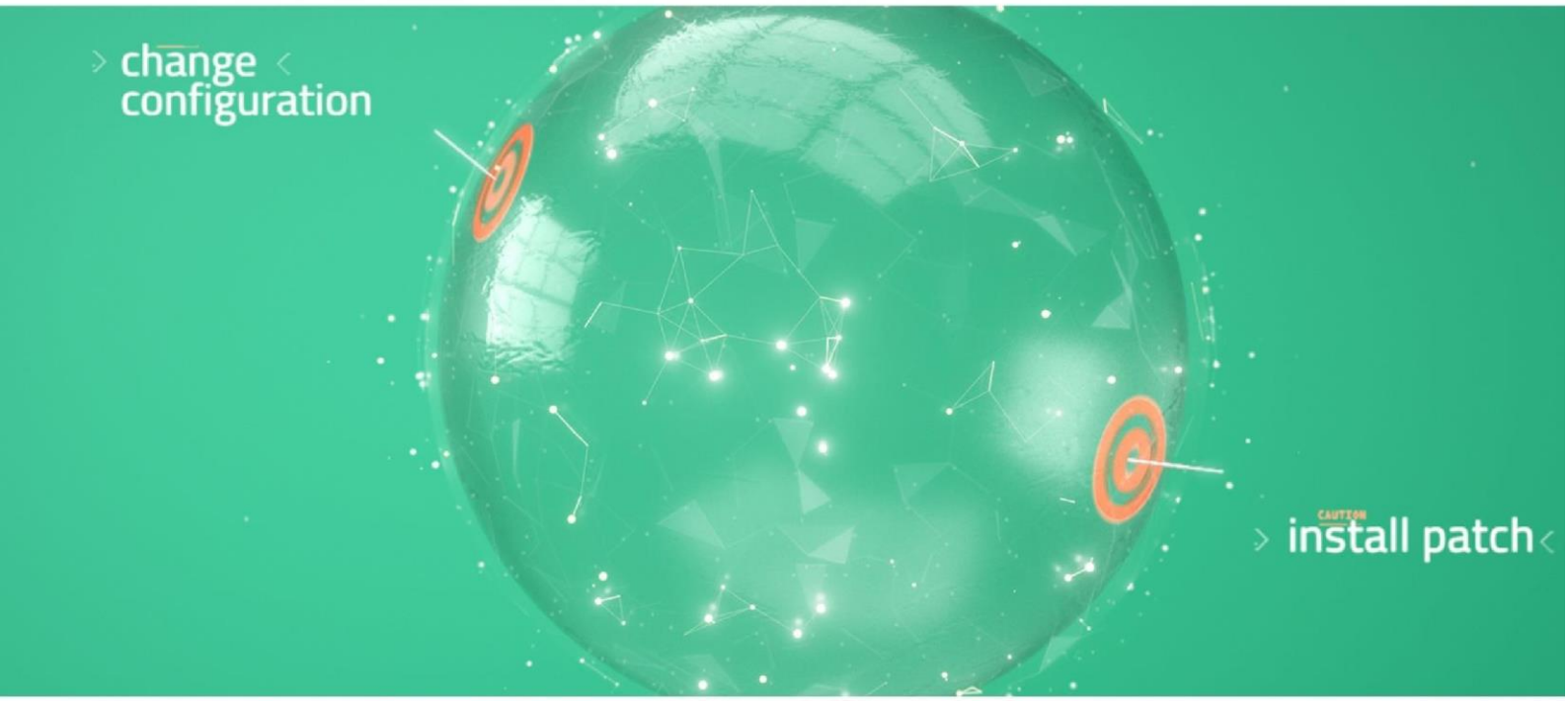
Cymulate



Pre Requirements

Technical Document

7/11/2019

Table of Contents

HOST PRE-REQUIREMENTS

Cymulate Agent software does not add a significant load on the operation system. Therefore, it is suitable to provide adequate resource to run Windows OS.

