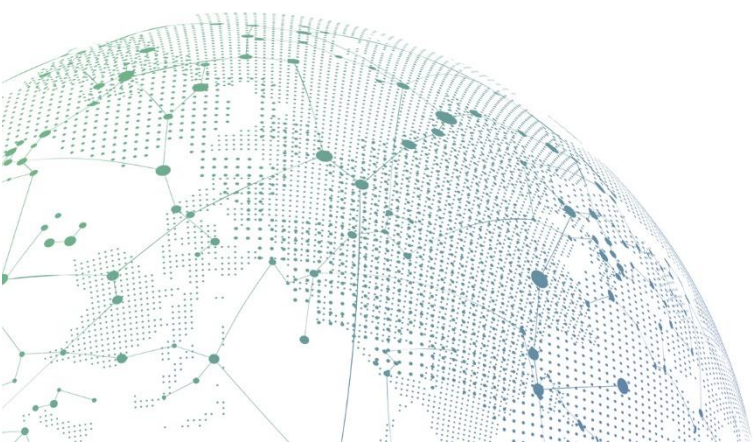




Endpoint Secure Best Practices untuk Skenario Berkorelasi dengan IAM untuk Mencegah Ancaman Jaringan

Versi 3.2.22



Catatan Perubahan

Tanggal	Deskripsi Perubahan
25 Februari 2021	Dokumen diterbitkan.
17 Mei 2021	Dokumen diperbaharui.

DAFTAR ISI

Bagian 1 Skenario1

1.1 Skenario1

1.2 Topologi2

1.3 Uji Coba Pengenalan3

Bagian 2 Korelasi IAM dengan Endpoint Secure4

Bagian 3 Konfigurasi Security Policy6

Bagian 1 Skenario

1.1 Skenario

Permasalahan yang saat ini dihadapi pelanggan.

Internet telah menjadi alat produktifitas yang sangat dibutuhkan bagi karyawan. Tetapi, karena kompleksnya lingkungan network dan maraknya ancaman dari berbagai jenis virus, terdapat berbagai masalah dalam manajemen internet dan keamanan yang tidak ada batasannya.

Sisi Network:

1. Aplikasi dengan Bandwidth tinggi seperti video mengambil banyak jatah bandwidth, sehingga berdampak pada karyawan lainnya yang saat mengakses internet akan menjadi lebih lambat, dan komplain internal pun meningkat.
2. Ketika karyawan sedang bekerja, mereka menggunakan internet untuk mengakses website hiburan, yang sangat mempengaruhi efisiensi pekerjaan.
3. Terdapat banyak aplikasi yang mengirimkan file keluar ranah internal seperti email, disk web dan QQ WeChat, sehingga resiko kebocoran data semakin besar, dan tidak banyak metode untuk melacaknya.

Sisi Endpoint:

1. Aset endpoint tidak sepenuhnya terurut, terminal aset yang ingin dilindungi menjadi tidak dikenali dan orang yang bertanggung jawab terhadap terminal itu juga tidak dapat dikenali.
2. Endpoint seringkali disisipi oleh virus, dan karena secara internal tidak ada pembatasan menyebabkan penyebaran yang cepat sehingga menjadi ancaman serius terhadap Local Area Network.
3. Para karyawan memiliki kesadaran keamanan yang rendah, dan resiko kerentanan operating system sangat signifikan, dimana sangat mudah menyebabkan ancaman menjadi tersebar.

Produk IAM dan Endpoint Secure telah dintegrasikan untuk membantu pelanggan mendapatkan lingkungan internet yang nyaman, aman, efisien dan mudah digunakan.

Autentikasi menggunakan data pengguna memastikan keamanan berdasarkan identitas pengguna.

Untuk mendapatkan autentikasi secara kabel dan wireless, IAM menyediakan beberapa metode autentikasi seperti 802.1x, bypass non-sensing, dan wireless Portal;

Menyediakan 29 metode autentikasi seperti AD domain, SMS, WeChat, dll., dimana dapat menjadi pilihan yang fleksibel sesuai skenario Internet;

Kontrol internet yang akurat, dan flow control memastikan pengalaman internet dan

bekerja secara efisien.

