

# AGENT INSTALLATION User Manual



# **Table of Contents**

1.	Definitions
1.1.	Breach+ Agent
1.2.	Cytomate Breach+
1.3.	Endpoint
2.	Agent Requirements
2.1.	Minimum System Requirements
1.	Windows OS
2.2.	Communication Matrix
3.	Downloading Breach+ Agent
3.1.	Windows OS4
4.	Installation
4.1.	Windows OS
5.	Running The Agent7
5.1.	Windows OS7
6.	Agent Components
6.1.	Dashboard15
6.2.	Email Gateway16
6.3.	Endpoint
6.4.	Network18
6.5.	Integrations19
6.6.	Account
6.7.	Authorization Module





# 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.

		January 3	0, 202
СУТОМАТЕ	LOC Login to your existing a	GIN ccount or <u>Create new</u>	A D A D
*507*507*5	Email Address*		54
	dento@cgtoniate.net		$\Rightarrow$
Walcomo Book	Password*		$\leq\langle$
WEICOTTE DACK!		ø	$\Rightarrow$
Discovering Unknown Threats	Remember me?	Forgot Password?	$\leq$
contact@cutomate net	Sign up	Login	$\mathbb{Z}$
	Sign in wi	th Microsoft	$\rightarrow$
Privacy Policy All Rights Reserved			

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

	-			
亘 Dashboard		🗊 Start Assesment	♠ Agent	P 🕈 Demo Account 🔻

# **3.1.Windows OS**

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

	Agent Installation Integ	gration Manager	
(1) Choose OS			_
	H Windows	🙏 Linux	
2 Download Ag	ent		
Click on follo	wing button to download agent	t.	
	က Downloa	nd Agent	

- 2) The agent download process will begin, but you may encounter Downloads, File Warnings that could impede the process.
  - i. To complete the download, right-click on the Downloads document and select "Keep" from the menu.
  - ii. 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.

+974 31526979



# 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.

runger Setup - BreachPlusAgent version 2.0 —		×
<b>Information</b> Please read the following important information before continuing.		
When you are ready to continue with Setup, dick Next.		
BreachPlusAgent 2.0		
This is Breach and Attack Simulation agent, which runs in both normal and privileged modes.		
Next	С	ancel

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

+974 31526979 💮 www.cytomate.net

↓ Setup - BreachPlusAgent version 2.0		_20		×
Select Destination Location			F	Y
Where should BreachPlusAgent be installed?			6	01)
Setup will install BreachPlusAgent into the following folder				
To continue, click Next. If you would like to select a different folde	r, click Browse.			
C:\Program Files (x86)\BreachPlusAgent		Br	owse	
At least 484.5 MB of free disk space is required.				

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

3 Setup - BreachPlusAgent Version 2.0	- 🗆 X
Installing	FR
Please wait while Setup installs BreachPlusAgent on your computer.	
Extracting files	
C:\Program Files (x86)\BreachPlusAgent\Cytomate Agent.exe	

0

CYTOMATE





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

└ Setup - BreachPlusAgent version 2	2.0 — 🗆	×
	Completing the BreachPlusAgent Setup     Wizard     Setup has finished installing BreachPlusAgent on your computer. The application may be launched by selecting the installed shortcuts.     Click Finish to exit Setup.     ☑ Launch BreachPlusAgent	•
	Back Finish	

- 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.

- All Apps Documents	Web Settings	People	Folders	Photos 🕨	BO	
Best match			<b>N</b>			
BreachPlusAgent		<b>X</b>				
Search the web			BreachPlu	usAgent		
Q breachplusagent - See more search results	<b>`</b>		Ар	p 		-

#### 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:

+974 31526979 💮 www.cytomate.net



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"

Wind	dows Security
$\leftarrow$	
$\equiv$	
ŵ	Home
0	Virus & threat protection
8	Account protection
((y))	Firewall & network 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

User Access Control Do you want to allow this app to make changes to your device?	x
Windows Security Verified publisher: Microsoft Windows Publisher Show more details	
Yes No	

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).



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.

Organize 🔻 🛛 New fold	er		≣ • 🕐
> 📥 OneDrive	Name	Date modified	Туре
🗸 💻 This PC	🚞 BreachPlusAgent	1/26/2024 3:09 PM	File folder
> 🟪 Local Disk (C:)	Common Files	1/9/2024 11:39 AM	File folder
> 🗕 Virtual Machin	adotnet	8/30/2022 3:36 PM	File folder

viii. The "BreachPlusAgent" folder will be added to the protected folders list.



