



**AGENT INSTALLATION**  
User Manual

## Table of Contents

1. Definitions.....	3
1.1. Breach+ Agent .....	3
1.2. Cytomate Breach+ .....	3
1.3. Endpoint.....	3
2. Agent Requirements.....	3
2.1. Minimum System Requirements.....	3
1. Windows OS .....	3
2.2. Communication Matrix .....	3
3. Downloading Breach+ Agent.....	3
3.1. Windows OS .....	4
4. Installation.....	5
4.1. Windows OS .....	5
5. Running The Agent.....	7
5.1. Windows OS .....	7
6. Agent Components.....	15
6.1. Dashboard .....	15
6.2. Email Gateway.....	16
6.3. Endpoint.....	17
6.4. Network.....	18
6.5. Integrations .....	19
6.6. Account.....	20
6.7. Authorization Module.....	21

## 1. Definitions

### 1.1. Breach+ Agent

Cytomate relies on a lightweight agent known as the "BreachPlusAgent" to evaluate the security of endpoints. Throughout this section, unless otherwise specified, we will refer to this agent as simply the "Agent."

### 1.2. Cytomate Breach+

Cytomate Breach+ is a Breach and Attack Simulation (BAS) solution that emulates, assesses, and validates the most recent attack tactics used by Advanced Persistent Threats (APTs) and other hostile groups. Breach+ goes beyond conventional security measures, rigorously validating your organization's defenses across 6 diverse attack vectors. Offering comprehensive insight into potential threats, Breach+ explores uncharted territories, uncovering vulnerabilities in numerous unknown attack paths. By exposing these security holes, Breach+ provides valuable insights to strengthen your organization's defenses.

### 1.3. Endpoint

The devices or machines on which the Breach+ Agent is installed and actively run test cases. The agent provides continuous evaluation of the security status of each endpoint, generating alerts and notifications when any security risks are detected.

## 2. Agent Requirements

### 2.1. Minimum System Requirements

#### 1. Windows OS

- RAM: 8GB
- Windows Versions: 10, 11
- Storage: 50GB

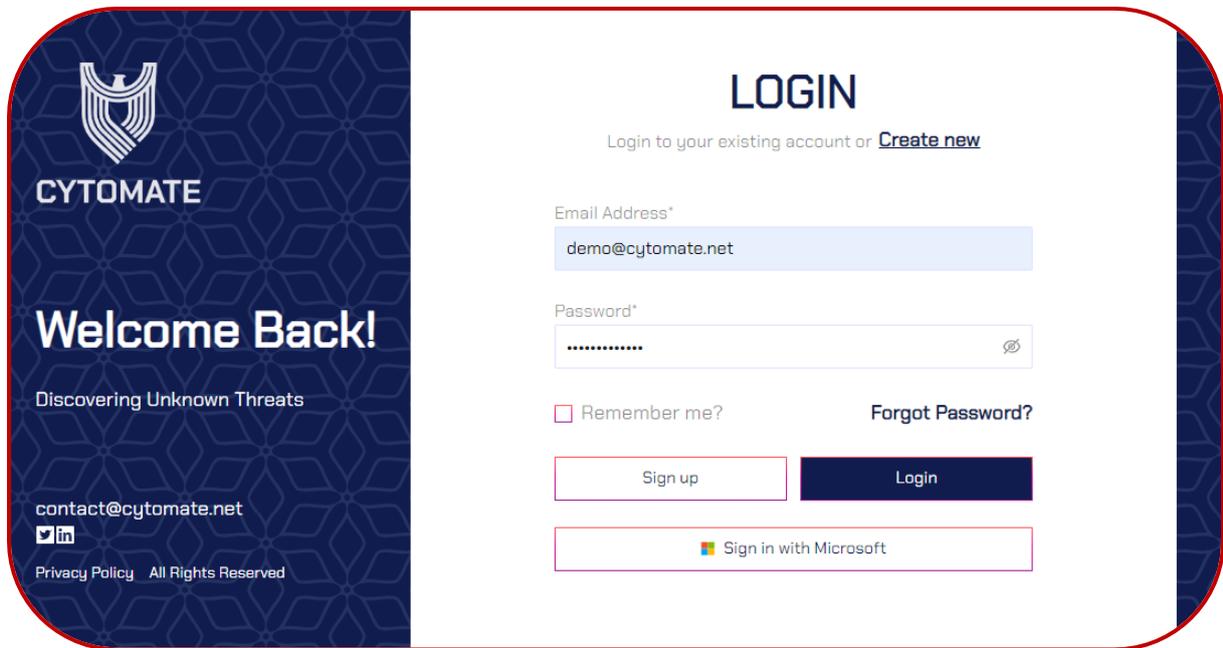
### 2.2. Communication Matrix

*Table 1 Communication matrix for the endpoint machine where agent is to be installed.*

Source	Destination	Port	Protocol
Endpoint VM(s)	apt-api.cytomate.net	443	TCP
Endpoint VM(s)	endpoint.cytomate.net	443	TCP
Endpoint VM(s)	c2.cytomate.net	ANY	ANY
Endpoint VM(s)	c3.cytomate.net	ANY	ANY

## 3. Downloading Breach+ Agent

- 1) The Breach+ agent can be downloaded directly from the Cytomate Breach+ portal:
  - i. Open <https://apt.cytomate.net/> (Use Google Chrome for the best experience.)
  - ii. Enter your credentials and click **Login**.

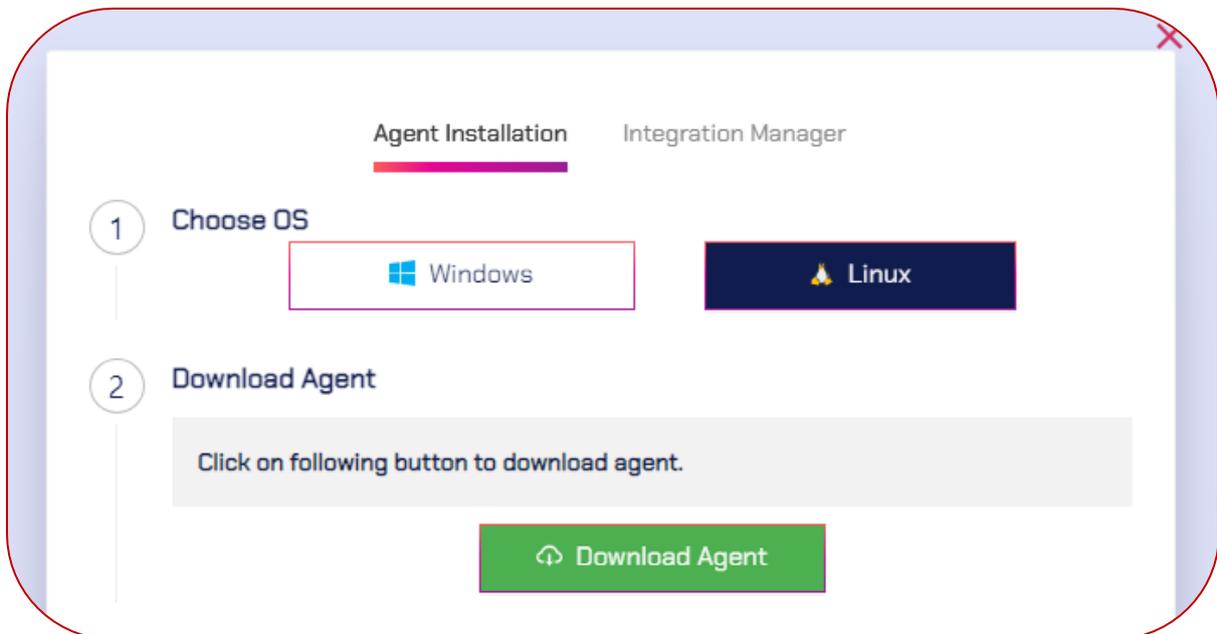


- 2) After a successful login, click on the "**Agent**" icon appearing on the top right side of the screen.



### 3.1.Windows OS

- 1) Select Windows agent, and then click on the "**Download Agent**" button.



- 2) The agent download process will begin, but you may encounter Downloads, File Warnings that could impede the process.
  - To complete the download, right-click on the Downloads document and select "**Keep**" from the menu.
  - Additionally, click on the "Show more" option of "**Make sure you trust Cytomate-BreachPlus-Setup.exe before you open it,**" and select "**Keep anyway**" again from the menu.
- 3) Navigate to your downloads folder to verify that the agent is downloaded.

Name	Date modified	Type	Size
▾ Today 📁 Cytomate-BreachPlus-Setup.exe	1/26/2024 3:01 PM	Application	102,033 KB

## 4. Installation

### 4.1. Windows OS

- 1) Once the agent has been downloaded successfully, you can begin the installation process by either double-clicking on the agent file or right-clicking and selecting the "Open" option.
- 2) To complete the installation process, keep following the setup wizard.