Criteria	Minimum required	Recommended
Memory	4 GB	4 GB
Disk Space	4 GB	4 GB
Network	One network interface	One network interface
Connection	Physical or logical connection to network segment where Cymulate Agent is deployed	

SUPPORTED SYSTEMS

Operating Systems:

- macOS (10.9 and up)
- Linux (Ubuntu, Debian, CentOS/RHTL, Fedora)
- Windows Vista SP2
- Windows 7 SP1
- Windows 8
- Windows 8
- Windows 10
- Server 2012 and over

Notes:

- On windows systems it is also expected that the operating system has a .NET Framework 4.5.2 or later.
- The platform works best with **Google Chrome** browser.

SUPPORTED MODULES

- Immediate Threats
- Email Gateway
- Web Gateway
- Web Application Firewall
- Phishing Awareness
- Endpoint Security
- Data Exfiltration
- Lateral Movement
- Full Kill-Chain APT

AGENT PRE-REQUIREMENTS

This section describes the Cymulate Agent & Cloud communication requirements.

Cymulate provides each customer with (at least one) set of credentials to login to the web interface (Cymulate Cloud).

Cymulate uses a lightweight agent called Cymulate Agent to test corporate network security and communicate with the Cymulate Cloud.

HTTP COMMUNICATION REQUIREMENTS

HTTPS communication requirements should be fulfilled to manage agents and perform attacks.

*If a firewall resides between agents and Cymulate cloud, the following ports must be opened:

Port	Direction of communication	Description	Sample FW Rule
TCP 443 (HTTPS)	Cymulate Agent **->** Cymulate Cloud	Cymulate Agent register and communicate with Cymulate Cloud over HTTPS protocol	Source: Instance_IP (where agent is installed) Destination: **app.cymulate.com** Port: HTTPS/443

Whitelist the following folders on your endpoint security controls* (Ex: Windows Defender, Antivirus):

Windows OS:

C:\Program Files (x86)\Cymulate\Agent (32-Bit Windows)

C:\Program Files\Cymulate\Agent (64-Bit Windows)

%programdata%\cymulate\Agent (If the agent was installed without Local Administrator privileges)

Mac OS:

Cymulate Agent is required to be installed and run with **root privileges**

/Applications/Cymulate/Agent

/Users/Shared/Cymulate

Linux OS:

Cymulate Agent is required to be installed and run with **root privileges**

$HOME/Cymulate/Agent

ATTACK VECTORS CONFIGURATION

Vector	Requirements	Comments
Email Gateway	Please see Email Gateway requirements	Cymulate email server will send emails with simulated malicious Attachments.
Web Gateway	See HTTP Communication requirements	Cymulate Agent will test inbound and outbound connections from the workstation.
Phishing	Make sure the following IP address is not blacklisted in your email gateway solutions: **52.174.198.166** (*smtp.lionnets.com*)	Cymulate phishing server will send fake emails as part of the generated campaign.

Web Application Firewall	Make sure the following IP is whitelisted / not detected as a bot: **34.241.253.89**	Cymulate attack server will send crafted payloads requests to the WAF protected site.
Endpoint	See HTTP Communication requirements	Cymulate Agent will drop and execute on the workstation a list of simulated malicious scenarios.
Lateral Movement	See HTTP Communication requirements	Cymulate Lateral Movement **(**Hopper) Agent will try to laterally move within the selected network using different protocols and spreading techniques.
Data Exfiltration	See HTTP Communication requirements	Cymulate Data Exfiltration - Agent will try to exfiltrate sentences, keywords or outside the company network using different protocols and exfiltration techniques.

Immediate Threats	Implement Email gateway, Web gateway & Endpoint security requirements listed above.	Cymulate Immediate Threats module will simulate a new "in the wild" threats on three vectors (If applicable) – Email Gateway, Web gateway & Endpoint
Kill Chain APT	Implement Email gateway, Web gateway & Endpoint security requirements listed above.	Cymulate Kill Chain APT module will entire flow of an APT in one go, it may use one or more of the following attack vectors: Email Gateway, Web gateway & Endpoint

**In some cases, the whitelisting is required in an organization level (policy)*

EMAIL GATEWAY REQUIREMENTS

MANDATORY REQUIREMENTS:

1. **Setup a dedicated mailbox under your email domain** (ex. cymulate@example.com)
2. **Configure organizational network filter policy** - make sure the following IP address is not blocked: 168.245.119.24

LINUX / MAC OS:

Configure Mailbox Rule:

1. Mailbox service will require the ability to forward mails to an external party
2. Create a simple inbox rule:
   a. When email is received from: Donotreply@cymulate.com
   b. Forward to: mail@smtp.cymulate.com
   c. Delete email.