C·\Program Files (v86)\BreachPlusAge	nt
c. (Frogram Fries (X00) (breach TasAge	
Foldor	

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.





	— Offline 🆋
CYTOMATE	
Breach+ Agent	
To generate API key, go to portal and navigate to Account, select Api tab and request new key. API Key Ø	
Login	

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

CYTOMATE	⊡ Account				🗘 Agont 🧬 🎗 Demo Ac
		Profile Package	Domains Api		```
88 Deshboard		_			
teb Web		First Namo	Last Nome	Email	Organization
I Wef		Demo	Account	demo@cytomate.net	Cytomate
🔆 Email Gateway		Address Qatar	Role client	Edit Profile →	
ିଲ୍ଲ Endpoint		Current Pasaword	New Paseword	Lost Changed	Lindete à
🕤 Cempelgn 🛛 👻	Demo Account	Current Password Ø	New Password Ø	21 Nov 2023, 10:40 AM	Update 7
Templates 🗸	Edit Avatar →				
ሰ Analytics 🗸					
Reports					
A Manage User					
🔗 Integrations					
🗭 Plugin					
Account					

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.

O

📞 +974 31526979 💮 www.cytomate.net



Account								♠ Agent	P Demo Acco
			Profile	Package	Domains	Арі			
API Key S Keys you have g	ettings enerated that can be us	ed to access the <b>Cy</b>	tomate APT	API.					Request New Key
<b>Q</b> ,	Name: Status: Last Updated: API kays function simil requests via Basic Auti	Default Active 14/08/2023, 13: arly to OAuth access entication to fetch	44:12 s tokens. Th security pro	ey serve as a <b>ovider alerts</b> a	ternative cred	dentials over H	TTPS, and can	be utilized for a	uthenticating API
API Key: ******	*****		*******	•••••213b					© Show

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.

СУТОМАТЕ	Endpoint 0 Assessments	S Email Gateway Assessments	tomate.net-D	ESKTOP-C3QU3L1 Integration Tasks	Online
品 Dashboard	Active Components	1	Active Integ	rations	2
🔅 Email Gateway	on this agent		on this agent		
閲 Endpoint	袋 Email Gateway 図 Endpoint		Azure Se	entinel	eint a
	A Network		Cantinal		
抗 Network	S Integrations	8	senunei	One	
Integrations					
ද Account					
-> Log Out					

0





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.

🗏 End	dpoint						♠ Agent	2 Q Demo Account
		Overview	Assessment	Reports	Agents	Scheduled Assessments		
		C	2	🔂 Refi	resh		📋 Delete	
l l								
	cytomate.net-DESKTOP-0	C3QU3L1	080027663c7	1		25 Jan 2024, 4:04:29 PM	Online	Edit

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.

Name	MAC Address	Platform	Created On	State	Modify
cytomate.net-DESKTOP-C3QU3L1	080027663c71	4	25 Jan 2024, 4:04:29 PM	Online	Edit

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

	Agent State	
	Edit Agent	
* Name	Authorizations	
cytomate.net-Demo	Endpoint Agent × + 3	
* Mac Address	* System Name	
080027663c71	DESKTOP-C3QU3L1	
Platform		
Windows		
	Update	
~		



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.

Agent State	
Change Agent State	
State: Active	
Disabled Agent	

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

0



#### 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.

¥		c	ytomate.net-D	ESKTOP-C3QU3L1	Online 🤞
CYTOMATE	Endpoint 0 Assessments	Email Gatewa Assessments	0 ע	Integration Tasks	
品 Dashboard	Active Components on this agent	1	Active Integ on this agent	rations	2
💥 Email Gateway	🕉 Email Gateway	0	💿 Azure Se	entinel	
හි Endpoint	强 Endpoint	1	🕢 Microsot	ft Defender for Endr	oint 🍠
. Natural	rt Network	8	Sentinel	One	
III NELWOIK	Integrations	8			
Integrations					
A Account					
[→ Log Out					



# **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-D	ESKTOP-C3QU3L1	Online 🖋
		-	Refrest			
CYTOMATE	Not Bypassed All time!	0	Not Tested All time!	314	Bypassed All time!	0
品 Dashboard			M 1	- F1		
🔅 Email Gateway			Logi	in email		
	* Email			* Password		
🛱 Endpoint						
🚠 Network	Server Hostname		i	Port		
${\mathscr O}$ Integrations						
A Account					111	
[→ Log Out	SSL/TLS					
			ÐL	oain		
	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.