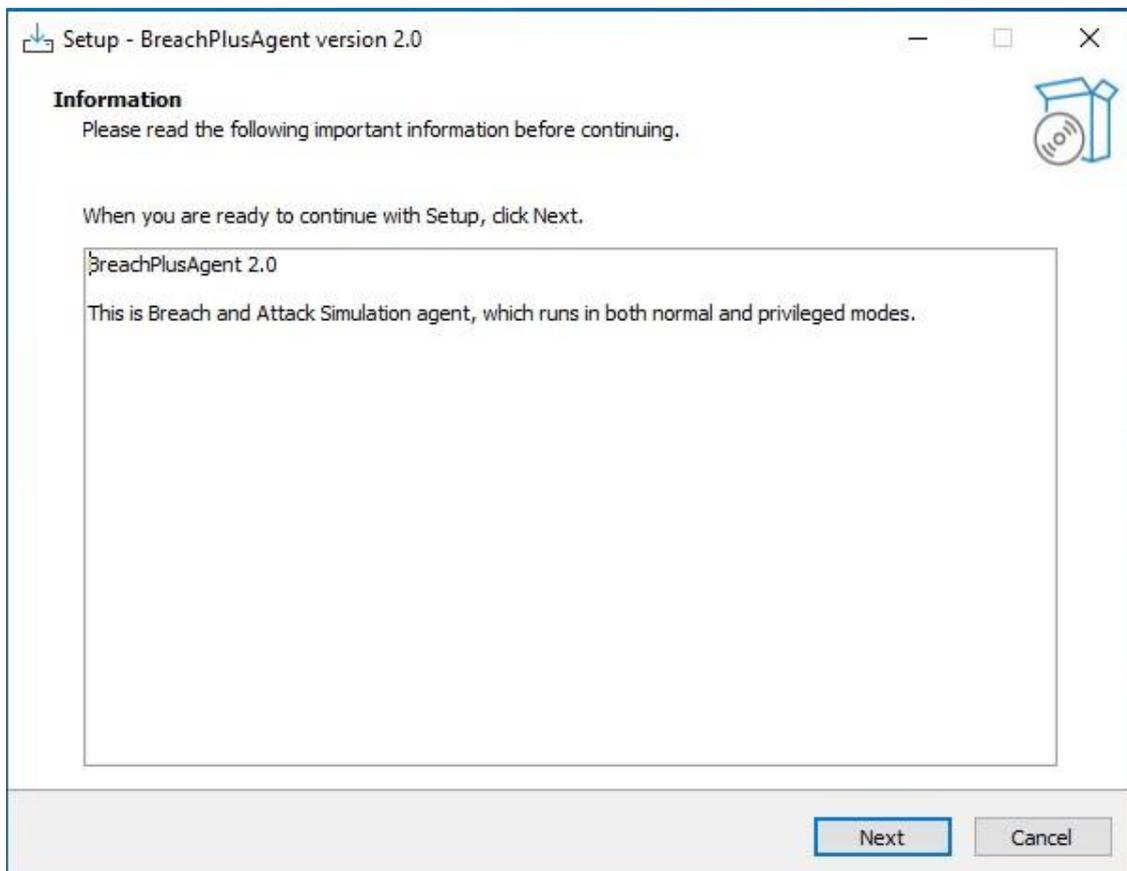
---

During installation, the following folder will be created:

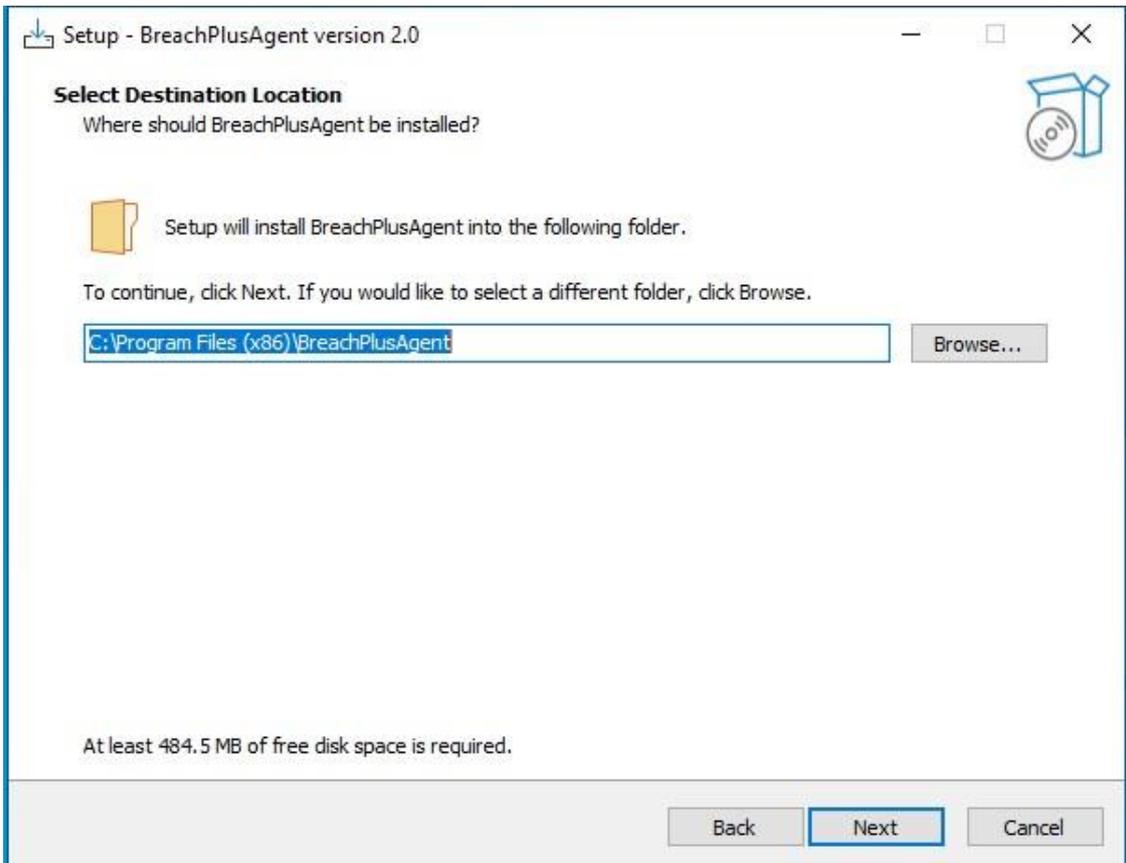
*C:\Program Files (x86)\BreachPlusAgent (64-Bit Windows)*

---

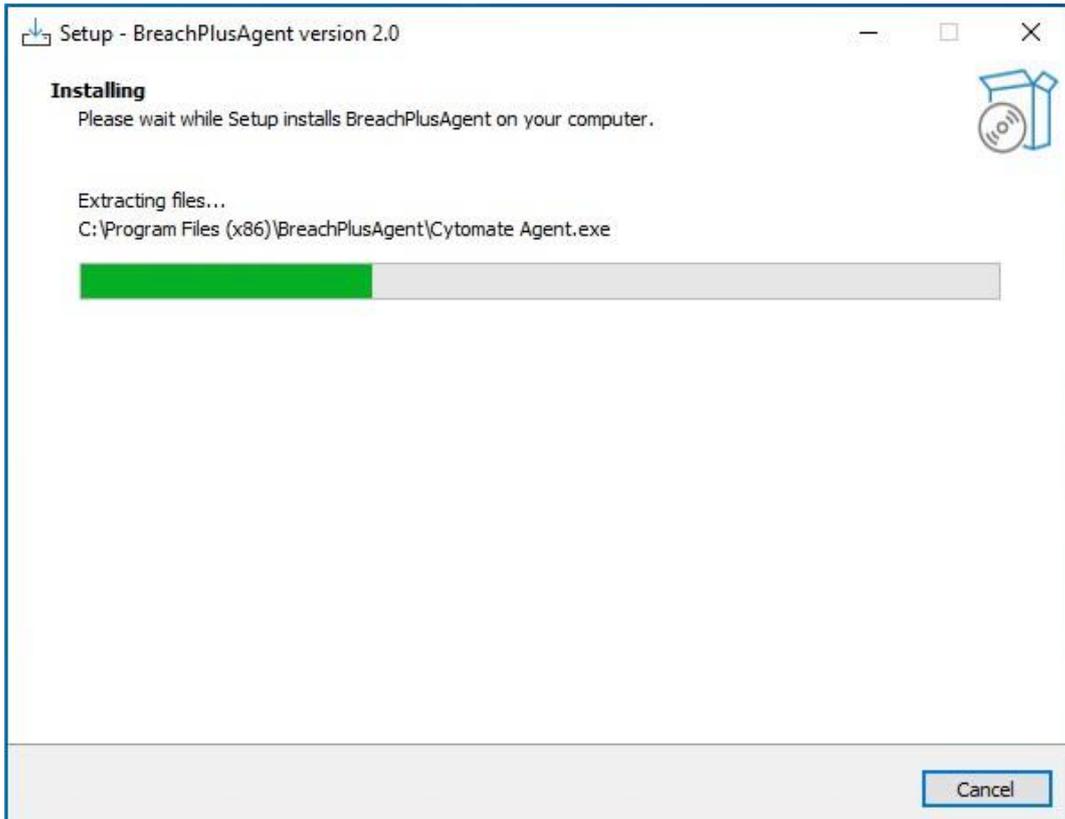
- i. Upon initiating the agent by double-clicking or opening it, a wizard interface will be displayed, presenting essential information. It is noteworthy that this agent is designed to function in both normal mode and privileged mode, providing flexibility in its operational capabilities.



- 3) Click **Next**
- 4) On the next wizard, you will be prompted to select a desired location where you want to install the Agent.

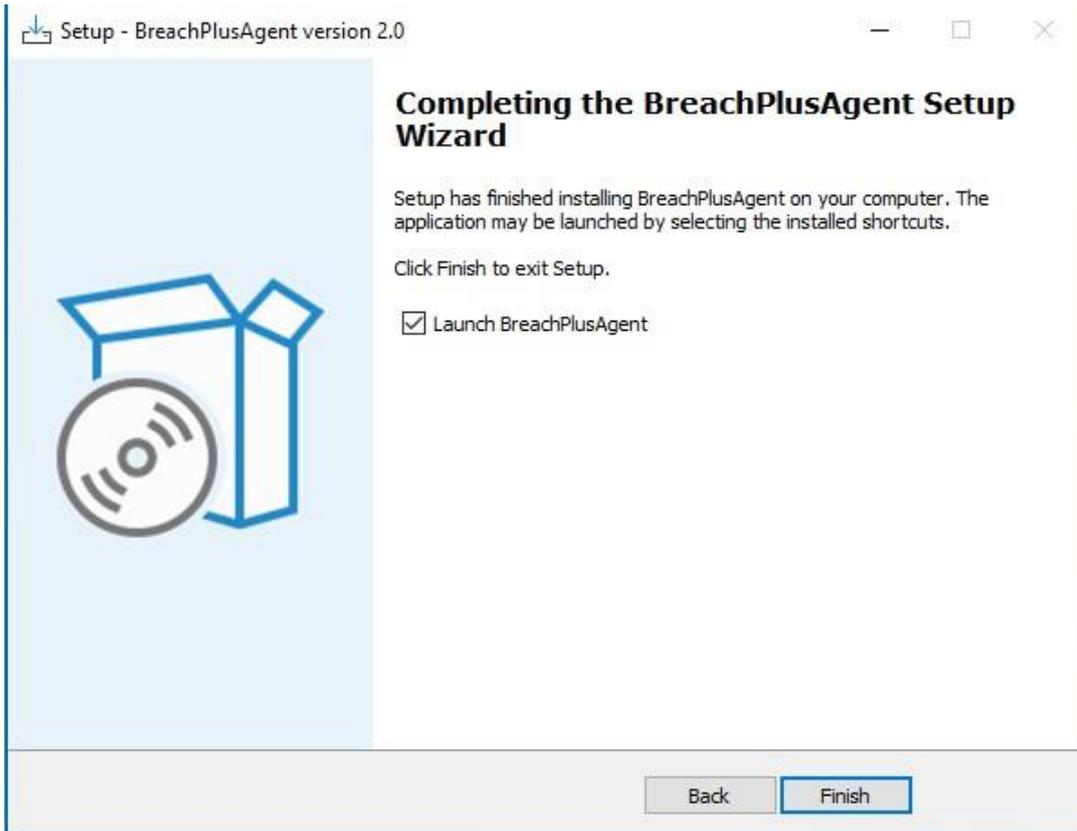


5) Upon clicking "Next," the installation process for the agent will commence.