IAM telah menjadi pelopor feature application identification library dan URL library, menyediakan segmen aplikasi manajemen dan kontrol, memblokir aplikasi yang tidak relevan dan menjadikan karyawan lebih efisien dalam menggunakan internet.

IAM telah mengakumulasi teknologi manajemen traffic profesional selama 10 tahun untuk memastikan pengalaman internet aplikasi secara normal, membatasi penggunaan aplikasi hiburan seperti pengunduhan audio dan video, dan meningkatkan performa penggunaan bandwidth sebesar 30%.

Audit keluar secara menyeluruh, menemukan risiko kebocoran data.

Sangfor IAM memiliki teknologi identifikasi dan audit profesional sesuai industri dan dapat secara efektif mengaudit berbagai tingkah laku pengguna online dan data keluar, termasuk mengaudit isi dari data keluar seperti dari web, email, cloud storage, WeChat, and QQ.

Melalui berbagai audit dan analisis dari pihak luar, kami menemukan celah dari kelakuan yang tidak wajar, peringatan lebih dulu terhadap risiko kebocoran, dan secara cepat menemukan sumber kebocoran.

Keamanan akses sekuriti Endpoint memastikan keamanan akses ke terminal.

Software keamanan endpoint terpasang secara resmi, dan software endpoint terminal dapat diinstall setelah ada sertifikat IAM.

Inspeksi akses keamanan Endpoint, termasuk pemindaian kelemahan sistem, instalasi antivirus, interface terbuka, dll hanya endpoint yang telah memenuhi standar keamanan yang diizinkan masuk ke jaringan;

Pemindaian kelemahan sistem endpoint real-time, kelemahan sistem dipindai, secara otomatis akan diperbaiki dan dilaporkan.

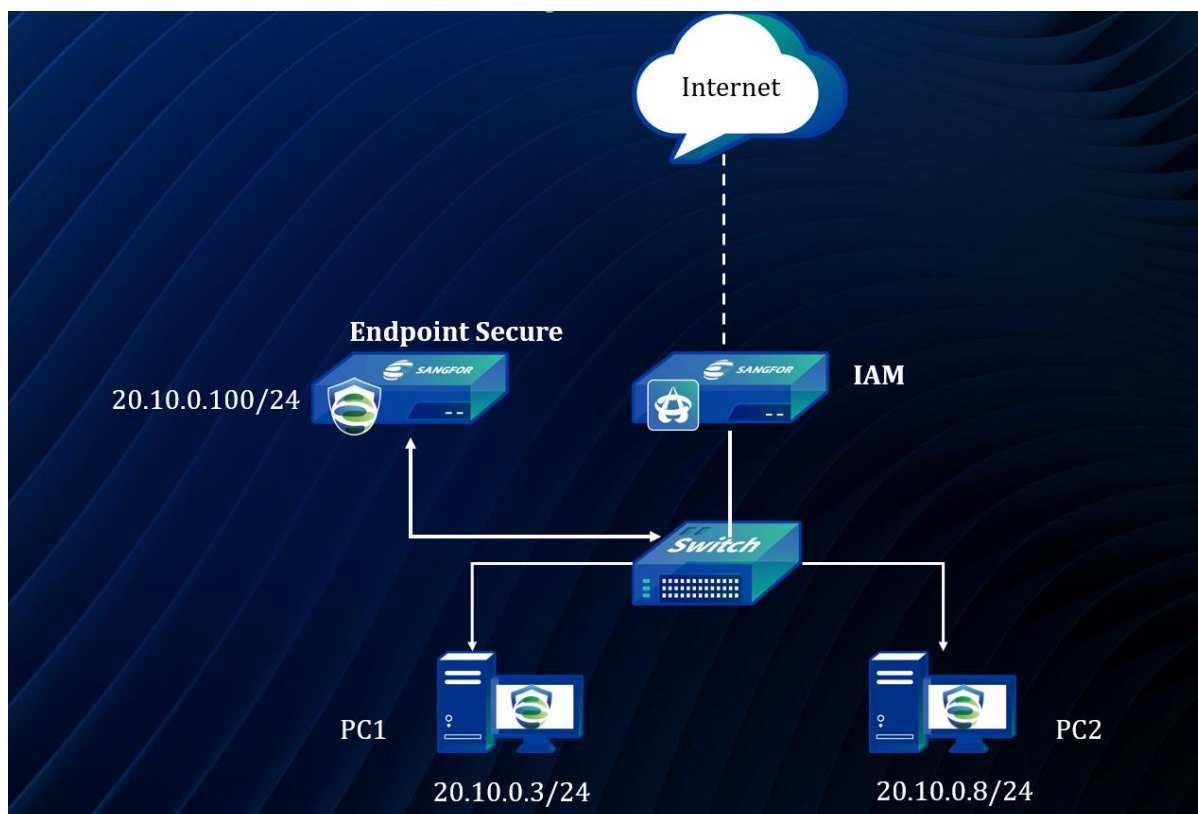
Terminal jaringan secara cerdas terhubung untuk menguatkan kemampuan proteksi.

