SANGFOR

Endpoint Secure

Best Practices for Scenarios_One Click Kill the Virus

Version 3.2.22

Change Log

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

CONTENT

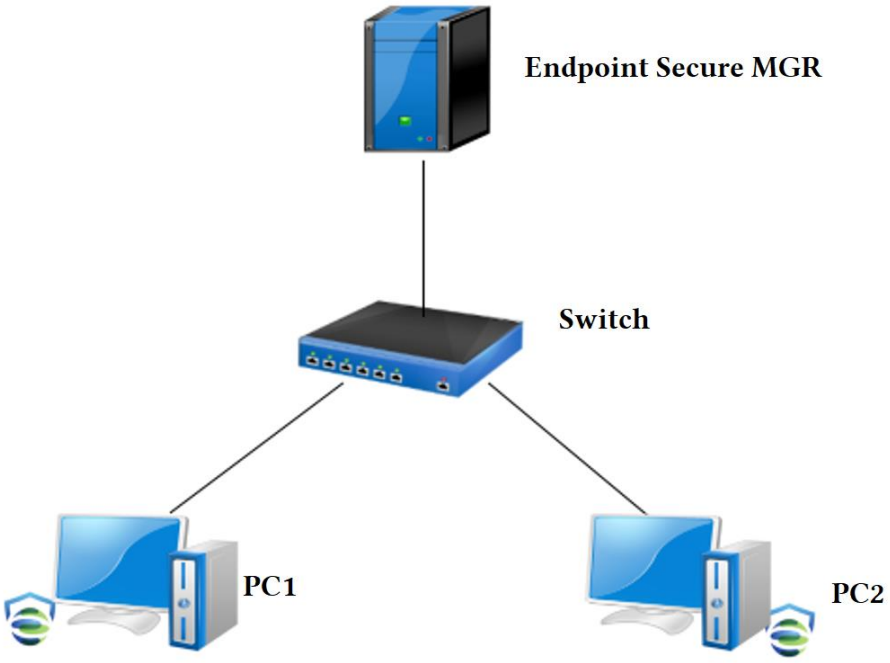
Chapter 1 Scenario

This program demonstrates the process and effect of ransomware attacks when the endpoint does not run the Endpoint Secure Agent, as well as the detection and protection effect against ransomware attacks after deploying the Endpoint Secure Agent. It is suitable for showing customers how the Endpoint Secure Agent detects ransomware attacks and provides protection.

Chapter 2 Preparation

2.1 Environment

2.1.1 Network Environment



Device	Account/Password	IP	Description
PC1	administrator/111111	20.10.0.3	PC initiating ransomware attacks
PC2	administrator/111111	20.10.0.8	PC attacked by ransomware with RDP brute-force cracking
MGR	admin/Endpoint Secure@support	20.10.0.100	Endpoint Secure MGR

Chapter 3 Demonstration Process

3.1 Testing

3.1.1 Content

When Endpoint Secure detects the same virus files on PC1 and PC2, it can fix the same virus files on PC1 and PC2 with one click.