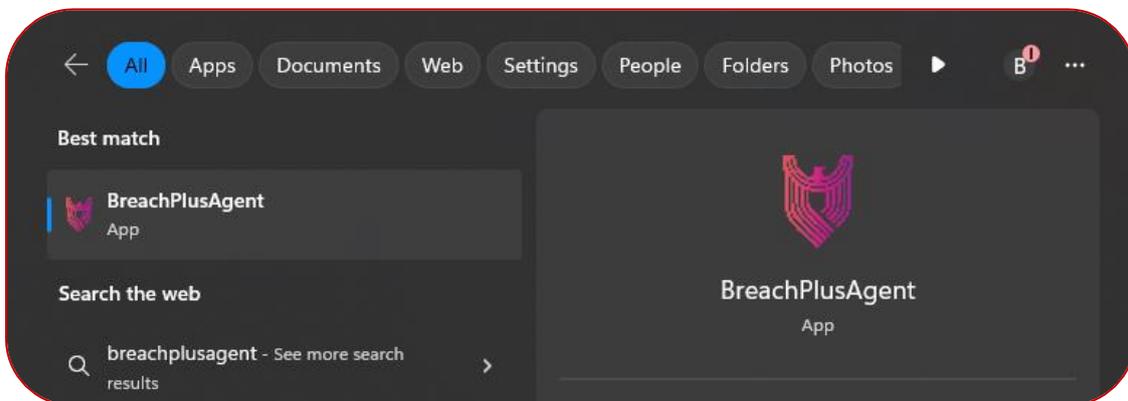




- 6) Following the installation, a final wizard will appear, indicating the completion of the **BreachPlusAgent** setup on your system.



- 7) To complete the installation process, click on the "**Finish**" button.
- 8) To check if installation was successful, follow these steps:
  - i. Search for "**BreachPlusAgent**" in Windows applications.
  - ii. Look for a new shortcut named "**BreachPlusAgent**" on your desktop.
- 9) If you find the Agent in either of these cases, the installation was successful, and the agent has been installed on your system.

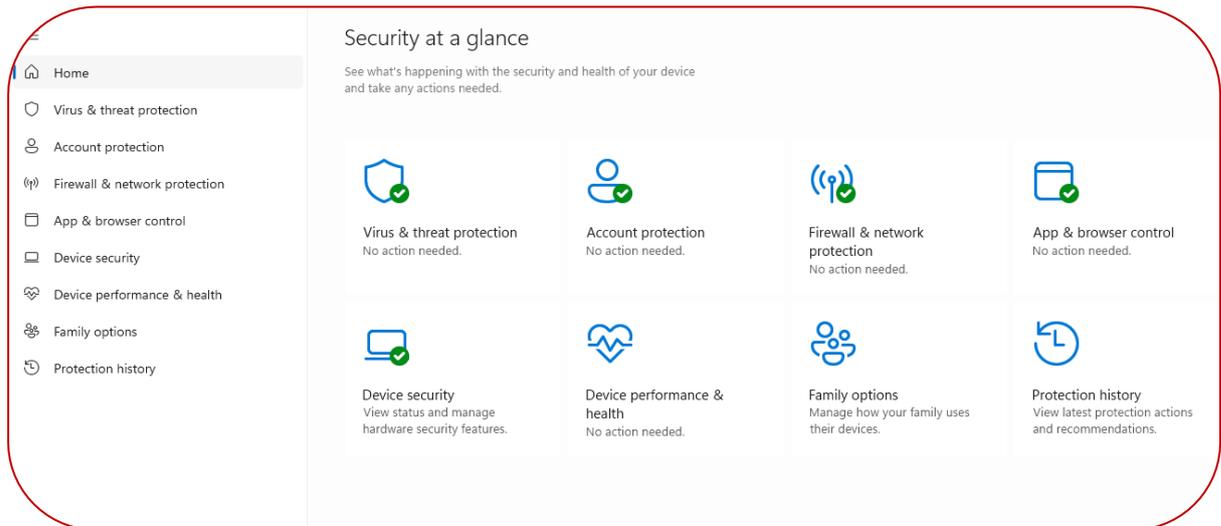


## 5. Running The Agent

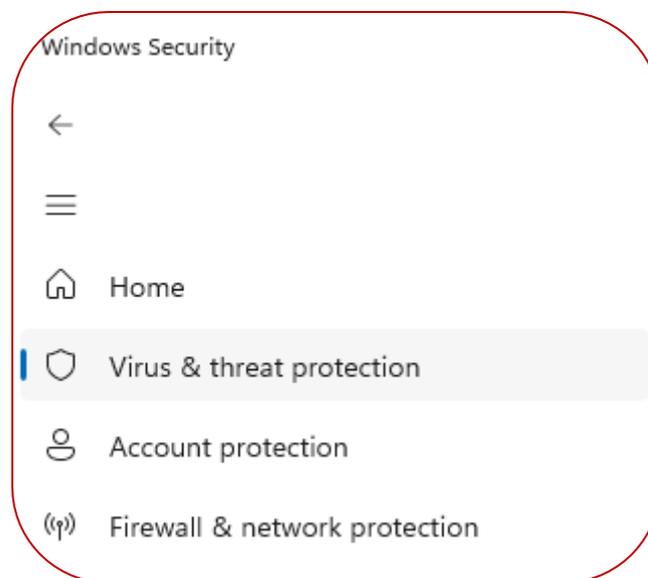
### 5.1.Windows OS

- 1) To ensure proper functionality of the agent, whitelist the folder where the agent is installed on the C-drive before starting it. Follow these steps to whitelist the folder:

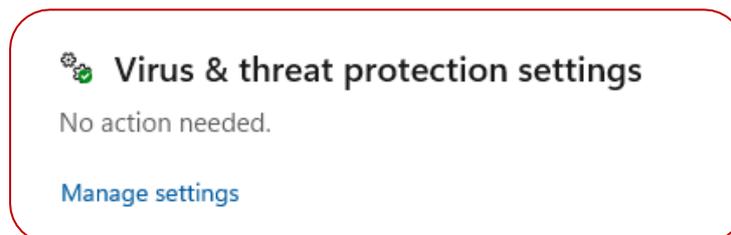
- i. Open Windows Defender, Windows Security, or any other antivirus or EDR solution (these steps are based on Windows Defender antivirus; yours may vary based on the AV and EDR).



- ii. From side menu open **“Virus & threat protection”**



- iii. From the displayed options, select **“Manage settings”** under **“Virus & threat protection settings.”** It will open Virus & threat protection settings.



- iv. From the displayed options, select **“Add or remove exclusions”** under **“Exclusions.”**

### Exclusions

Microsoft Defender Antivirus won't scan items that have been excluded. Excluded items could contain threats that make your device vulnerable.

[Add or remove exclusions](#)

- v. On clicking, “**User Access Control**” will prompt you to either allow this app to make changes to your device or not.
  - i. Click on **Yes**



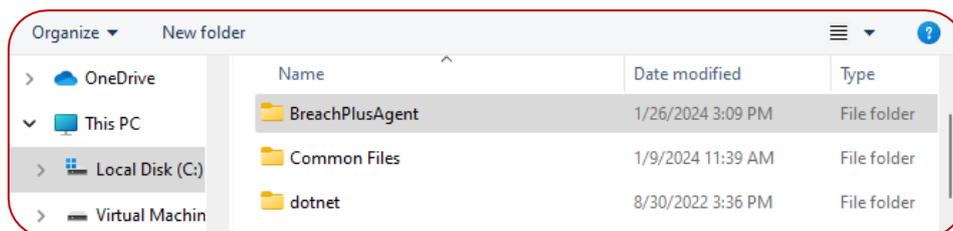
- vi. From the next window, you can select the folders (exclusion) that you want to allow (here, you will select the BreachPlusAgent folder in C-drive).