IAM mendukung malicious URL filtering, network antivirus detection, zombie host detection, dll. sampai melindungi Internet security;

Endpoint Secure menggunakan algoritma artificial intelligence sebagai inti, sangat meningkatkan efek pengecekan dan membunuh virus pada terminal, dan dapat memeriksa dan membunuh virus baru ransomware dengan cara yang komprehensif.

Melalui jaringan terminal, ancaman ke endpoint terdeteksi oleh IAM kemudian endpoint secure memindai dan memperbaiki terminal di waktu bersamaan.

1.2 Topologi

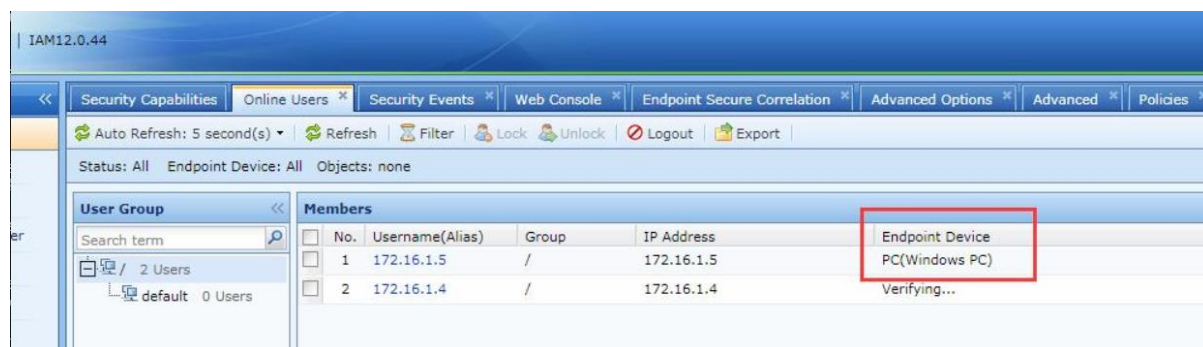


Perangkat	Akun/Password	IP	Deskripsi
PC1	administrator/111111	20.10.0.3/24	
PC2	administrator/111111	20.10.0.8/24	
MGR	admin/@sangfor123	20.10.0.100/24	Endpoint Secure MGR
IAM	admin/@sangfor123	LAN: 20.10.0.1/24	IAM

1.3 Ujicoba Pengenalan

1.3.1 Kondisi Korelasi

1. IAM membutuhkan akses ke ES TCP Port 443, IAM harus versi 12.0.16 atau di atasnya.
2. Ketika endpoint dikenali sebagai PC, IAM/IAG akan mengalihkan permintaan http terminal ke halaman instalasi ES.