WINDOWS OS:

There are two options to configure the email gateway module:

1. **Configure Mailbox Rule:**
   1. Mailbox will require the ability to forward mails to an external party
   2. Create a simple inbox rule:
      a. When email is received from: Donotreply@cymulate.com
      b. Forward to: mail@smtp.cymulate.com
      c. Delete email.

2. **Communication using Outlook API (SMTP):**

Cymulate agent will use Outlook API in order to monitor incoming/outgoing email traffic using Outlook.

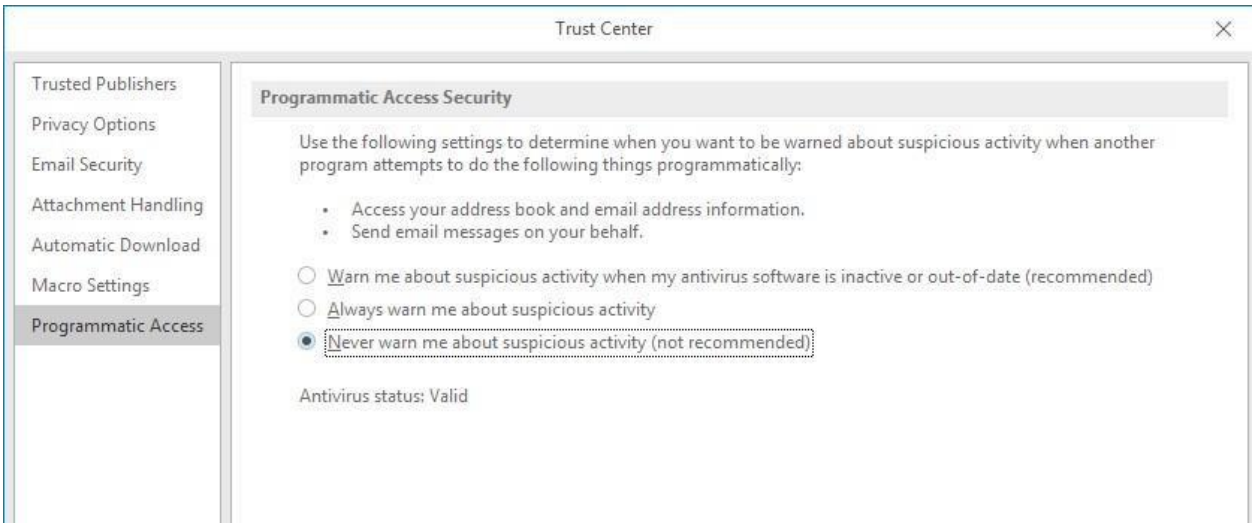
Follow the next steps to enable Cymulate Agent to use Outlook API:

1. Outlook 2010 and above is required
2. Add *cymulate.com* domain to **Safe Senders List** in **Outlook**.

   How Do I Add a Domain to Safe Senders in Outlook?
3. Update **Trust Center** preferences in **Outlook**:
   a. In **Outlook**, click on **File**, and then click on **Options**.
   b. Click on **Trust Center**, and then click on **Trust Center Settings**.

c. Click on **Programmatic Access.**

d. Select the 3rd option - Never warn me about suspicious activity.



Troubleshooting:

1. **Options are not available:**
   exit Outlook, and then start Outlook again in elevated mode. To do this, type Outlook on the desktop or in the Start Search box, right click the Microsoft Outlook search result, click on Properties, click on the Compatibility tab, and then click on Run this program as an administrator.

2. ***Multiple Outlook Profiles:***

In case more than one profile configured in Outlook, please make sure to set as default the profile of the target mailbox.