### Exclusions

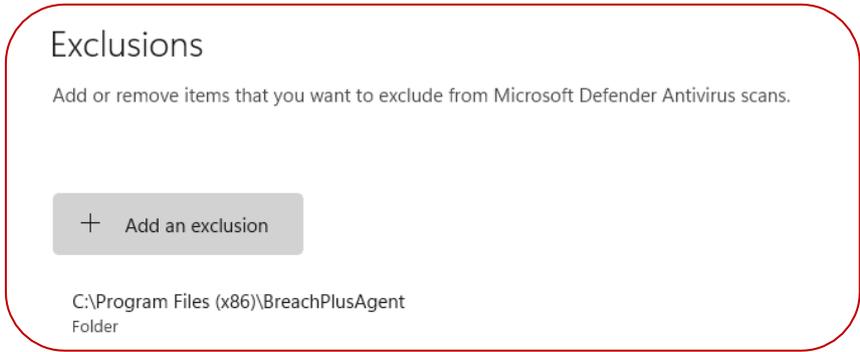
Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

+ Add an exclusion

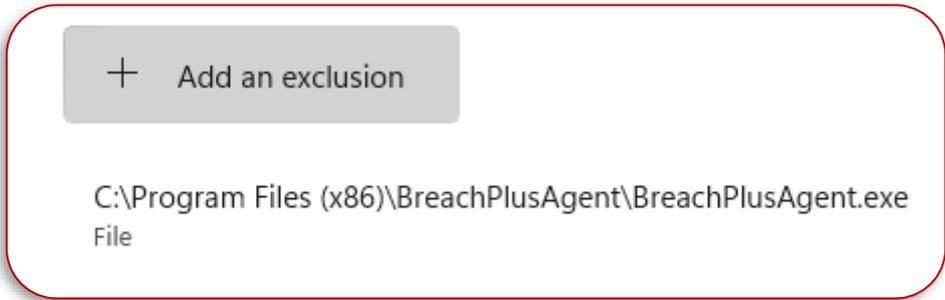
- vii. Click on the “+ **Add an exclusion**” button, select the “**BreachPlusAgent**” folder from path **C:\Program Files (x86)**, and click on the “**Select Folder**” button at the bottom of the window.



- viii. The “**BreachPlusAgent**” folder will be added to the protected folders list.



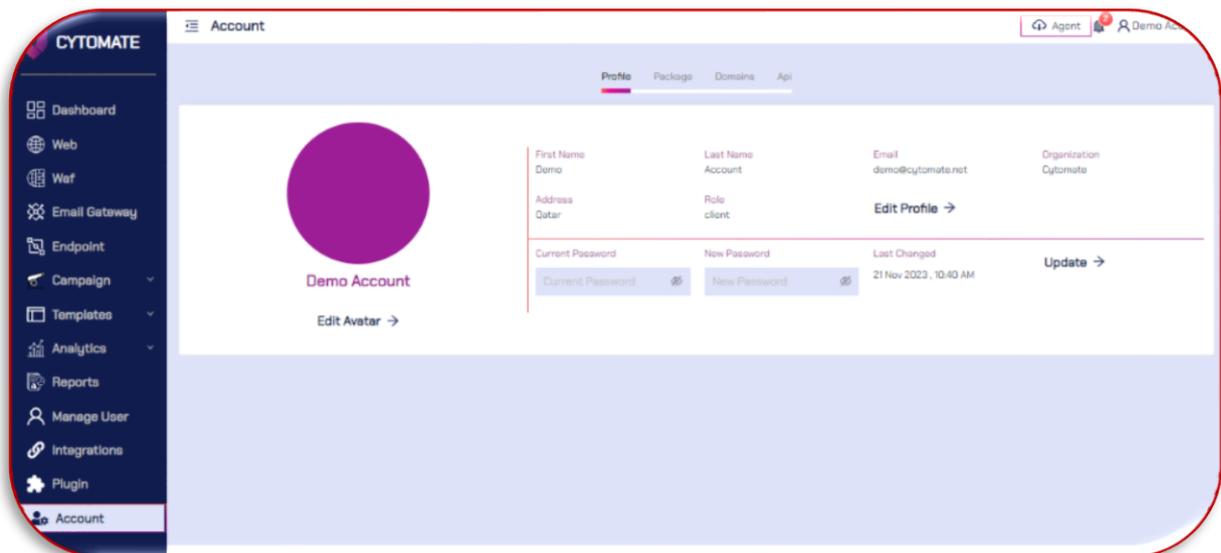
- ix. Click on the “+ Add an exclusion” button again, select the “Cytomate Agent.exe” file from path “C:\Program Files (x86)\BreachPlusAgent\BreachPlusAgent.exe”, and click on the “Select File” button at the bottom of the window.



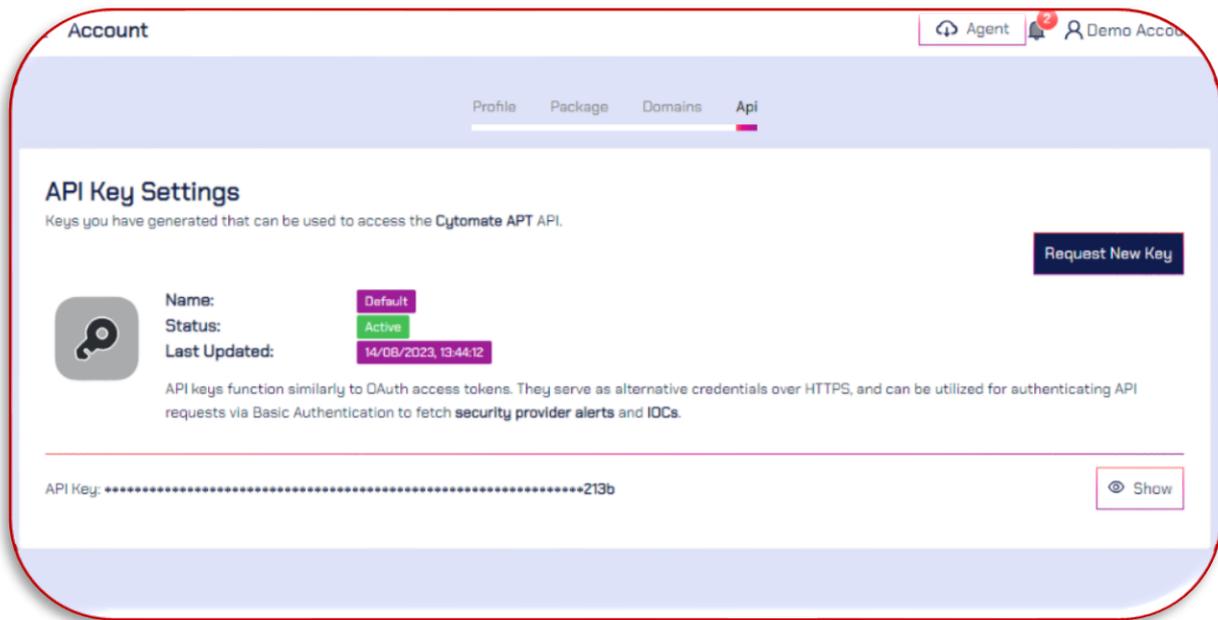
- 2) Upon double-clicking or opening the agent, a login form will be displayed, requiring you to provide your API key for a successful login.



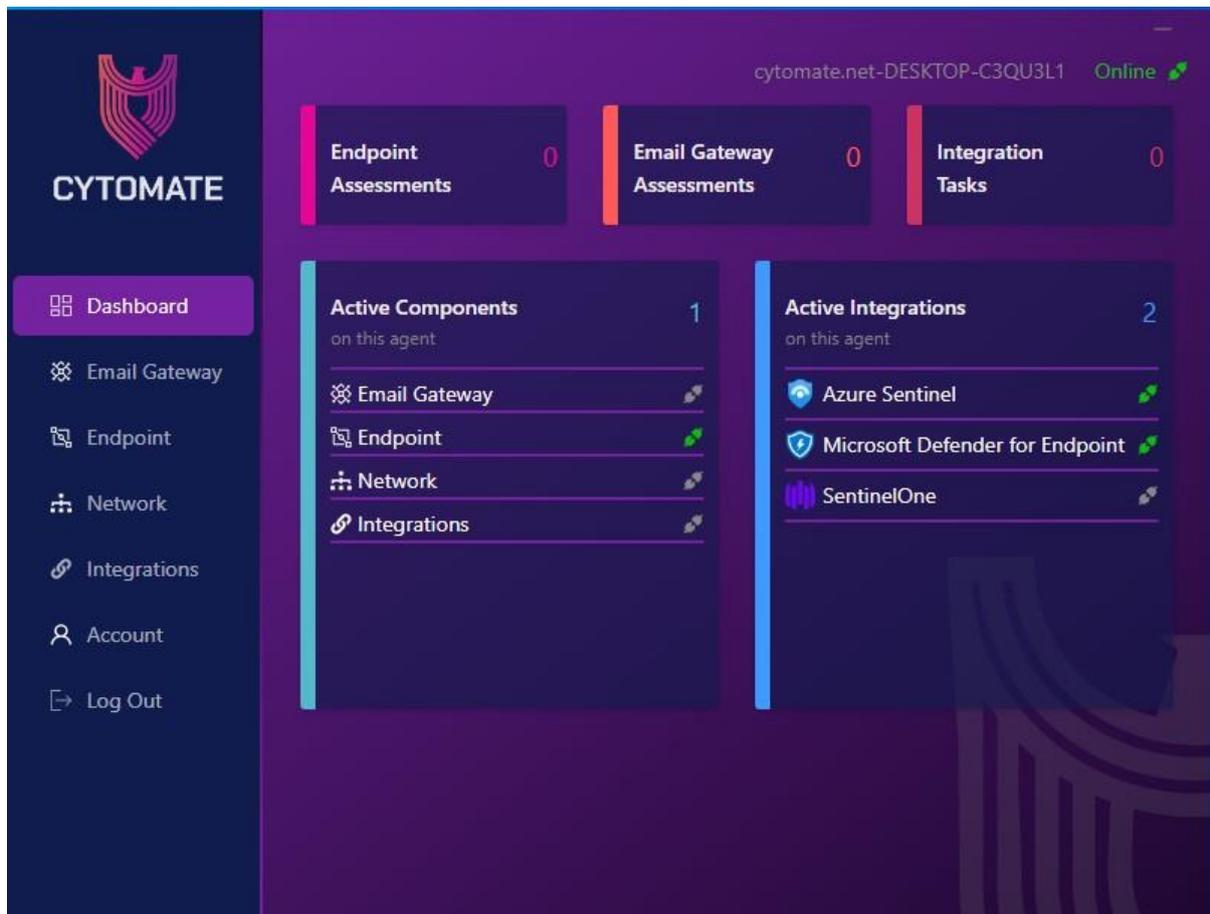
- i. To locate your API key for agent login, navigate to the "Accounts" section on <https://apt.cytomate.net/>.