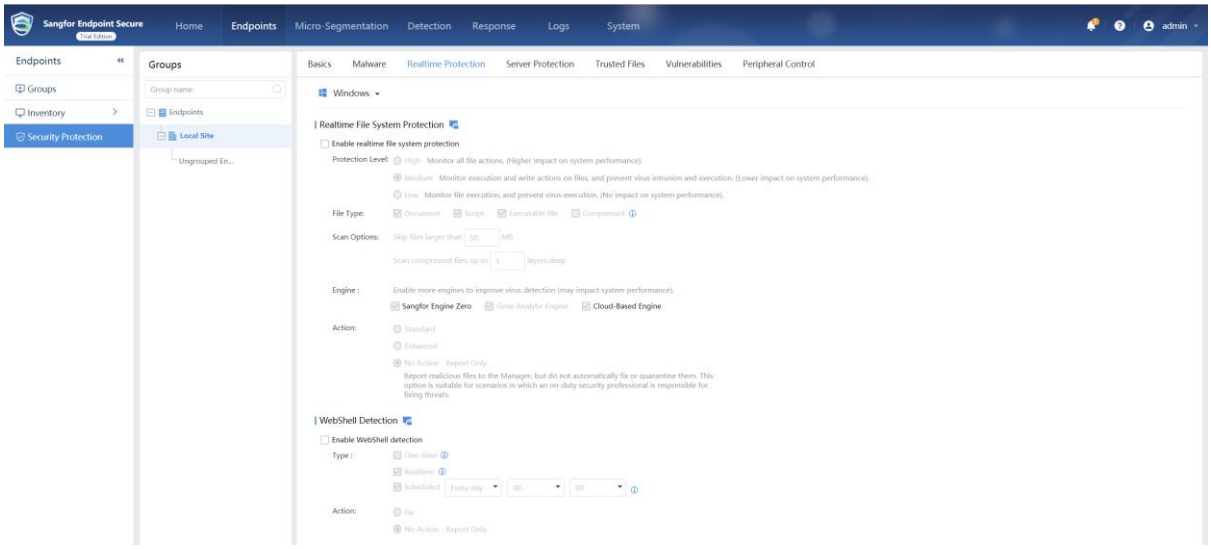
3.1.2 Expected Results

You can see the security incident of PC1 and PC2 in Endpoint Secure, The security incident describes that Endpoint Secure detected the same virus files on PC1 and PC2, and these virus files have the same md5 value. After you choose to fix the virus file in PC1, you can fix the same virus file of other PC.

3.1.3 Steps

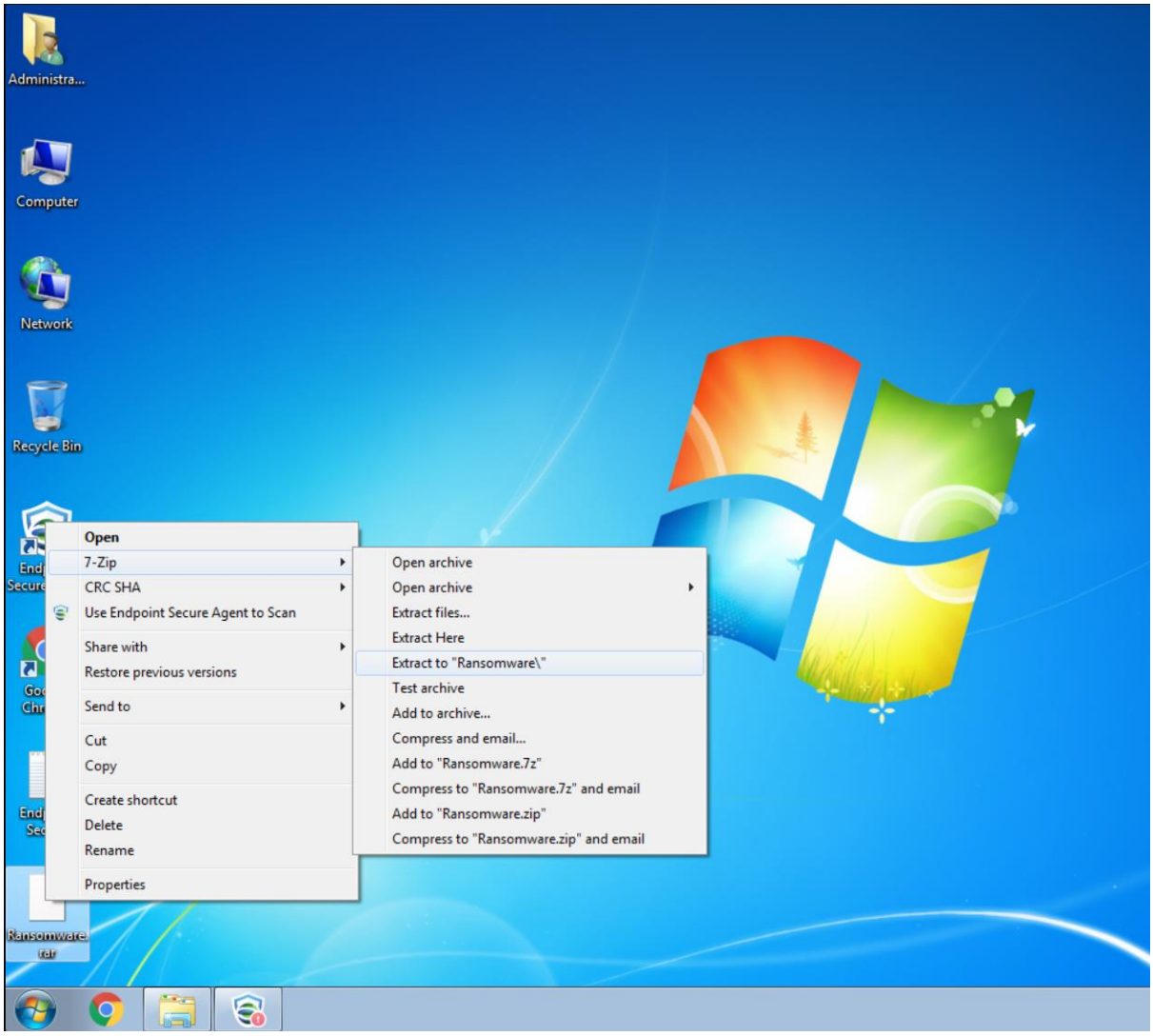
3.1.3.1 Policy Setting

1.Disable all protection policy. If the protection policy enabled, virus file will be fixed automatic by Endpoint Secure, so we need to disable the protection policy to test.