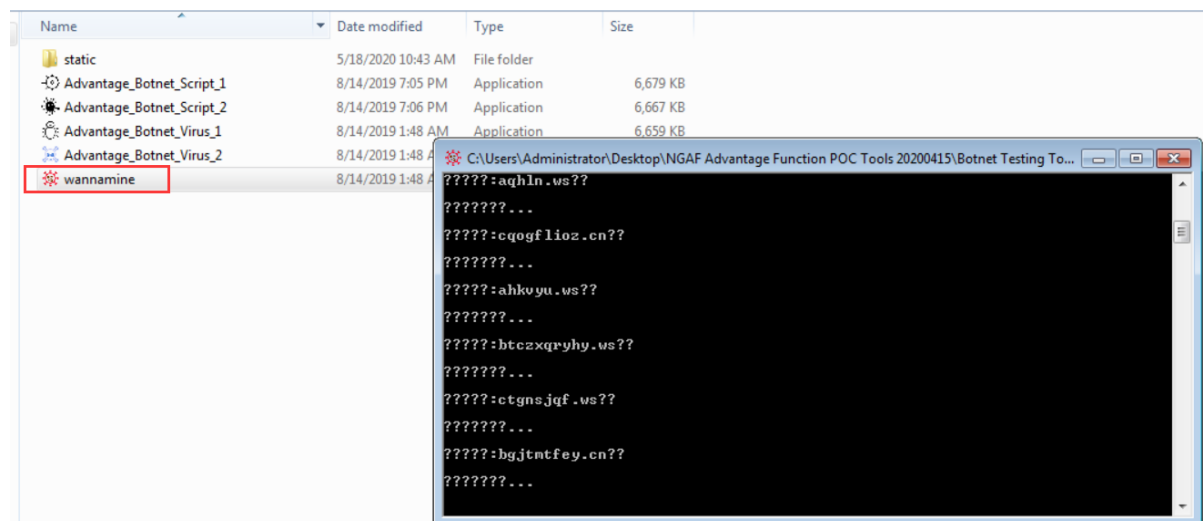
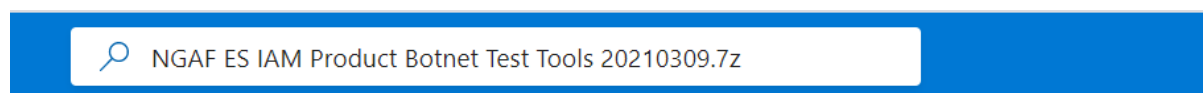


Agar terminal dapat mengenali PC lebih cepat, anda dapat mengunduh dan menginstal QQ dan masuk.

3. IAM/IAG hanya akan mengalihkan permintaan http ke halaman instalasi agen ES, jadi tolong gunakan http untuk membuatnya halamannya muncul.

1.3.2 Ujicoba Alat

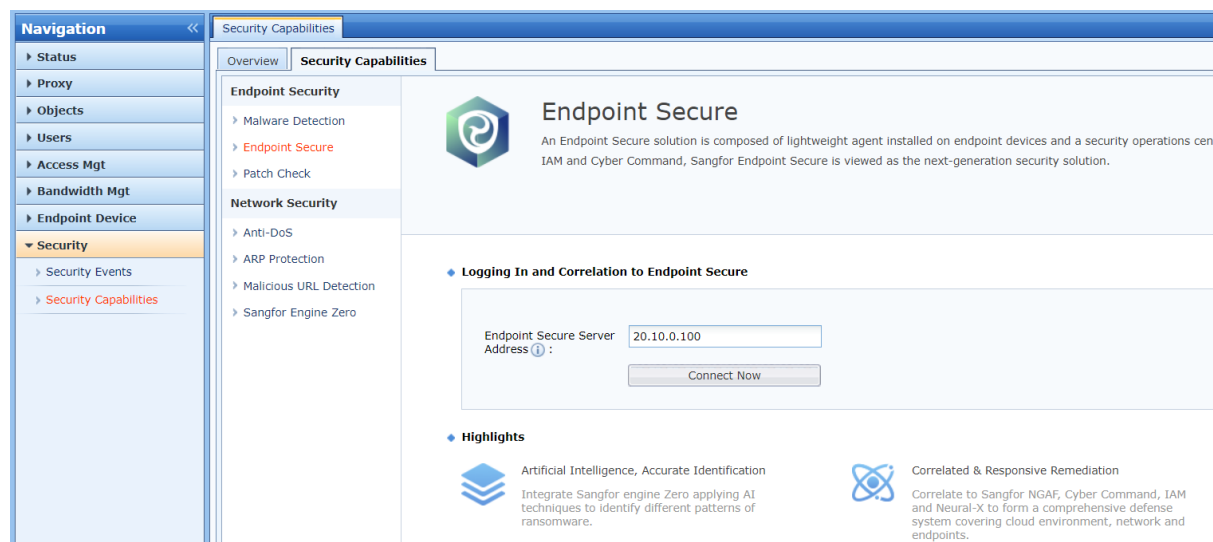
1. Untuk mengetes Botnet, kamu dapat menggunakan **NGAF ES IAM Product Botnet Test Tools 20210309.7z**, carilah di PMO. Lalu jalankan wannamine.exe di PC. Wannamine.exe akan mencoba menggunakan DNS untuk menyelesaikan Botnet URL.