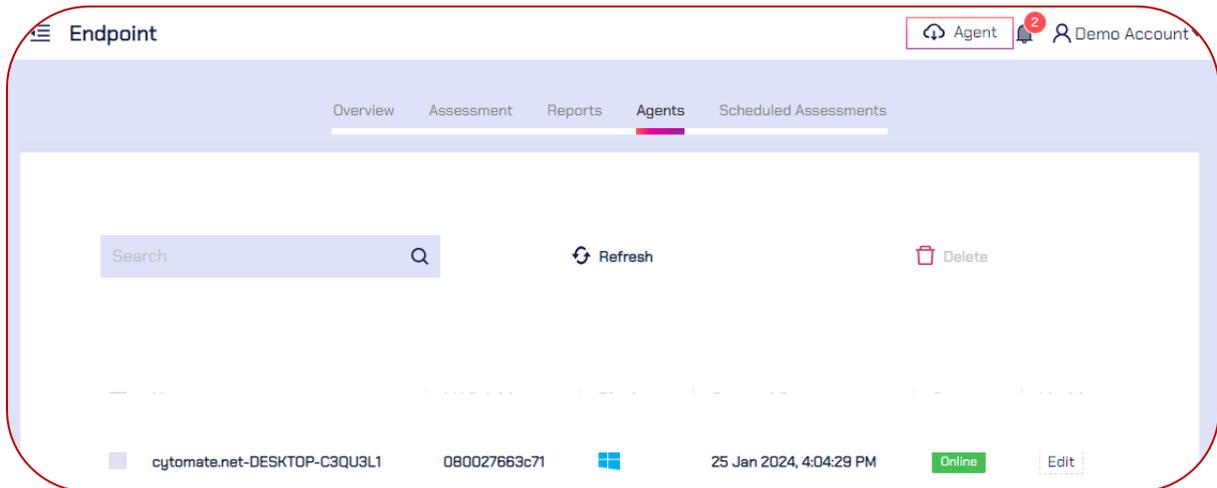
- ii. Within the "**Accounts**" page, you will find four options; choose the "**API**" option. Scroll to the bottom of the page, where you will find the API key. Click on "**Show**" to reveal the API key, and subsequently, copy this key. Paste the copied API key into the login page of your agent to complete the authentication process.



- 3) Upon successful login, the agent will present an interactive dashboard, offering comprehensive information related to the services you are utilizing. This dashboard serves as a centralized hub, providing real-time insights and updates on various aspects of the services, enhancing user engagement, and facilitating effective management of the associated functionalities.

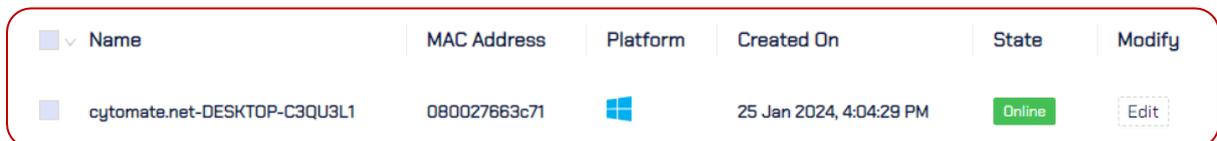


- 4) Now, if you go to account on <https://apt.cytomate.net> and click on **Endpoint** from the side menu, and then select the **Agents** tab, you will see all agents in your use.

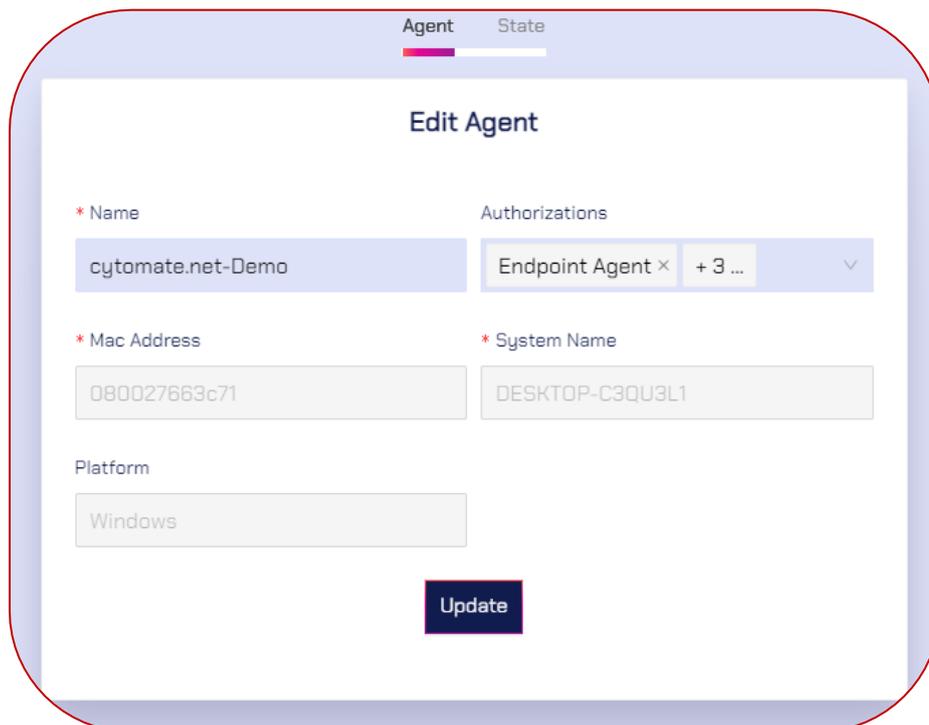


This means your agent has been successfully connected to your account and is ready for use.

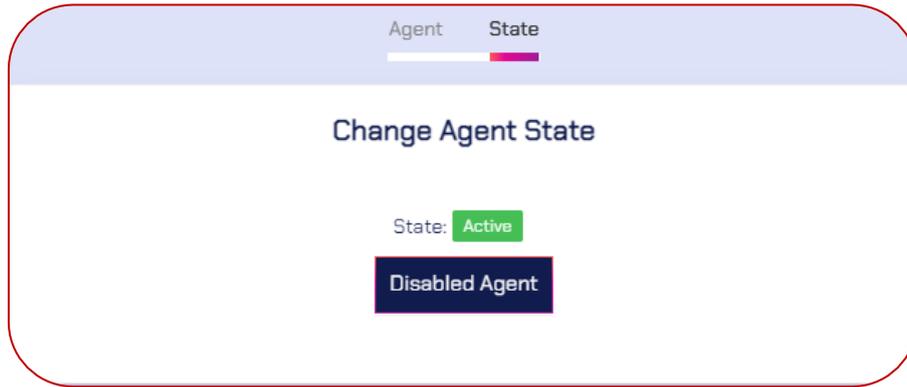
- 5) If you wish to rename the agent, navigate to “**Endpoint**” from the side menu and select the “**Agents**” tab.
- i. From the list of agents, select the one you want to rename and click on the “**Edit**” button.



- ii. A pop-up window will appear where you can change the name. Click on the Update button to apply the changes.



- iii. The state of the agent can be verified through the "State" tab under the "Edit" option. Additionally, you have the capability to disable the agent by selecting the "Disabled Agent" button.



- 6) Finally, the updated agent name will be visible under the “Agents” tab and on the agent itself.

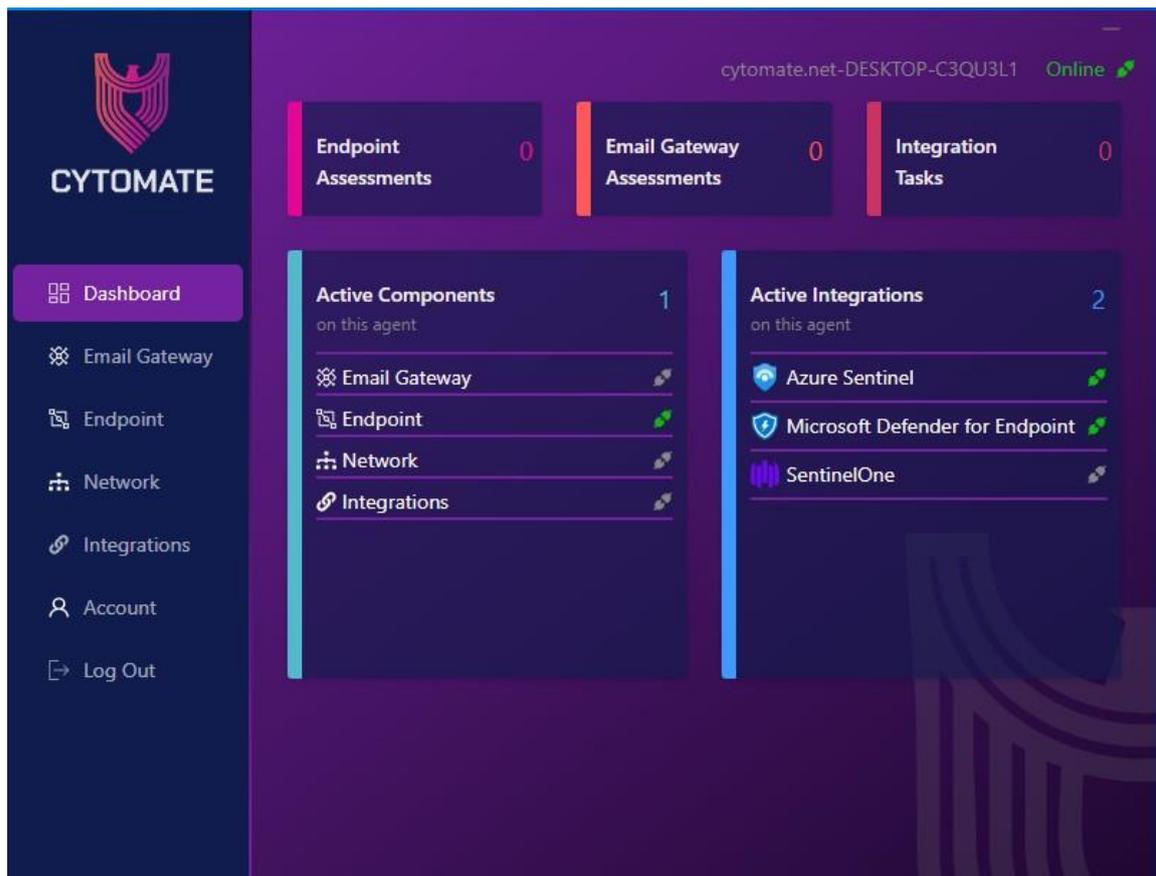
Name	MAC Address	Platform	Created On	State	Modify
cytomate.net-Demo	080027663c71		25 Jan 2024, 4:04:29 PM	Online	Edit

## 6. Agent Components

During our discussion, we will systematically explore each module of the agent, delving into detailed descriptions of their functionalities. Additionally, step by step configurations, if required, will be provided for module to ensure a thorough understanding and seamless integration of the agent's features.

