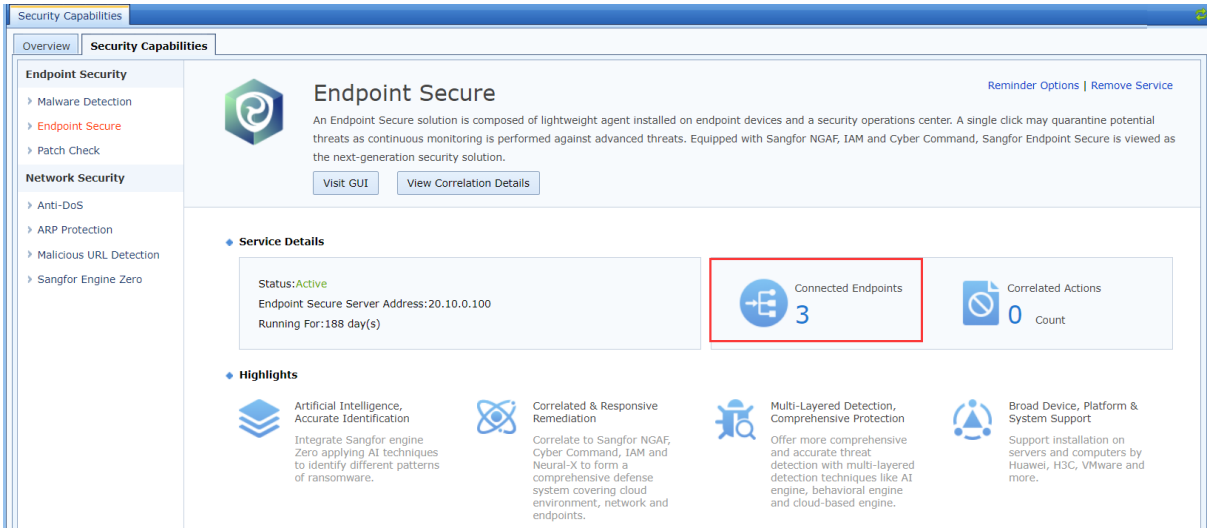
3. IAM/IAG will only redirect http requests to the ES Agent installation page, so please use http web pages to trigger traffic.

Chapter 2 Correlate IAM with Endpoint Secure

1. Log in IAM web console, and go to Security-> Security Capabilities path. Input the IP address of Endpoint Secure.



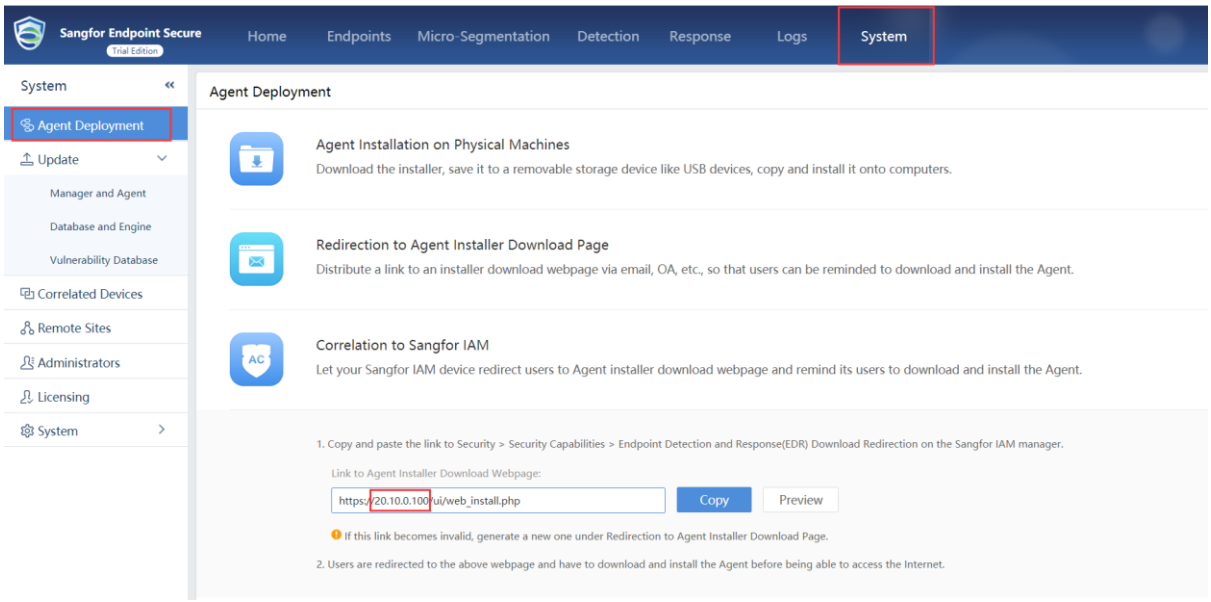
2. After IAM connected to Endpoint Secure, you can see the endpoint counts that how many endpoints already connected to MGR