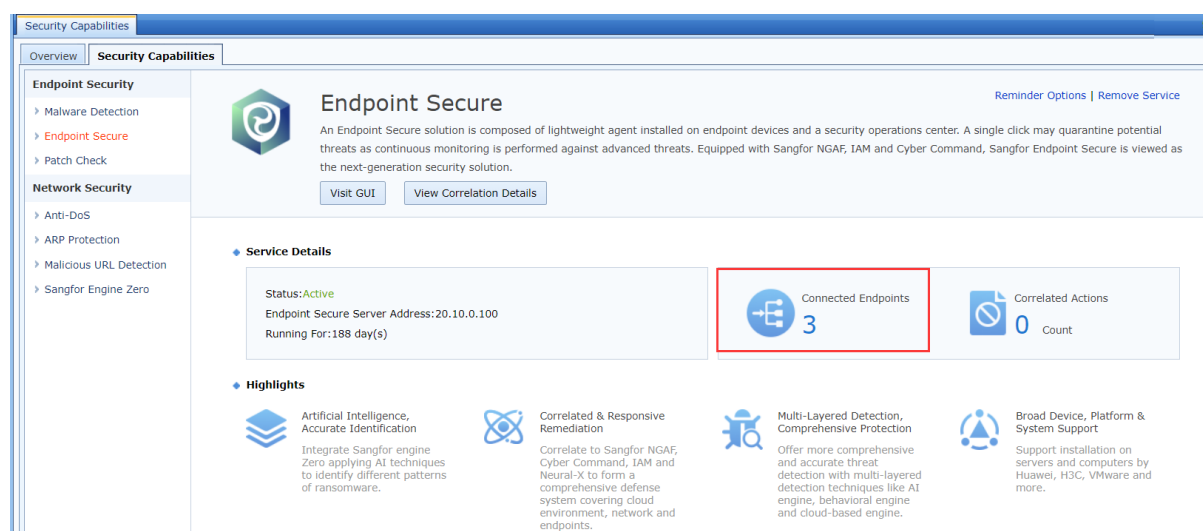
Chapter 2 Korelasi IAM dengan Endpoint Secure

Korelasi IAM untuk Mencegah Ancaman Network

1. Masuk ke dalam console web IAM, lalu pergi ke security→ Security Capabilities path. Masukkan alamat IP dari Endpoint Secure.



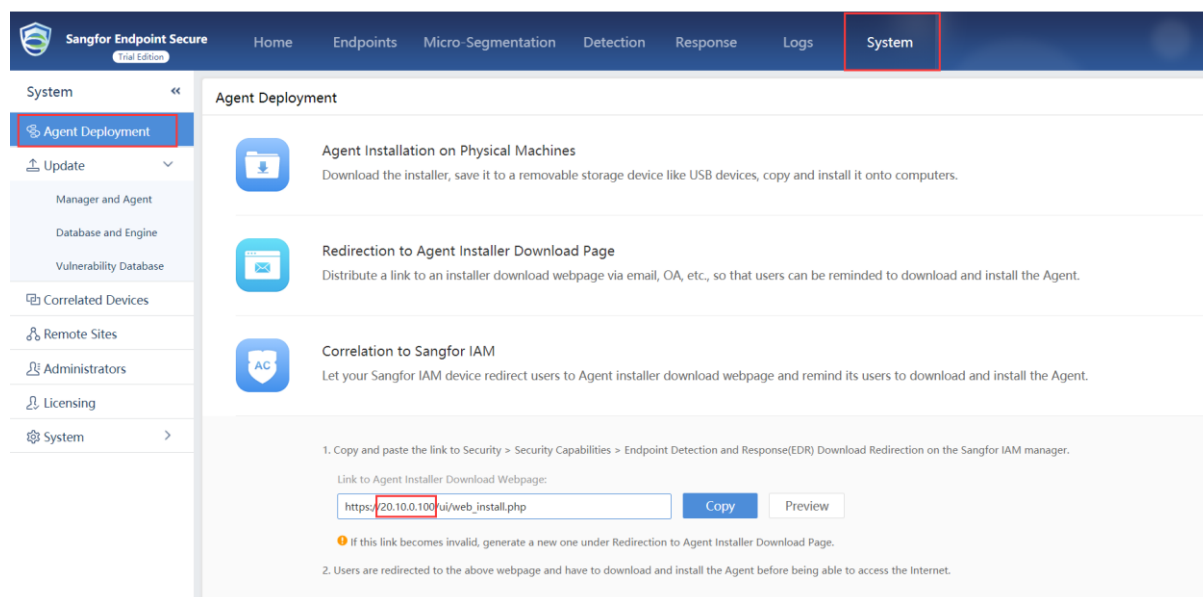
2. Setelah IAM terhubung ke Endpoint Secure, Anda dapat melihat jumlah endpoint yang telah terkoneksi ke MGR.