### 6.1. Dashboard

The agent will present an interactive dashboard, offering comprehensive information related to the services you are utilizing. The dashboard provides numerical assessments of your endpoint and email gateway, offering a quick overview of their statuses. Furthermore, it highlights active integrations, showcasing the modules you've activated for use, along with details on the active components. This comprehensive display ensures a holistic view of your system's status and integrations.



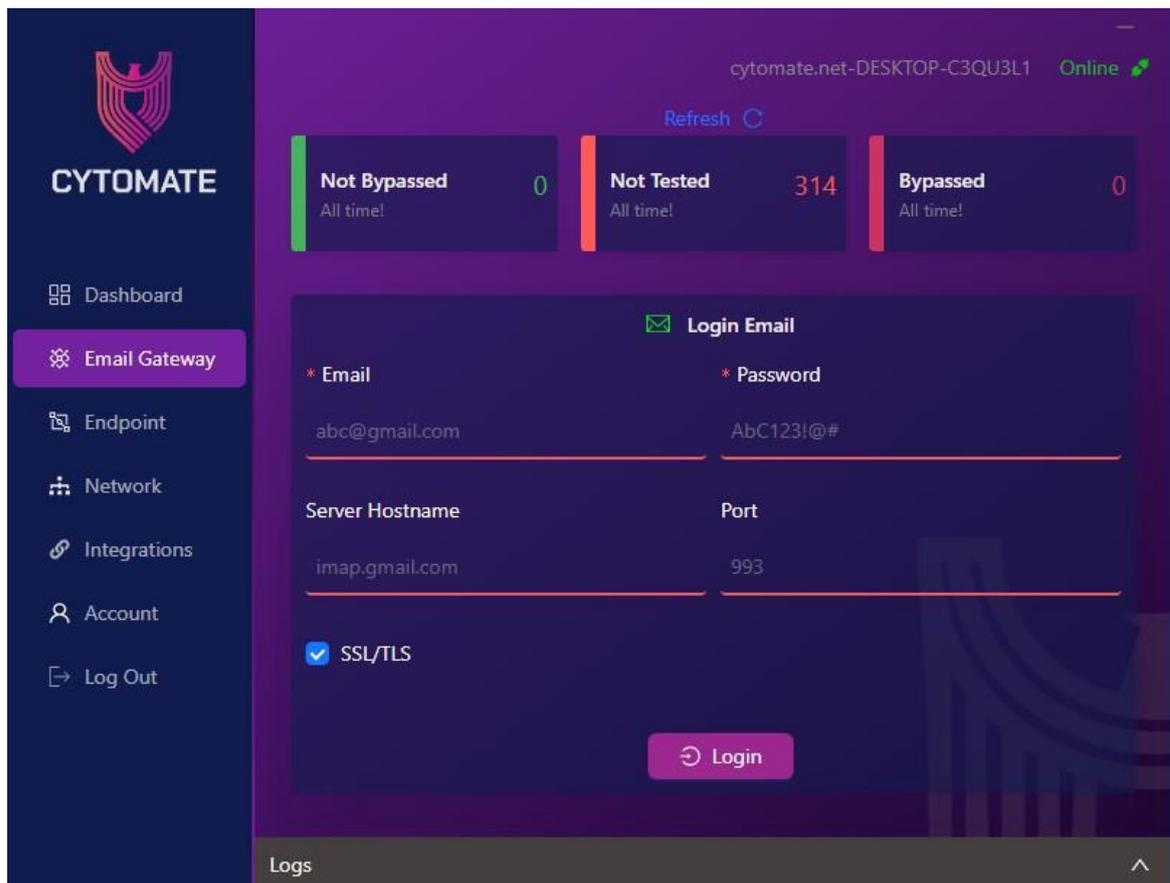
## 6.2. Email Gateway

To access the email gateway component, you must integrate the agent with your email gateway through the login process. A successful login requires the addition of your organization:

- Email
- Password
- Server Hostname (Optional but required in some scenarios)
- Port

Once successfully logged in, the Breach+ agent automatically establishes a connection with the client's email server using the IMAP protocol. Subsequently, it retrieves emails from the inbox and checks for the presence of specific extensions. This automated process ensures a seamless assessment of the email content for enhanced security measures.

On the email gateway user interface, it will also provide information about the email gateway exploits which is not tested. also tells how many exploits successfully bypassed your email gateway defenses and how many were effectively blocked.



cytomate.net-DESKTOP-C3QU3L1 Online

Refresh

Not Bypassed All time!	0	Not Tested All time!	314	Bypassed All time!	0
---------------------------	---	-------------------------	-----	-----------------------	---

### Login Email

\* Email: abc@gmail.com

\* Password: AbC123!@#

Server Hostname: imap.gmail.com

Port: 993

SSL/TLS

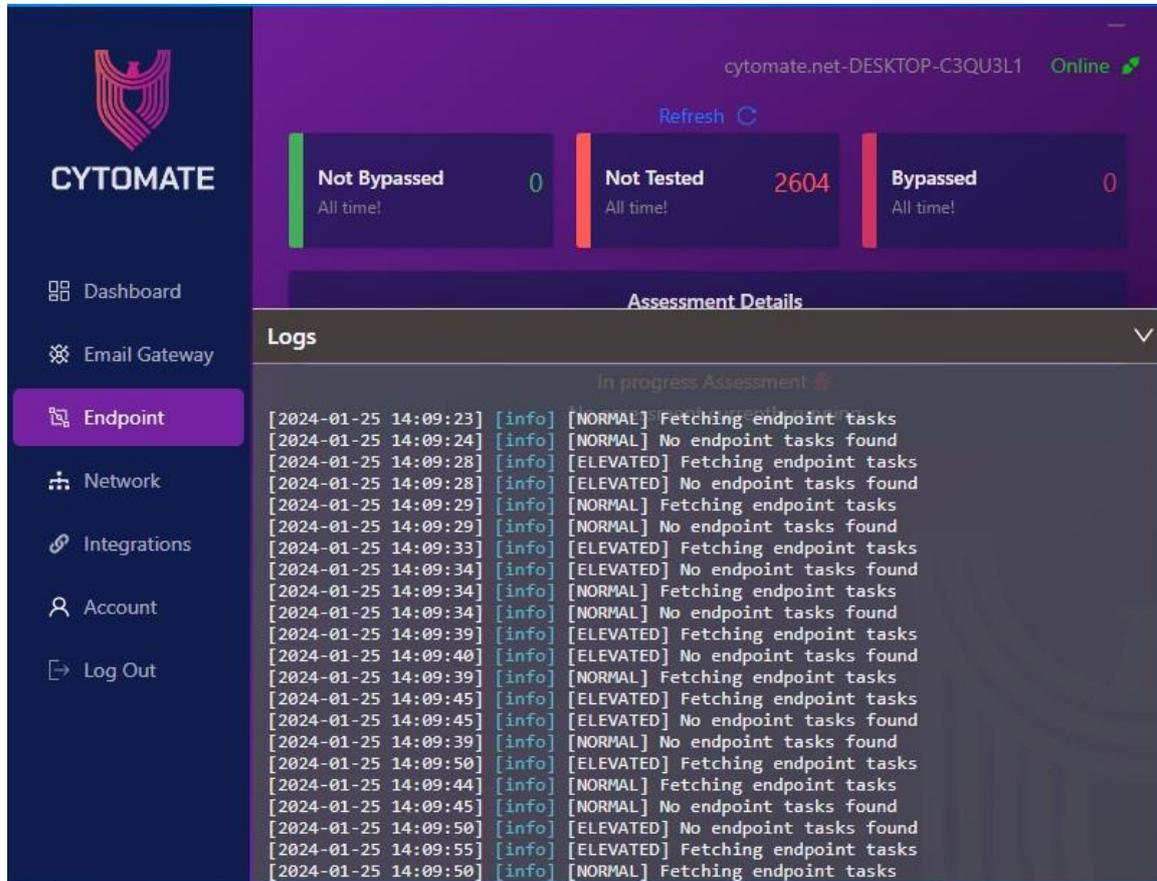
Login

Logs

### 6.3.Endpoint

Within the endpoint component of the Breach+ agent, it has the capability to capture comprehensive logs detailing endpoint assessments. These logs include the initiation date and time of the assessment, the severity level assigned to each assessment, and specific details outlining the assessment findings. This logging feature provides a valuable record of assessment activities, aiding in the analysis and understanding of the security posture of the endpoint.