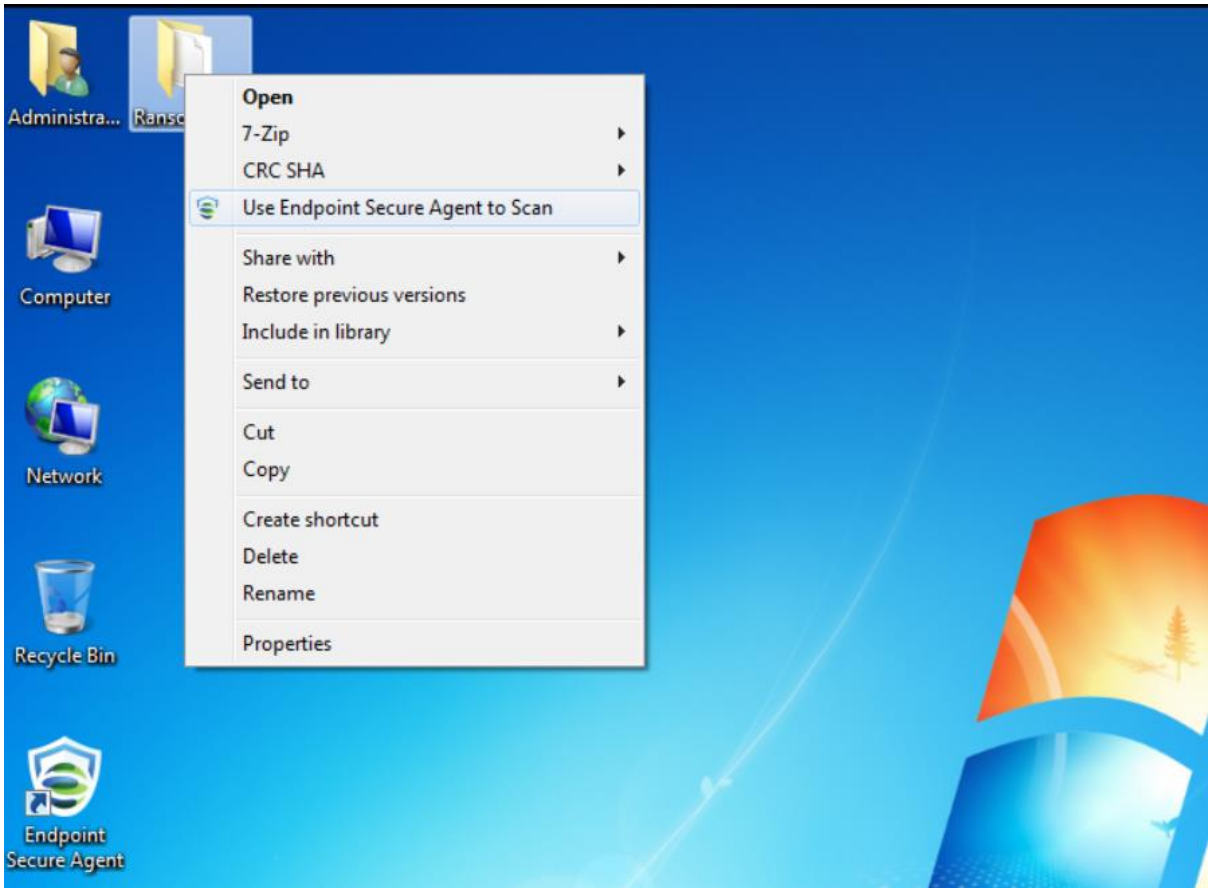


3.1.3.2 Initiating an Attack

1. Unzip virus files on PC1 and PC2.

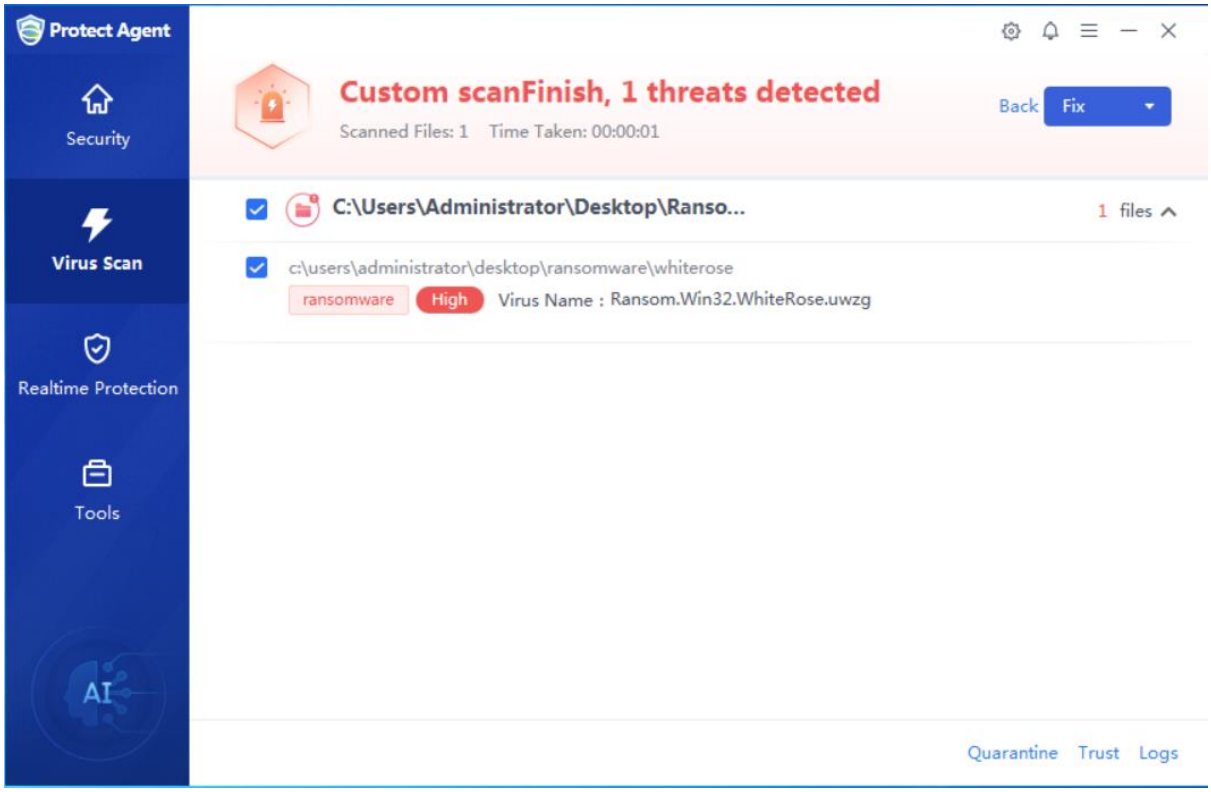


2.You can Use Endpoint Secure Agent scan the virus directory manually, or you can use Endpoint Secure issue the scan task for all PC.

