Cymulate

PoC Requirements 2024

Proof Of Concept 2024 - Requirements

Contents

Cymulate agent requirements

Before running assessments that test your cybersecurity posture, you first need to deploy the Cymulate agent. There are two types of agents currently available:

- **Agent (process-based)** – For Mac and Linux, this is a lightweight agent that communicates with the Cymulate platform. The process-based agent requires a dedicated machine to operate such as a laptop, desktop, or Virtual Machine (VM) and must be logged in to run assessments.
- **Agent (service-based)**– This agent is service-based and has a more scalable and modular architecture. Main benefits of the service-based agent is that the user does not need to be logged in and multiple user profiles can be used to run assessments. Currently available for Windows only.

  To add new user profiles for the agent, Active Directory users must have *Interactive Logon* enabled.

System requirements

Make sure to meet the following system requirements for the agent.

Criteria	Minimum requirement	Recommended
CPU	2 cores	4 cores
Memory (RAM)	8GB	16GB
Free disk space (SSD)	30GB	60GB
Network	One network interface	One network interface

Additional requirements for process-based (Mac and Linux) agents:

1. The user must be logged in to the dedicated machine where the Cymulate agent is installed.
2. The user logged in to the machine with the installed Cymulate agent must have Read, Write, and Delete permissions.
3. If an automated passwords changing policy is being used, the user logged in to the Cymulate agent machine should be excluded from that policy.

Communication requirements

To perform security assessments on a network, it is necessary for the Cymulate Agent to be able to communicate with the Cymulate platform. This communication requires HTTPS and is required for managing agents and performing attacks.

If a firewall is present between the Cymulate agent and the Cymulate platform, certain ports need to be opened either directly or through a proxy to enable the required communication.

Source	Destination	Port	Description
Cymulate agent machine	Cymulate Cloud Domain ***.app.cymulate.com** ***.us-app.cymulate.com**	443 HTTPS	Essential communication between the Cymulate agent and the Cymulate cloud platform.
DLP Evidential Server	***.Cymulatedlp.com**	443 HTTPS	Used to receive exfiltrated data.
Advanced Scenarios	**Cypy.app.cymulate.com**	443 HTTPS	Used to download resources

Supported operating systems

The Cymulate agent is supported for the following operating systems.

OS type	OS	Version	Architecture
Windows	Windows 10 client	1607+	x64
	Windows 11	22000+	x64
	Windows server	2012+	x64
	Windows server core	2012+	x64
	Nano server	1809+	x64
Mac	Mac	10.15+	x64
Linux (legacy agent)	Alpine Linux	3.12+	x64
	CentOS	7+	x64
	Debian	10+	x64
	Fedora	33+	x64
	openSUSE	15+	x64
	Red Hat Enterprise Linux	7+	x64
	SUSE Enterprise Linux (SLES)	12 SP2+	x64
	Ubuntu	16.04, 18.04, 20.04+	x64
	Oracle Linux server	9.3+	x64
Linux (service based agent)	Oracle Linux Server	9.3+	x64
	Ubuntu	20.04+	x64
	Red Hat Enterprise Linux	8.1+	x64

Important Note:

Remember that if your mainly case is Security Control Validation, we must have a baseline computer from your company. You can use for example the same image is deployed to every new employee, it also must include all applications that the users use (Microsoft Office and Adobe for example) also it must include your official Antivirus Solution Installed.

It`s recommended also you have a dedicated domain username account with password (to be inserted in the platform) and a dedicated user mailbox for the PoC. (As this mailbox will receive a lot of samples of malwares it is not recommended you use production ones).

If the company have a proxy, please be sure this computer access the internet though proxy also.

Based on that explanation, please see the following checklist for your PoC Computer:.

Criteria	Minimum requirement
Company Anti-Virus (EPP, ERD) Installed	If one of the use cases is check your Endpoint Security posture please have it.
Proxy Access (If Applicable)	If the company have a proxy, please be sure this computer access the internet though proxy also
Acrobat Reader (If Applicable)	If users usually have Acrobat Reader installed on their computer, install it.
Microsoft Office (If Applicable)	If the company use Microsoft Office, install it
Dedicated Mailbox	If one of the use cases is check your Mail Security posture please have it.
Dedicated Network Username	Malwares behaviors will be simulated with the account logged on the computer. To be sure not to impact any production account, we recommend you to have a dedicated account.