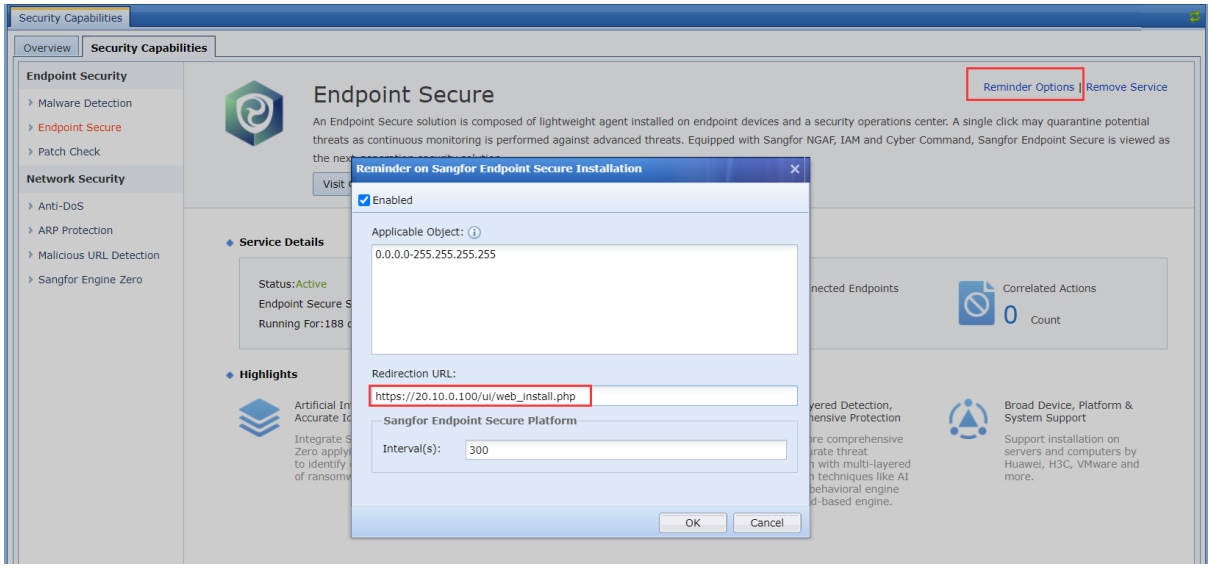
3.In order to IAM could redirect reminder page to risk endpoint, you must configure reminder policy in IAM.

First, configure risk reminder page address in Endpoint Secure, you can you System-> Agent Deployment-> Correlation to Sangfor IAM page and configure ES agent download address so that IAM can direct PC to ES agent download page.

Note: You must ensure that the internal endpoints are able to access the ES agent download address.