W			c) Refresh	/tomate.net-D	ESKTOP-C3QU3L1	Online 🖋
CYTOMATE	Not Bypassed All time!	0	Not Tested All time!	2604	Bypassed All time!	0
品 Dashboard			Assessment	Details		
🛞 Email Gateway	Logs					V
뚾 Endpoint	[2024-01-25 14:09:23] [2024-01-25 14:09:24]	[info] [info]	In progress Asso [NORMAL] Fetching [NORMAL] No endpo	essment di g endpoint ta pint tasks fo	asks bund	
🚓 Network	[2024-01-25 14:09:28] [2024-01-25 14:09:28] [2024-01-25 14:09:29]	[info] [info] [info]	[ELEVATED] Fetchi [ELEVATED] No end [NORMAL] Fetching	ing endpoint dpoint tasks g endpoint ta	tasks found asks	
𝔗 Integrations	[2024-01-25 14:09:29] [2024-01-25 14:09:33] [2024-01-25 14:09:34]	[info] [info] [info]	[NORMAL] No endpo [ELEVATED] Fetchi [ELEVATED] No end	ing endpoint point tasks fo	bund tasks found	
A Account	[2024-01-25 14:09:34] [2024-01-25 14:09:34] [2024-01-25 14:09:39]	[info] [info]	[NORMAL] Fetching [NORMAL] No endpo [FLEVATED] Fetchi	g endpoint ta pint tasks fo	asks ound tasks	
[→ Log Out	[2024-01-25 14:09:40] [2024-01-25 14:09:39] [2024-01-25 14:09:45] [2024-01-25 14:09:45] [2024-01-25 14:09:50] [2024-01-25 14:09:50] [2024-01-25 14:09:50] [2024-01-25 14:09:50] [2024-01-25 14:09:55] [2024-01-25 14:09:55]	[info] [info] [info] [info] [info] [info] [info] [info] [info] [info]	ELEVATED] No end [NORMAL] Fetching [ELEVATED] Fetching [ELEVATED] No end [NORMAL] No endpo [ELEVATED] Fetching [NORMAL] Fetching [ELEVATED] No endpo [ELEVATED] No endpo [ELEVATED] No endplo [ELEVATED] No endplo [ELEVATED] Fetching	point tasks g endpoint ta dpoint tasks point tasks for tasks for ing endpoint ta point tasks for dpoint tasks ing endpoint tasks z endpoint tasks	found asks tasks found tasks asks ound found tasks ssks	



# 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.

W		cytomate.ne	 et-DESKTOP-C3QU3L1 Online 🖋
CYTOMATE	Not Bypassed 0 All time!	Not Tested 1 All time!	Bypassed 0 All time!
品 Dashboard		Assessment Details Queued Assessments: 0	
쬸 Email Gateway 閐 Endpoint		In progress Assessment 🕯 No assessment currently runr	ning
📩 Network			
Integrations			
A Account			
[→ Log Out			
	Logs		^

O





# **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.

W		
CYTOMATE	Total Tasks 4 All time!	Total IOCs 0 Last ten minutes!
品 Dashboard	Remaining Tasks	Overall Alert Status Summary
🔅 Email Gateway	- Microsoft 🖋 4	
쭯 Endpoint	Ø Defender for Endpoint	
🕂 Network	Azure Sentinel	No data
Integrations		
A Account		
[→ Log Out		
	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.

W	User Info	
CYTOMATE	Name Email Organization	Demo Account demo@cytomate.net Cytomate
品 Dashboard	Address Role	Qatar client
🔅 Email Gateway	— System Details —	
跑 Endpoint	Platform Arch	win32 x64
📅 Network	Kelease Version	Windows 10 Pro
Integrations	Total Memory Free Memory Cpu Model	6351802368 2506178560 12th Gen Intel(R) Core(TM) i7-12700KF
A Account	Cpus Cpu Speed	6 3610
[→ Log Out	Hostname Username	DESKTOP-C3QU3L1 Offensive

0





# **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.



	Agent	State		
	Edit A	gent		
* Name		Authorizations		
sharklasers.com-DESKTOP-002IH0	1	Endpoint Agent ×	Email Gateway Agent ×	Q
* Mac Address		Email Gateway Agent		$\checkmark$
000c297af890		Endpoint Agent Integration Manager		$\checkmark$
Platform				
Windows				

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

0