Supported browsers

- Google Chrome
- Microsoft Edge

Windows agent minimum user permissions

To install and run the Windows agent properly, the service account used for the agent must have the following permissions:

- program data read/write access
- program files read/write access
- perform interactive login from users (domain & local)
- run process under a different user profile
- load user profile
- read user token
- impersonate user

Exclusions

The HTTPS/443 traffic between the Cymulate agent and the Cymulate platform should be excluded from any mechanisms such as anti-malware, URL filtering ,etc.

Accounts opened via the Cymulate website are automatically opened in the EU environment regardless of your region. In this case, follow the EU region exclusions.

Testing exclusions

Once the agent is installed, you can test the exclusions by running an agent Diagnostics test. For more information, see Running a Diagnostics test for an agent.

Directory exclusions

Some directories must be excluded/whitelisted for the assessments to run properly. Based on your operating system, exclude the following directories **(and their sub-folders)** on your security controls. Your security controls must also allow downloading encrypted files to these paths.

Windows agents (x64)

- *C:\Program Files\Cymulate\Agent**
- *C:\ProgramData\Cymulate\Agent**

Mac

- */Applications/Cymulate/Agent*
- */Users/Shared/Cymulate/Agent*

Linux

- */usr/lib/Cymulate/Agent/*
- */usr/share/Cymulate/Agent/*

Linux Service based agent

- */usr/local/lib/Cymulate/Agent/**
- */usr/local/share/Cymulate/Agent/*

Cymulate Mac and Linux Agents must be installed and run with root privileges.

Module specific requirements

Email Gateway requirements

During Email Gateway assessments, numerous emails are sent in a short period of time, which can trigger spam filters. To accurately test your organization's security engines, such as anti-virus, sandbox, URL filter, and more, it is necessary to whitelist the Cymulate attack server IP address/domain from your email's anti-spam filtering.

This allows assessment emails sent through the Cymulate SendGrid server to reach the configured mailbox without being mistakenly flagged as spam. This exclusion is essential to ensure an effective evaluation of your organization's email security.

1. Set up a dedicated mailbox under your email domain (ex. cymulate@example.com).
2. Exclude one of the following from anti-spam filtering and Rate Limiting and Throttling policies:
    - **IP address** - 168.245.119.24
    - **Domain** - cymulatemailgateway.com

Supported email platforms

The Cymulate Agent supports multiple communication options with a dedicated mailbox:

- **Microsoft Exchange** - HTTP connection to Microsoft Exchange (Preferred). The agent will prompt for user mailbox credentials and exchange server IP/Hostname address.
- **Office 365**- HTTPS connection via Office 365 API (Preferred).

  Note:

  Hybrid mailboxes are not supported by Microsoft Graph API.

- **GSuite**- There are two available connection options:
    - **IMAP** connection via GSuite.
    - **HTTPS** connection via Gsuite.
        - Service account option. See Configuring the GSuite client for agent SMTP connection.
        - OAuth 2.0 option. See Configuring the GSuite client for HTTPS OAuth2.0 SMTP connection
- **Dynamic IMAP -** The Dynamic IMAP option enables a connection with any email client, including those currently unsupported, or for users preferring dynamic IMAP connections.
- **Outlook client (IMAP and SMTP)** - available for Windows OS only - Connecting to an Outlook application running on the local machine that the Cymulate agent is installed on. The Cymulate agent will use Outlook COM object to monitor incoming /outgoing email traffic using Outlook (Outlook 2013 and above is required).

Please follow the next steps to enable Cymulate Agent to use the Outlook API:

1. Add cymulate.com domain to Safe Senders List in Outlook (How Do I Add a Domain to Safe Senders in Outlook?)
2. In Outlook, go to *File* > *Options.*
3. Click **Trust Center**, and then click **Trust Center Settings**.
4. Click **Programmatic Access**.
5. Select *Never warn me about suspicious activity* and click **OK**.

Web Application Firewall requirements

During WAF assessments, Cymulate sends a high volume of web payloads in a short amount of time which can trigger anti-bot/anti-DDoS mechanisms.