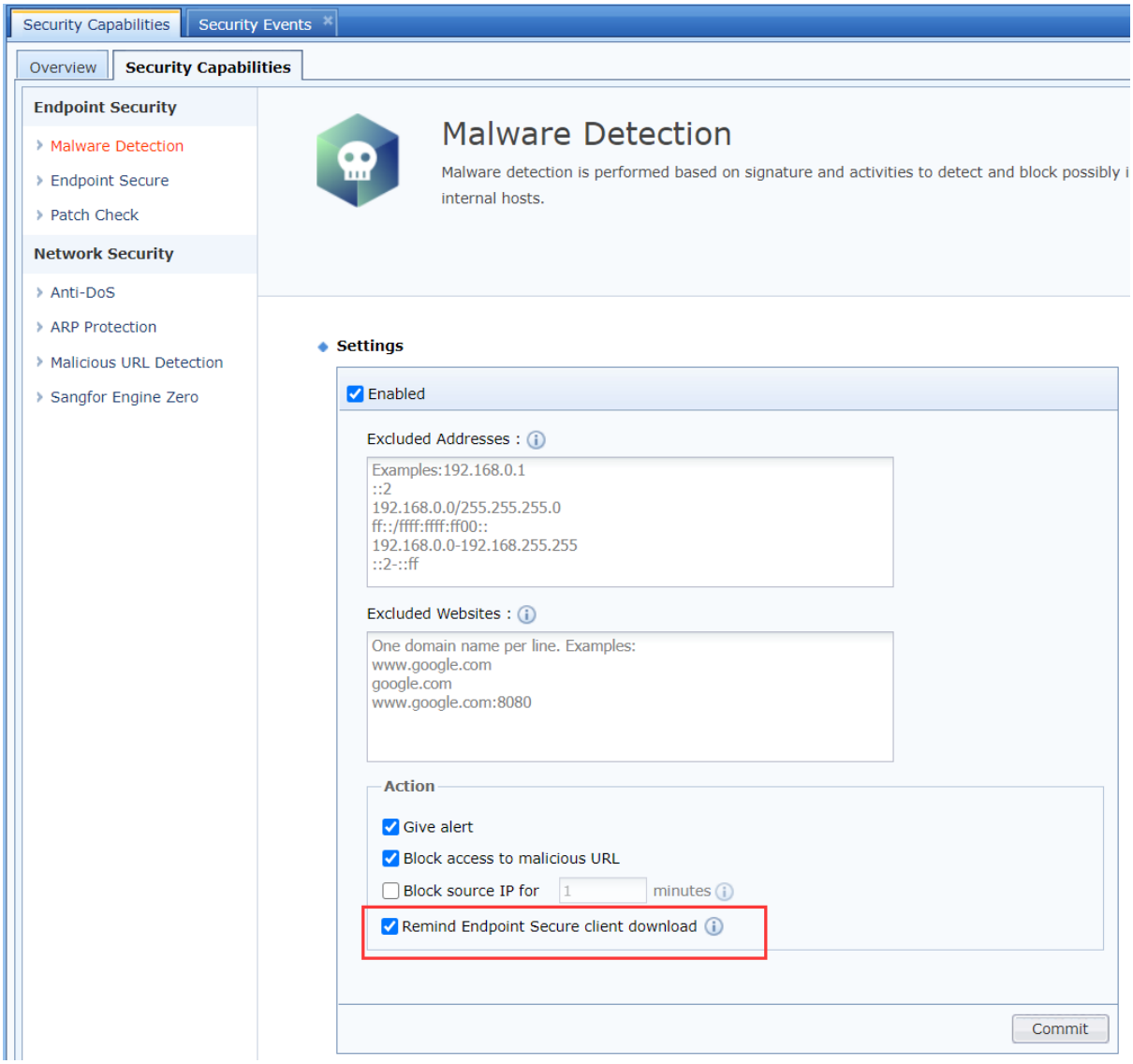


Second, configure reminder policy in IAM, please ensure the redirection URL is same as you configured in ES.