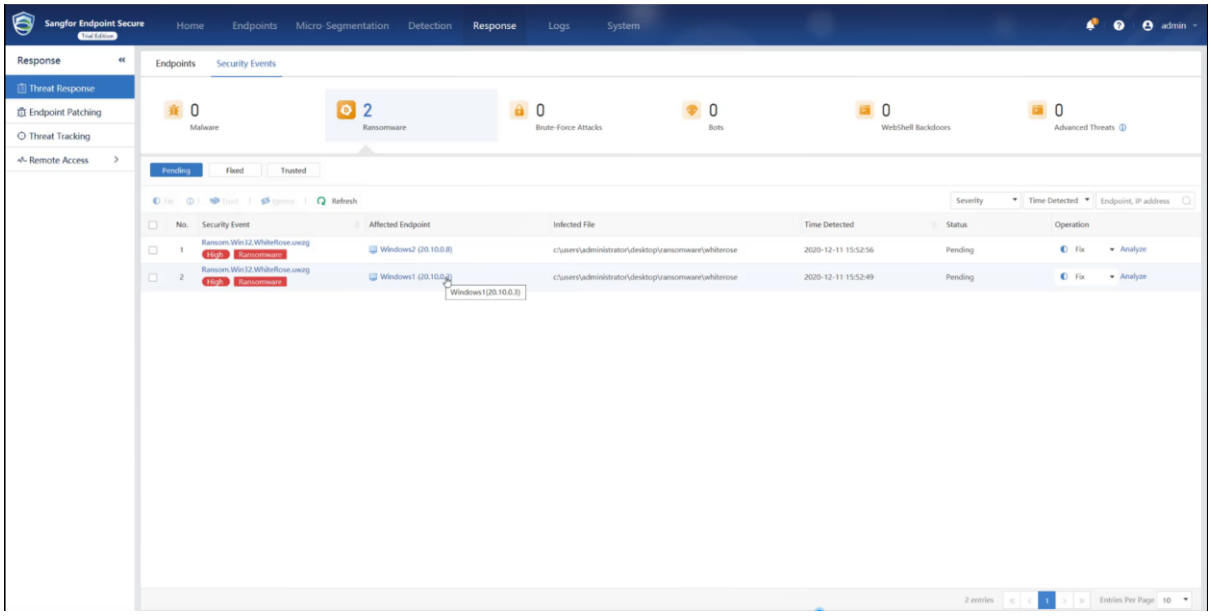


3.1.3.3 Attacking Effect

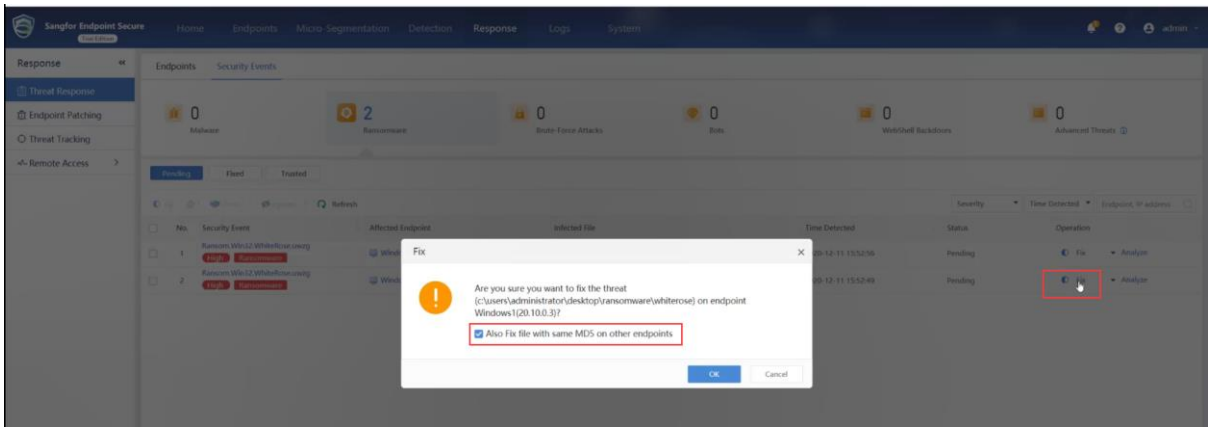
1.You can see that Endpoint Secure can detect the virus file in PC1 and PC2.



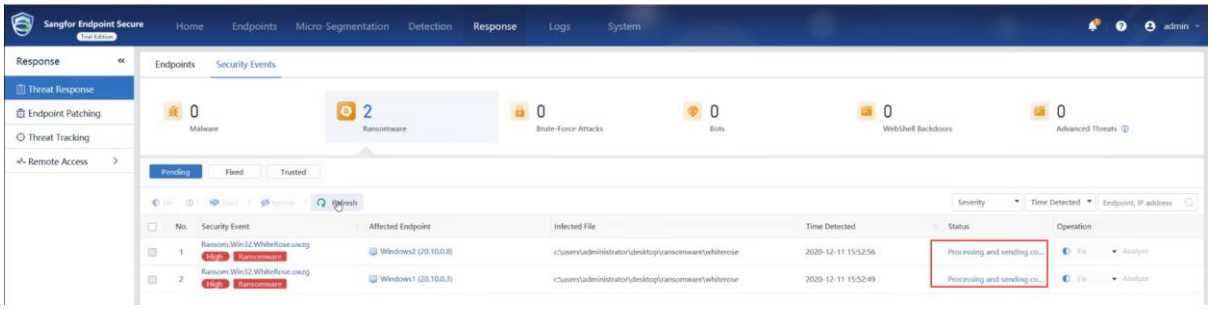
2.You can query security incident in Endpoint Secure MGR.



3.Select one PC and click "Fix". And check "Also Fix file with same MD5 on other endpoints"



4. Wait Endpoint Secure MGR issue fix task.



5. After fix task finished, you can see the virus in PC1 was fixed and same in PC2.