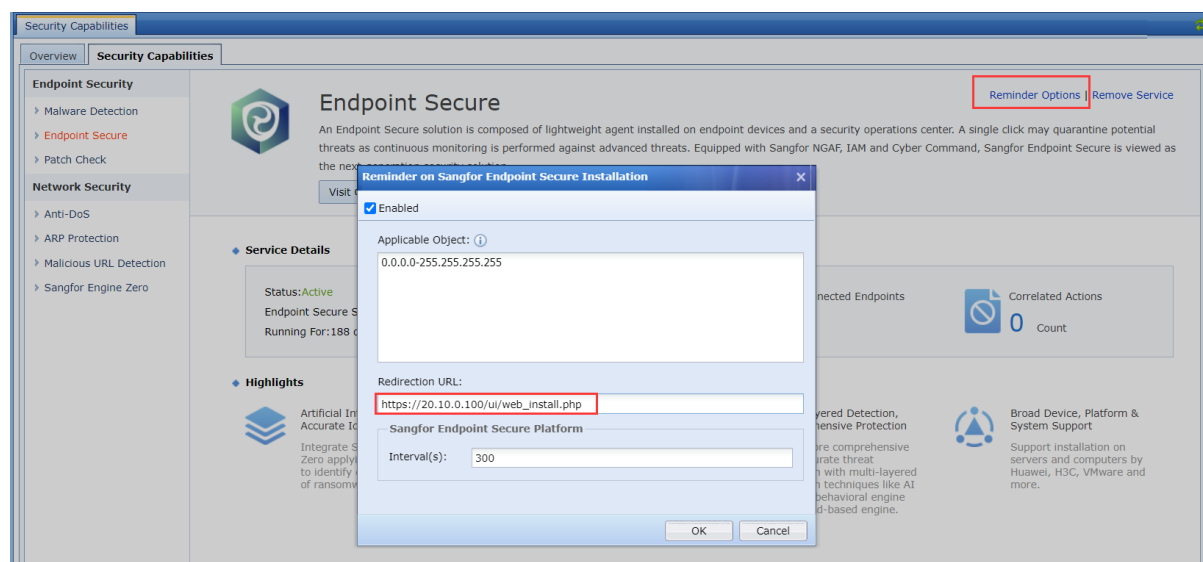
3. Agar IAM mengalihkan halaman peringatan ke resiko endpoint, anda harus mengatur policy di IAM.

Pertama, atur halaman peringatan resiko di Endpoint Secure, anda dapat melakukannya melalui System-> Agent Deployment-> Correlation ke halaman Sangfor IAM dan mengatur alamat ES agent download agar IAM dapat mengalihkan PC ke halaman download agen ES. Catatan: Anda harus memastikan bahwa endpoint internal anda dapat mengakses alamat ES agent download.