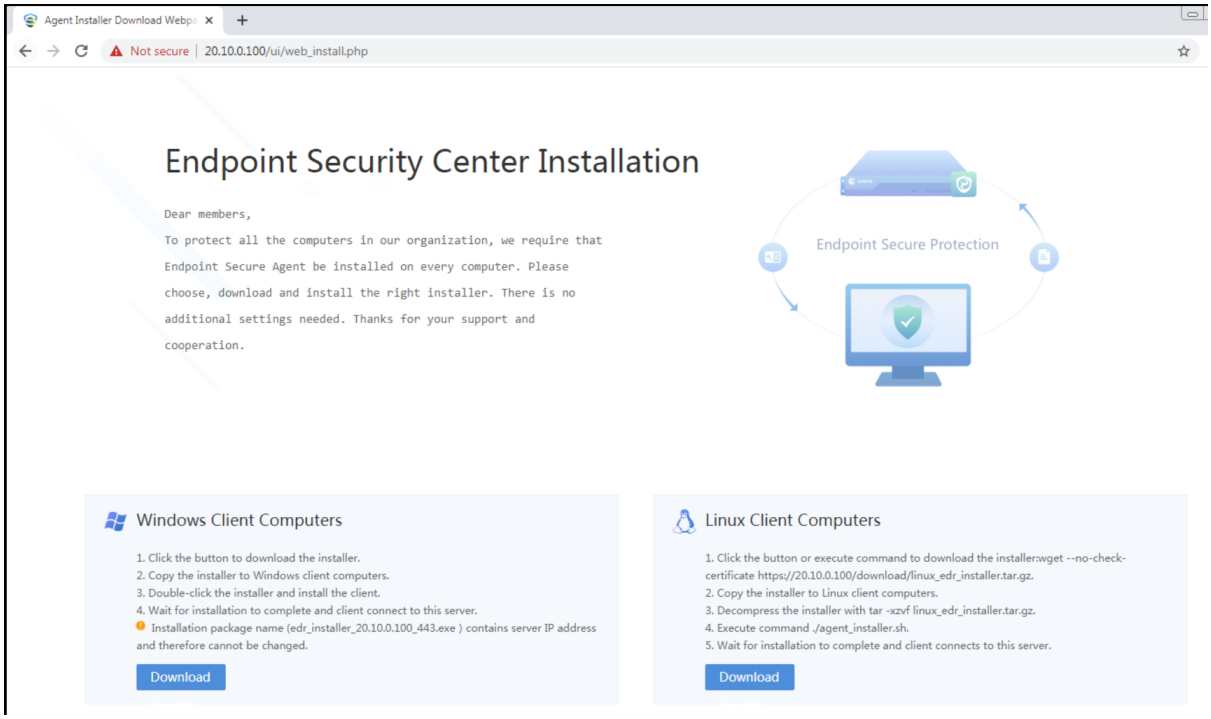


Chapter 3 Configure Security Policy

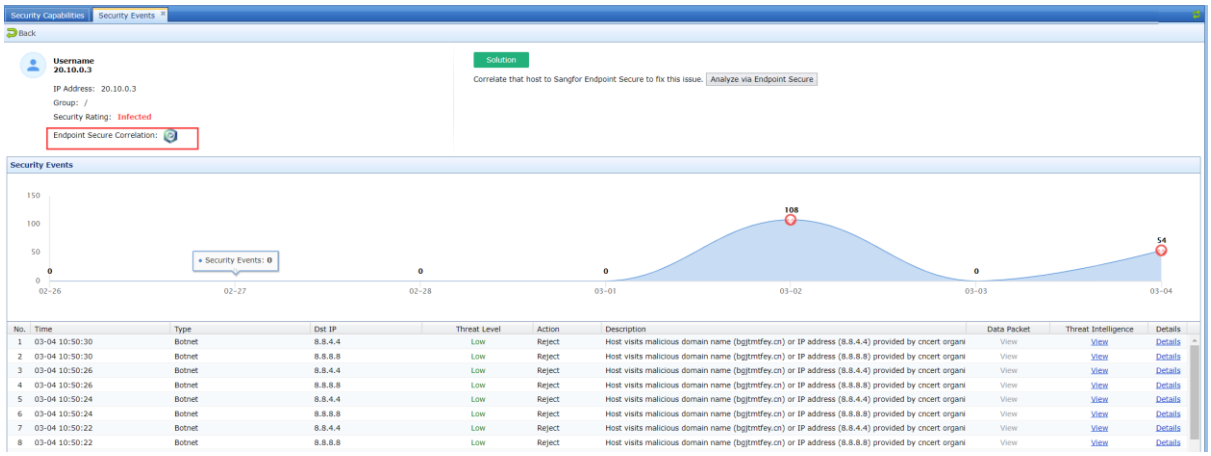
1. Enable Malware Detection Policy in IAM, and you'd better check "Remind Endpoint secure client download".