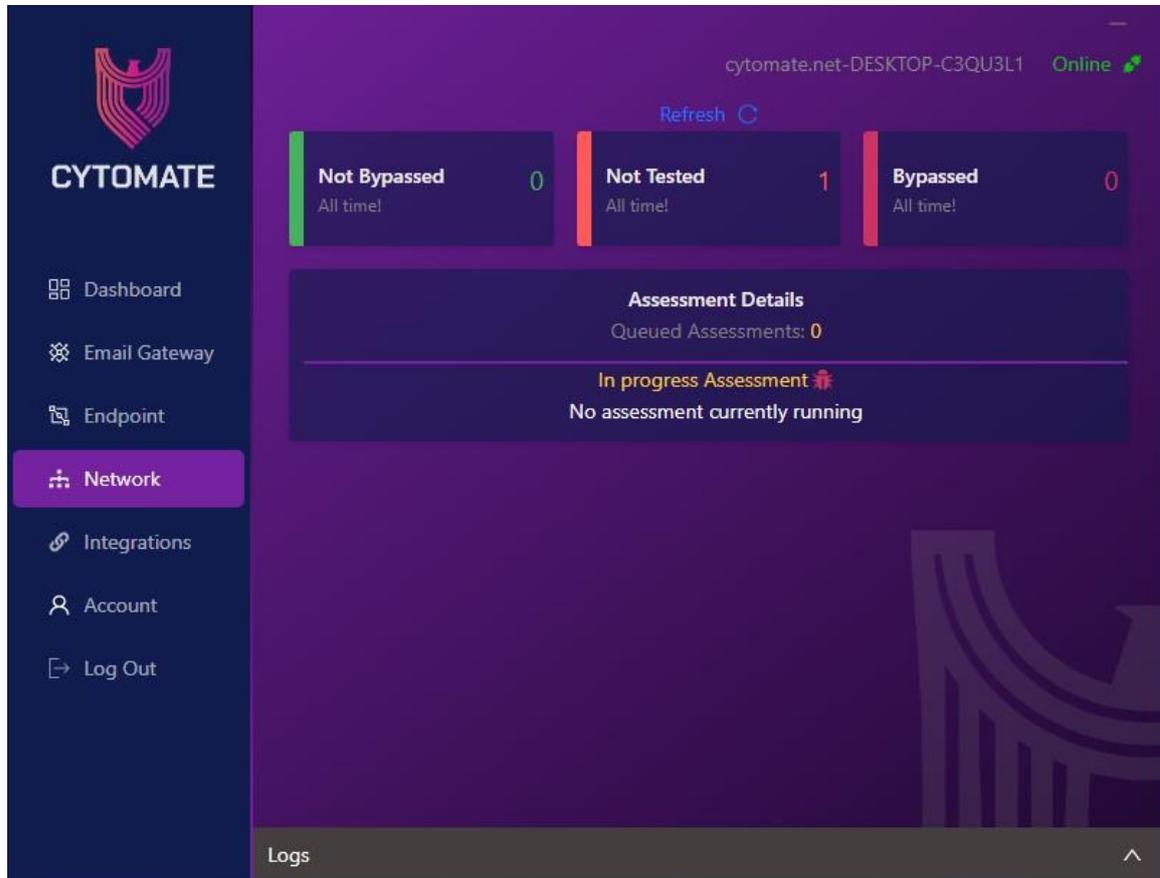
The agent's user interface will furnish details on endpoint exploits that have not been tested, alongside information on how many exploits successfully evaded your endpoint defenses and how many were effectively blocked.



The screenshot displays the CYTOMATE dashboard interface. On the left is a navigation sidebar with options: Dashboard, Email Gateway, Endpoint (highlighted), Network, Integrations, Account, and Log Out. The main content area shows the user's session as 'cytomate.net-DESKTOP-C3QU3L1' and 'Online'. Three summary cards are visible: 'Not Bypassed' (0), 'Not Tested' (2604), and 'Bypassed' (0). Below these is a 'Logs' section titled 'Assessment Details' with a dropdown arrow. The logs are filtered by 'In progress Assessment' and show a series of entries with timestamps, severity levels, and messages such as '[info] [NORMAL] Fetching endpoint tasks' and '[info] [ELEVATED] No endpoint tasks found'.

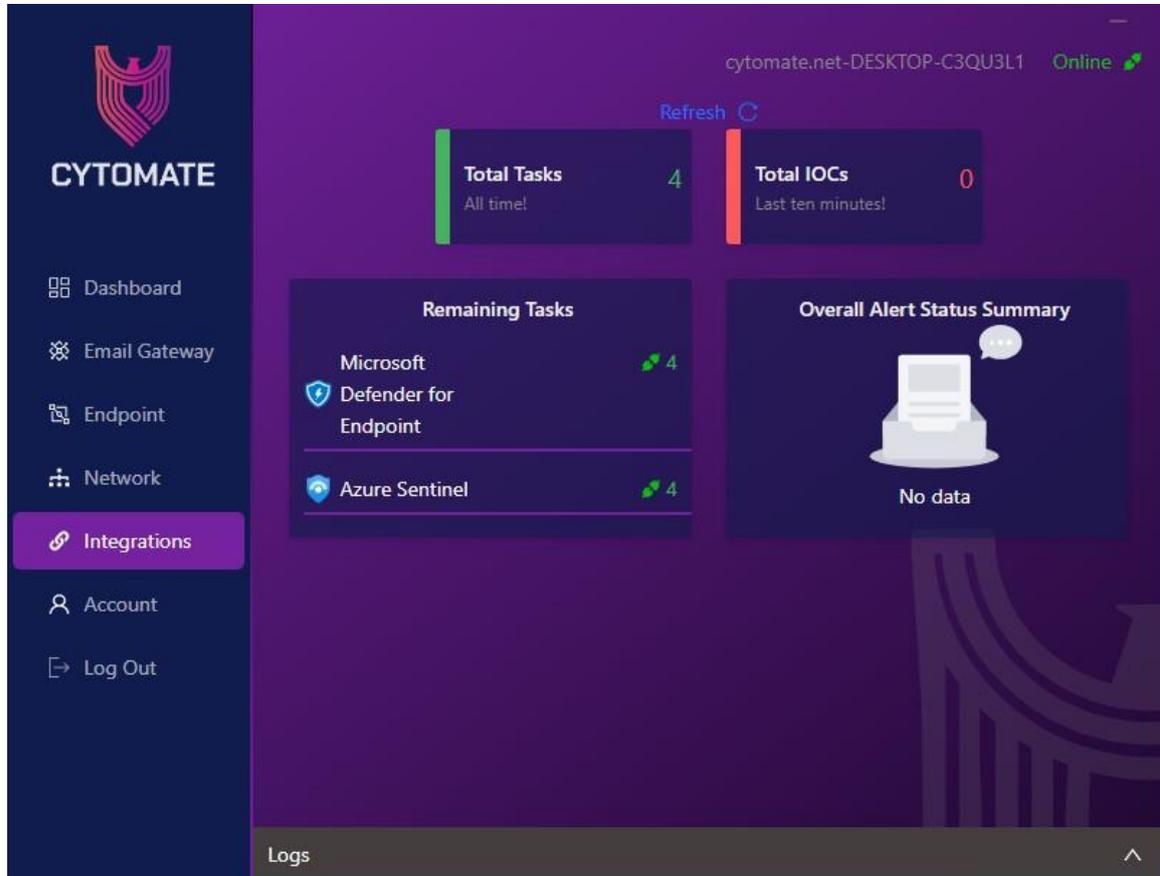
## 6.4. Network

In the network component, the user interface will provide concise details about your network assessment. It includes information on the number of assessments currently in progress and those that have been completed. Additionally, it will display the count of tested exploits and distinguish how many successfully bypassed security controls and how many were effectively blocked. This overview enhances your understanding of the ongoing network security status and the performance of your security controls.



## 6.5. Integrations

In the integration component, the Breach+ agent provides a valuable feature allowing you to integrate with Azure Sentinel or Microsoft Defender for Endpoints. Within this integration, the total number of tasks involves the execution of exploits. Upon successful execution, user can observe alerts generated by these integrations. Furthermore, the overall alert status summary will detail the number of exploits prevented, detected, and those that went undetected. This integration capability enhances your security controls, providing a seamless connection with these Microsoft services for a more robust and comprehensive cybersecurity infrastructure.

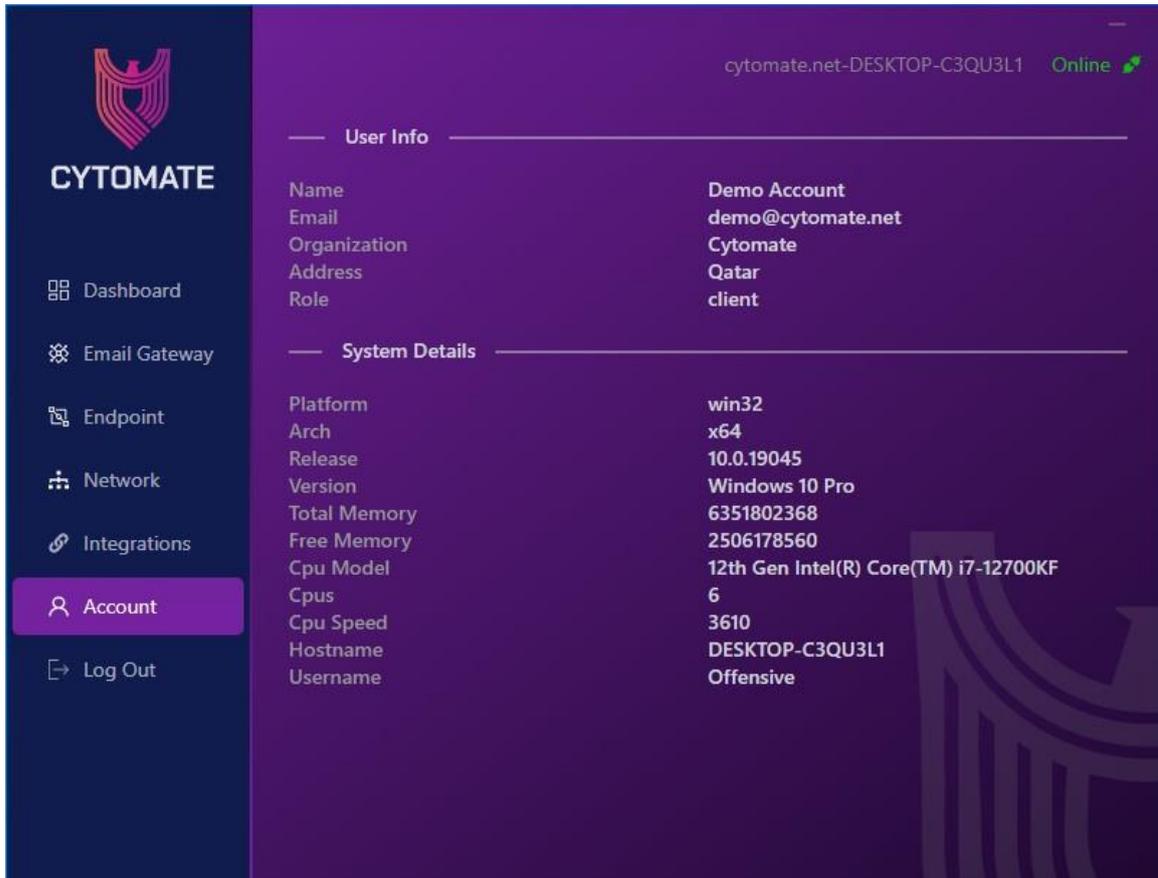


The screenshot displays the CYTOMATE dashboard interface. On the left is a dark sidebar with the CYTOMATE logo and navigation menu items: Dashboard, Email Gateway, Endpoint, Network, Integrations (highlighted), Account, and Log Out. The main content area has a dark purple background and shows the following data:

- Top right: User/Device info: `cytomate.net-DESKTOP-C3QU3L1` Online
- Refresh button: Refresh
- Total Tasks: 4 (All time!)
- Total IOCs: 0 (Last ten minutes!)
- Remaining Tasks:
  - Microsoft Defender for Endpoint: 4
  - Azure Sentinel: 4
- Overall Alert Status Summary: No data (with a laptop icon and speech bubble)
- Bottom: Logs

## 6.6.Account

Within the "Account" menu, you will find user information detailing the account utilized in the agent, along with system details indicating the environment on which the agent is running. This section provides essential insights into the account associated with the agent and the specific system configurations facilitating its operation.



The screenshot displays the 'Account' page in the CYTOMATE interface. The left sidebar contains navigation options: Dashboard, Email Gateway, Endpoint, Network, Integrations, **Account** (selected), and Log Out. The main content area is divided into two sections: 'User Info' and 'System Details'.

**User Info**

Name	Demo Account
Email	demo@cytomate.net
Organization	Cytomate
Address	Qatar
Role	client

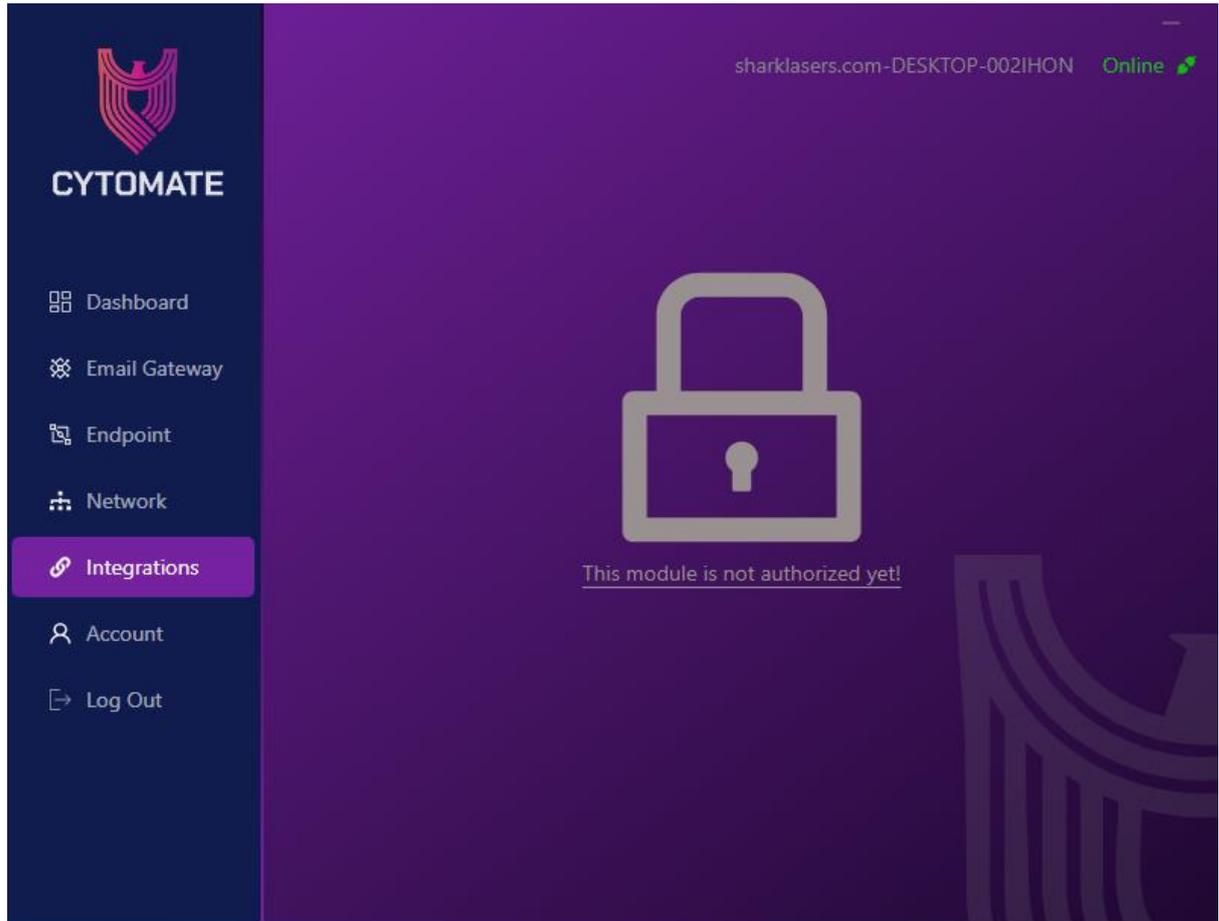
**System Details**

Platform	win32
Arch	x64
Release	10.0.19045
Version	Windows 10 Pro
Total Memory	6351802368
Free Memory	2506178560
Cpu Model	12th Gen Intel(R) Core(TM) i7-12700KF
Cpus	6
Cpu Speed	3610
Hostname	DESKTOP-C3QU3L1
Username	Offensive

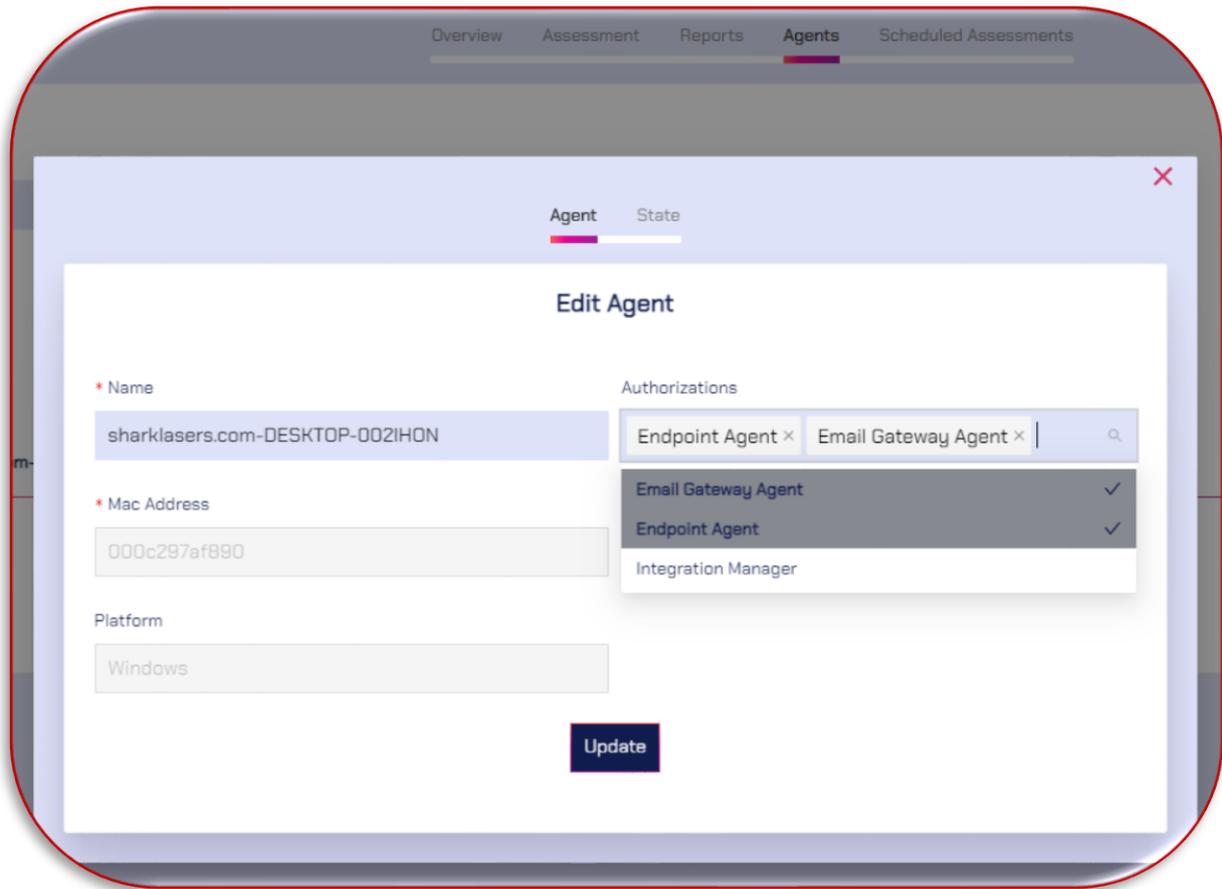
At the top right of the main content area, the status 'cytomate.net-DESKTOP-C3QU3L1 Online' is displayed with a green checkmark icon.

## 6.7. Authorization Module

In Breach+ agent, only Endpoint module is enabled by default. All other modules are locked. They must be enabled from the Breach+ webapp. In the screenshot below, integration module is locked



To enable this module, login to Breach+ webapp, go to Endpoint and then go to Agent Tab. Click on the Edit from the listed agents and enable the modules that are required.



After enabling all required modules from Breach+ dashboard. Logout and login to the Breach+ Agent again and all modules will be authorized.