To ensure the assessment accurately tests the resilience of your application's security measures, it is essential to whitelist the specific source IP addresses provided. By excluding these IPs from your WAF's anti-bot/anti-DDoS protection, you enable the assessment to function without interference, allowing for a comprehensive evaluation of your application's defenses against web-based attacks.

***Note**: Be Aware also with other engines that may block Cymulate IPs, as Geolocation Rules, or other Reputation Based rules.*

EU

- 54.217.50.18
- 52.208.202.111
- 52.49.144.209

US

- 54.237.172.129
- 35.169.219.115
- 52.4.48.52

Important note for Imperva users

If you are using **Imperva**, please contact their customer support to disable the Three Strike Rule. This adjustment prevents the source IP from being blocked, yet continues to block WAF violations, ensuring Cymulate assessments run smoothly.

Support Documents for Exclusions:

The below guides provides a general understanding of the whitelisting process on this 3rd party solution.

Cymulate makes **no warranty** to update the information contained herein or for the use of this guide and assumes no responsibility for any errors which may appear in the document.

Cymulate disclaims all liability for any damages arising from the use or misuse of this guide, whether special, indirect, consequential, or compensatory damages, including liability for infringement of any intellectual property rights relating to the use of information in or reliance upon this document.

- Cloudflare - Setting up Exclusions
- F5 WAF - Setting up exclusions

Endpoint Security requirements

Support Documents for Exclusions:

The below guides provides a general understanding of the whitelisting process on this 3rd party solution.

Cymulate makes **no warranty** to update the information contained herein or for the use of this guide and assumes no responsibility for any errors which may appear in the document.

Cymulate disclaims all liability for any damages arising from the use or misuse of this guide, whether special, indirect, consequential, or compensatory damages, including liability for infringement of any intellectual property rights relating to the use of information in or reliance upon this document.

- Cybereason - Setting up Exclusions
- SentinelOne - Setting up Exclusions
- CylancePROTECT - Setting up Exclusions
- Trellix EDR - Setting up Exclusions
- Microsoft Defender - Setting up Exclusions
- CrowdStrike Falcon - Setting up Exclusions
- Cynet – Setting up Exclusions
- Carbon Black Cloud - Setting up Exclusions
- Palo Alto Cortex XDR - Setting up exclusions

Phishing Awareness requirements

To ensure that Phishing Awareness assessments run properly, you should exclude the Cymulate attack server from your email solution's anti-spam/anti-phishing protection. By doing so, phishing emails sent through the Cymulate SendGrid server can reach the target mailboxes without being flagged as spam. This exclusion is necessary for an effective evaluation of your organization's phishing awareness.

Exclude/Whitelist the following from anti-spam or anti-phishing protection:

EU:

- 168.245.71.63.
- support-eu.lionnets.com

US:

- 168.245.71.63.
- support-us.lionnets.com

Hopper requirements

The Hopper module assesses an organization’s privilege management and network segmentation. To ensure this layer of security is tested without being blocked by the EDR, it is necessary to whitelist the following binary hashes **on all machines** in the network:

- **File name**: CymulateLM.exe
  - **MD5**: 7e1c9df044bcafe8e5a4372793985368
  - **SHA-256**: db5f25b745f701d905d5d6f3979f9d4aec2ae22ad8f5bb66c428324b5e25b0a4
  - **SHA-1**: 18076280e739af9c4c8c93ef99e6a20777c80ff5
- **File name:**CymulateLM64.exe
  - **MD5**: 62b9e0dfd0ef2cd88fdcd412523c7d9f
  - **SHA256**: 2a01f07131420d454f9da5742b33e3ec755b4499199269a75fbf1476e18c18c6
  - **SHA1**: 34332fb1cb2035c1f11d15e6765d334588dba836

Whitelist the following binary HASH on the agent machine (machine used as the Hopper starting point):

- **File name:**HopperMaster.dll
  - MD5, SHA1, SHA256 hash values for **HopperMaster.dll** can be found under *Settings* > *Agents* > *Download agent* > *Agent hashes*.

Advanced Scenarios

Whitelist the following URL:

- Cypy.app.cymulate.com