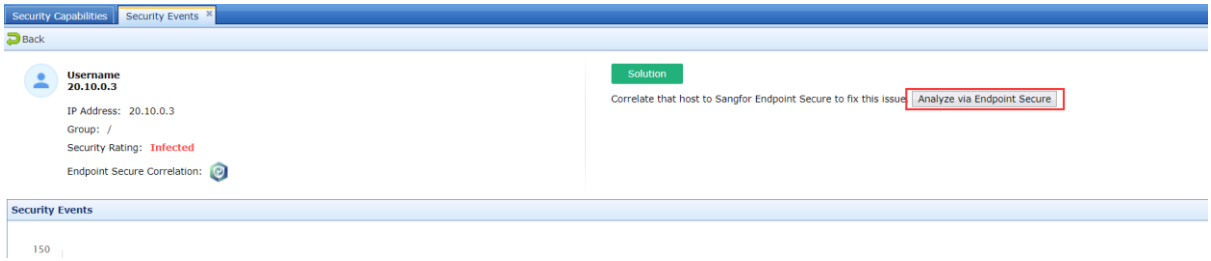
4. After you configured the policy in both IAM and Endpoint, when endpoint access the botnet, IAM will redirect botnet page to ES agent download page.



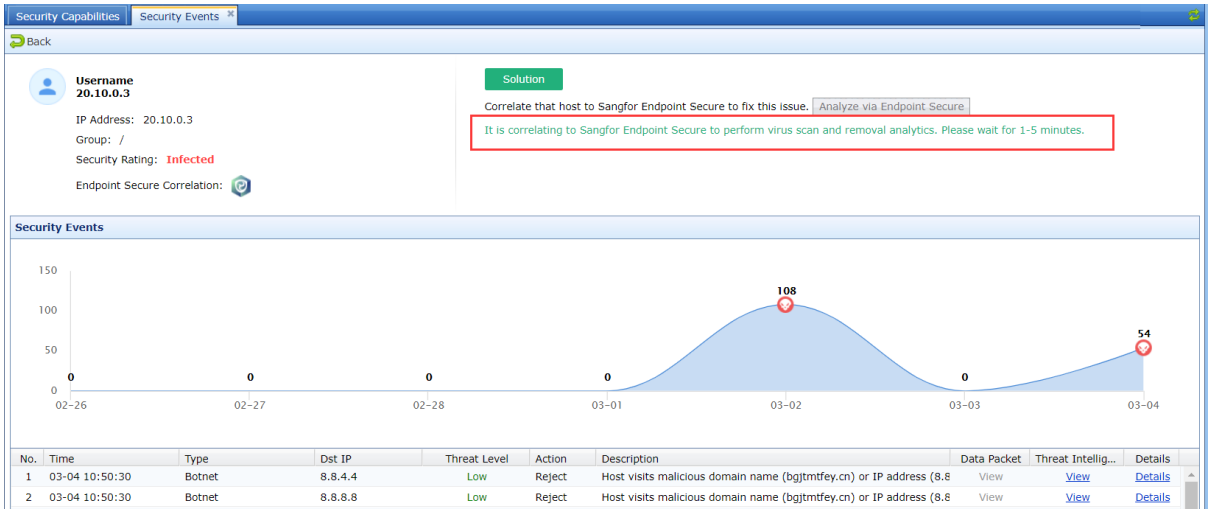
5. After install the ES agent in PC, you can see the connection status in IAM.