Korelasi IAM untuk Mencegah Ancaman Network

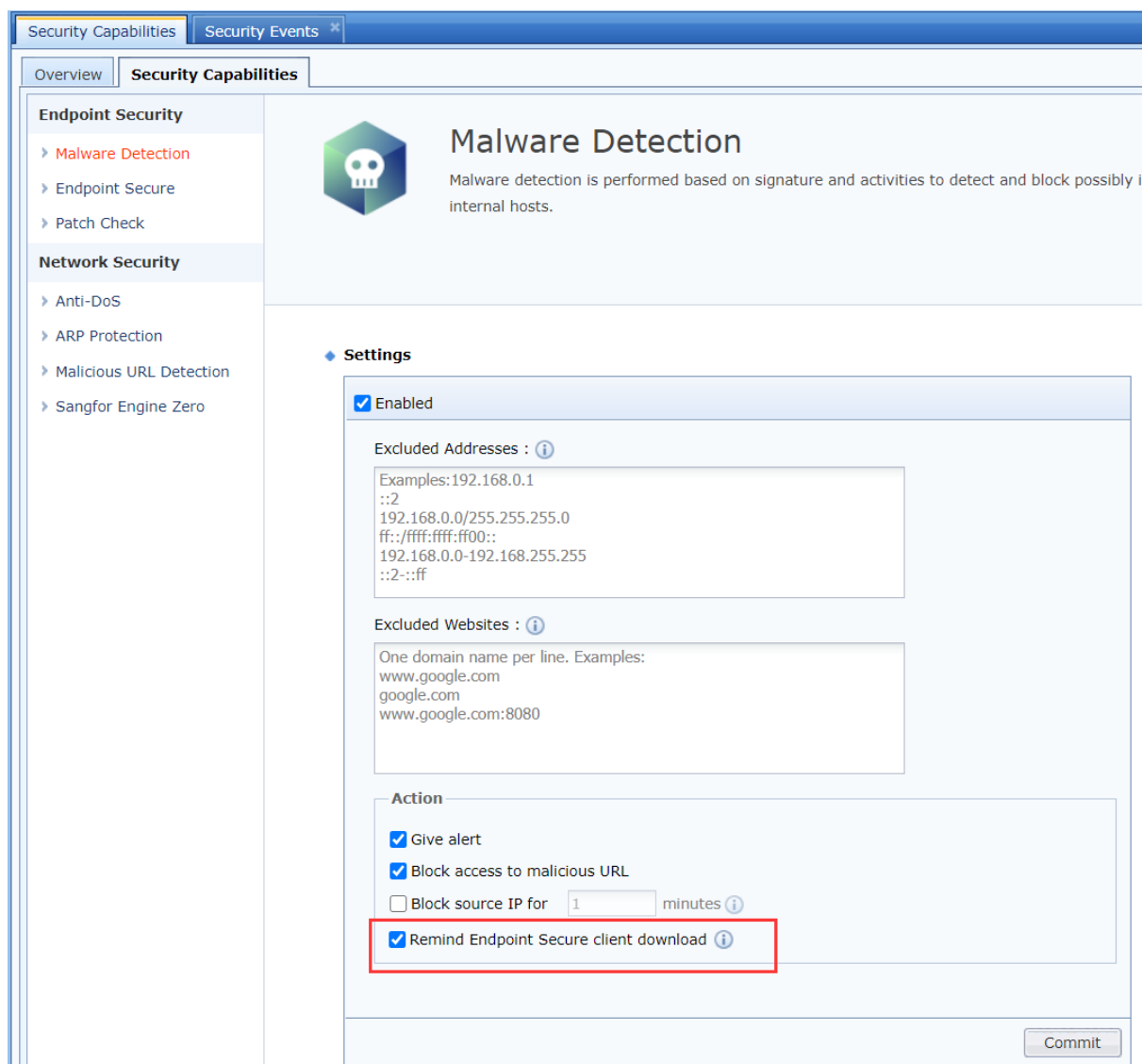


Kedua, atur reminder policy di IAM, mohon pastikan alamat URL sama dengan yang telah dikonfigurasi di ES.



Bagian 3 Konfigurasi Security Policy

1. Aktifkan Malware Detection Policy di IAM, dan anda sebaiknya mencentang "Remind Endpoint secure client download".



4. Setelah ada melakukan konfigurasi policy baik di IAM dan Endpoint, Jika endpoint mengakses botnet, IAM akan mengalihkan halaman botnet ke halaman unduh agent ES.

Agent Installer Download Web: x +

Not secure | 20.10.0.100/ui/web_install.php

Endpoint Security Center Installation

Dear members,

To protect all the computers in our organization, we require that Endpoint Secure Agent be installed on every computer. Please choose, download and install the right installer. There is no additional settings needed. Thanks for your support and cooperation.