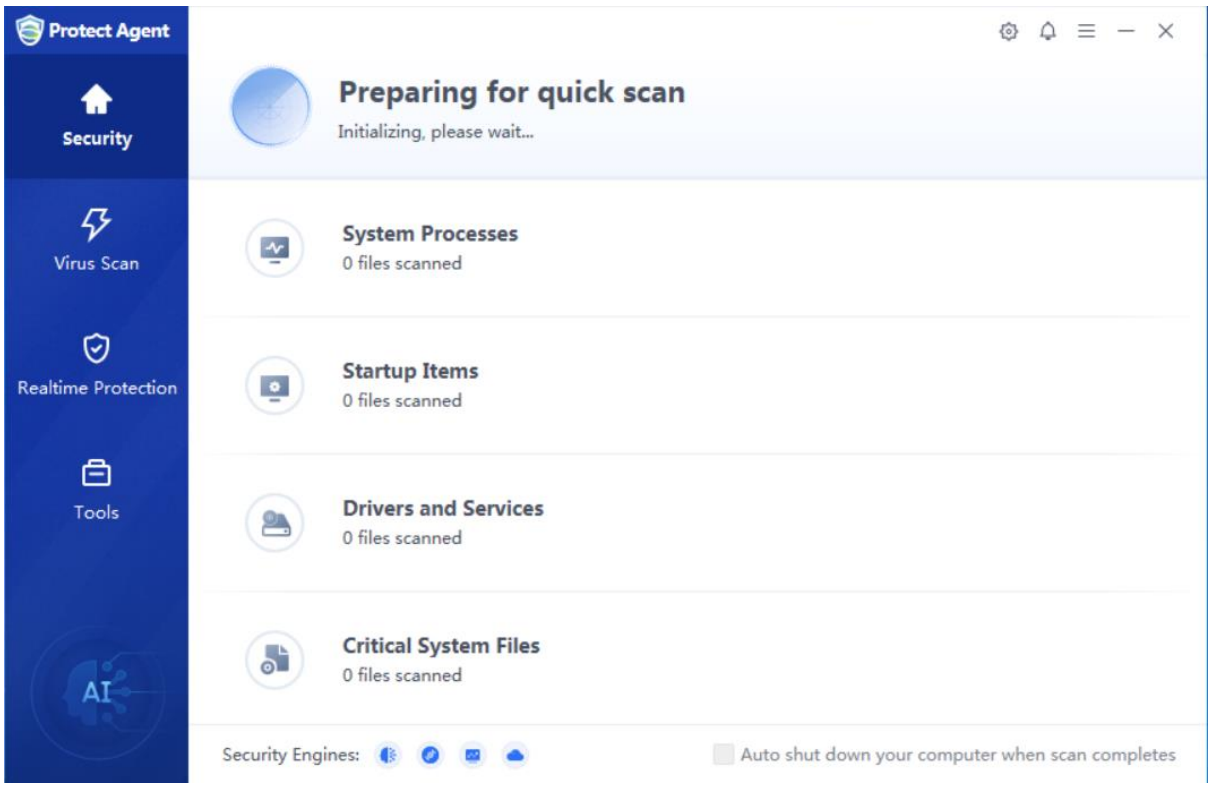


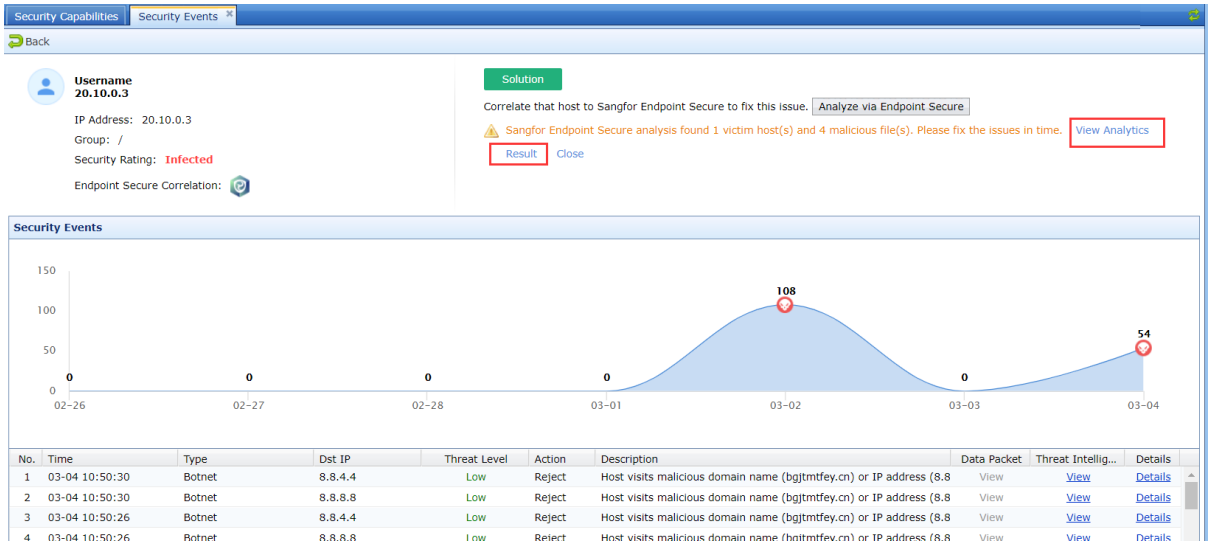
6. If you want to get more information of malware, you can click “Analyze via Endpoint Secure” to correlate to ES agent to scan disk of PC.



7. After ES agent completed the disk, you can view the detail of malware in IAM.


Security Capabilities
Security Events
Back
Username
20.10.0.3
IP Address: 20.10.0.3
Group: /
Security Rating: Infected
Endpoint Secure Correlation:
Solution
Correlate that host to Sangfor Endpoint Secure to fix this issue.
Analyze via Endpoint Secure
It is correlating to Sangfor Endpoint Secure to perform virus scan and removal analytics. Please wait for 1-5 minutes.
Security Events
150
100
50
0
108
54
02-26
02-27
02-28
03-01
03-02
03-03
03-04
No. Time Type Dst IP Threat Level Action Description Data Packet Threat Intellig... Details
1 03-04 10:50:30 Botnet 8.8.4.4 Low Reject Host visits malicious domain name (bgjtmtfey.cn) or IP address (8.8 View View Details
2 03-04 10:50:30 Botnet 8.8.8.8 Low Reject Host visits malicious domain name (bgjtmtfey.cn) or IP address (8.8 View View Details


Protect Agent
Security
Virus Scan
Realtime Protection
Tools
AI
Preparing for quick scan
Initializing, please wait...