Windows Client Computers

1. Click the button to download the installer.
2. Copy the installer to Windows client computers.
3. Double-click the installer and install the client.
4. Wait for installation to complete and client connect to this server.

Installation package name (edr_installer_20.10.0.100_443.exe) contains server IP address and therefore cannot be changed.

Download

Linux Client Computers

1. Click the button or execute command to download the installer: `wget --no-check-certificate https://20.10.0.100/download/linux_edr_installer.tar.gz`.
2. Copy the installer to Linux client computers.
3. Decompress the installer with `tar -xvf linux_edr_installer.tar.gz`.
4. Execute command `./agent_installer.sh`.
5. Wait for installation to complete and client connects to this server.

Download

5. Setelah menginstall agen ES di PC, anda dapat melihat status koneksinya di 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](#)

Security Events

150

0 50 100 150

02-26 02-27 02-28 03-01 03-02 03-03 03-04

Security Events: 0

108

54

No.	Time	Type	Det IP	Threat Level	Action	Description	Data Packet	Threat Intelligence	Details
1	03-04 10:50:30	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.4.4) provided by cn-cert.org	View	View	Details
2	03-04 10:50:30	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.8.8) provided by cn-cert.org	View	View	Details
3	03-04 10:50:26	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.4.4) provided by cn-cert.org	View	View	Details
4	03-04 10:50:26	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.8.8) provided by cn-cert.org	View	View	Details
5	03-04 10:50:24	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.4.4) provided by cn-cert.org	View	View	Details
6	03-04 10:50:24	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.8.8) provided by cn-cert.org	View	View	Details
7	03-04 10:50:22	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.4.4) provided by cn-cert.org	View	View	Details
8	03-04 10:50:22	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (bgmtmfey.cn) or IP address (8.8.8.8) provided by cn-cert.org	View	View	Details

6. Jika anda ingin mendapatkan informasi lebih perihal malware, anda dapat mengklik "Analyze via Endpoint Secure" untuk mengkorelasi agen ES agar memindai disk PC.

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](#)

Security Events

150

7. Setelah agen ES menyelesaikan disk, anda dapat melihat detail dari malware di IAM.

Korelasi IAM untuk Mencegah Ancaman Network

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

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 (bgjtmfey.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 (bgjtmfey.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

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 (bgjtmfey.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 (bgjtmfey.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 (bgjtmfey.cn) or IP address (8.8	View	View	Details
4	03-04 10:50:26	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (bgjtmfey.cn) or IP address (8.8	View	View	Details

8. Anda dapat memilih untuk mengkarantina atau mengabaikan file virus tersebut.

Analytics Results						
<input type="checkbox"/> Isolate <input checked="" type="checkbox"/> Trust <input type="checkbox"/> Ignore						
<input type="checkbox"/>	No.	Host(s)	Virus Type	Infected Files	Status	Operation
<input type="checkbox"/>	1	20.10.0.3	Ransom virus	Malicious Files: c:\users\administrator\desktop File Hash: 00BD67CFCCF7141C8FB6C622442B Time Detected: 2021-03-04 11:23:03	Waiting	Isolate, Trust, Ignore Big Data Analytics
<input type="checkbox"/>	2	20.10.0.3	Ransom virus	Malicious Files: c:\users\administrator\desktop File Hash: 00BD67CFCCF7141C8FB6C622442B Time Detected: 2021-03-04 11:23:03	Waiting	Isolate, Trust, Ignore Big Data Analytics
<input type="checkbox"/>	3	20.10.0.3	Other viruses	Malicious Files: c:\users\administrator\appdata File Hash: 2B13B58CCBB7F3CE02C9BF957F7F Time Detected: 2021-03-04 11:23:03	Waiting	Isolate, Trust, Ignore Big Data Analytics
<input type="checkbox"/>	4	20.10.0.3	Worm	Malicious Files: - File Hash: 50BE57183774946DADACCD896B2I Time Detected: 2021-03-04 11:23:03	Waiting	Isolate, Trust, Ignore Big Data Analytics

Page 1 of 1 Entries Per Page: 10 1-4 of 4

Close



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