System Processes
0 files scanned
Startup Items
0 files scanned
Drivers and Services
0 files scanned
Critical System Files
0 files scanned
Security Engines:
Auto shut down your computer when scan completes


Security Capabilities
Security Events
Back
Username
20.10.0.3
IP Address: 20.10.0.3
Group: /
Security Rating: Infected
Endpoint Secure Correlation:
Solution
Correlate that host to Sangfor Endpoint Secure to fix this issue.
Analyze via Endpoint Secure
Sangfor Endpoint Secure analysis found 1 victim host(s) and 4 malicious file(s). Please fix the issues in time.
View Analytics
Result
Close
Security Events
150
100
50
0
108
54
02-26
02-27
02-28
03-01
03-02
03-03
03-04
No. Time Type Dst IP Threat Level Action Description Data Packet Threat Intellig... Details
1 03-04 10:50:30 Botnet 8.8.4.4 Low Reject Host visits malicious domain name (bgjtmtfey.cn) or IP address (8.8 View View Details
2 03-04 10:50:30 Botnet 8.8.8.8 Low Reject Host visits malicious domain name (bgjtmtfey.cn) or IP address (8.8 View View Details
3 03-04 10:50:26 Botnet 8.8.4.4 Low Reject Host visits malicious domain name (bgjtmtfey.cn) or IP address (8.8 View View Details

8. You can choose to deal with virus files, such as quarantine or ignore virus files.