CyberArmor.AI Installation Guide — Windows, Mac and Chrome

Last verified: 2026-11-21, against the code only, on `main` at commit 3310fef64 (endpoint agent 1.0.20, browser extension 2.3.28): every step's page order, question, button and menu wording was read from the installer, extension and status-menu sources. Nothing was re-run on a device for that pass, and the screenshots still show the installers of 2026-10-24, so the pictures of the server question, of Installation Type and of Custom Setup differ from what you will see. The device runs this guide rests on are the earlier ones that follow.

Earlier: 2026-10-29, the whole guide was checked against the code on `main` at commit 1f4497db6. The certificate's name in step 9 was read from `install_local_proxy.sh` and `install_local_proxy.ps1` on 2026-10-29; those renamed dialogs have not yet been seen on a device. Part D (Windows) was run end to end on 2026-10-29 on a clean Windows 11 computer with the signed 1.0.13-rc.15 MSI downloaded from the United States portal (app.cyberarmor.ai), which was before that rename. Part C steps 8–11 (Mac) were run end to end on 2026-10-26 on a clean macOS 26 VM against the live Singapore portal (am-app.cyberarmor.ai) at release 1.0.13-rc.12: the agent installed and enrolled into `cn-demo-bank`, Full Disk Access was granted by path, the daemon was restarted, and `cyberarmor-status` then reported `[ ok ] endpoint.monitoring_health` and, after the local proxy was set up, `CyberArmor — Protected` with AI-traffic inspection on. The browser extension steps describe extension 2.3.20. The screenshots were taken on 2026-10-24; where a picture and the text differ, the text describes what you will see.

This guide connects a computer to your organization's CyberArmor.AI service. There are three ways, and you can use more than one on the same computer:

What to install	Best for	Time	Needs an administrator password on the computer?
Browser extension (Chrome, Edge, Brave)	The fastest start. Protects AI use **only in the browser profiles you install it in** — Chrome, Edge and Brave are each separate, and so is each profile inside them (see Part B, Step 7).	About 3 minutes per profile	No
Mac agent	Full protection on a Mac, including desktop AI apps.	About 5 minutes	Yes
Windows agent (beta)	Full protection on 64-bit Windows PCs.	About 5 minutes	Yes

Before you start, you need:

1. A sign-in to the Customer Portal: **https://am-app.cyberarmor.ai** (Asia and Middle East) or **https://app.cyberarmor.ai** (United States). See the **Customer Portal User Guide**, section 1. If your organization runs its own CyberArmor.AI server, use the address your administrator or partner gave you wherever this guide names a portal address.
2. A role that can issue install tokens: **Deployer**, **Analyst** or **Tenant admin**.

Every installation follows the same three steps:

Download → Get a one-time token → Install and paste the token

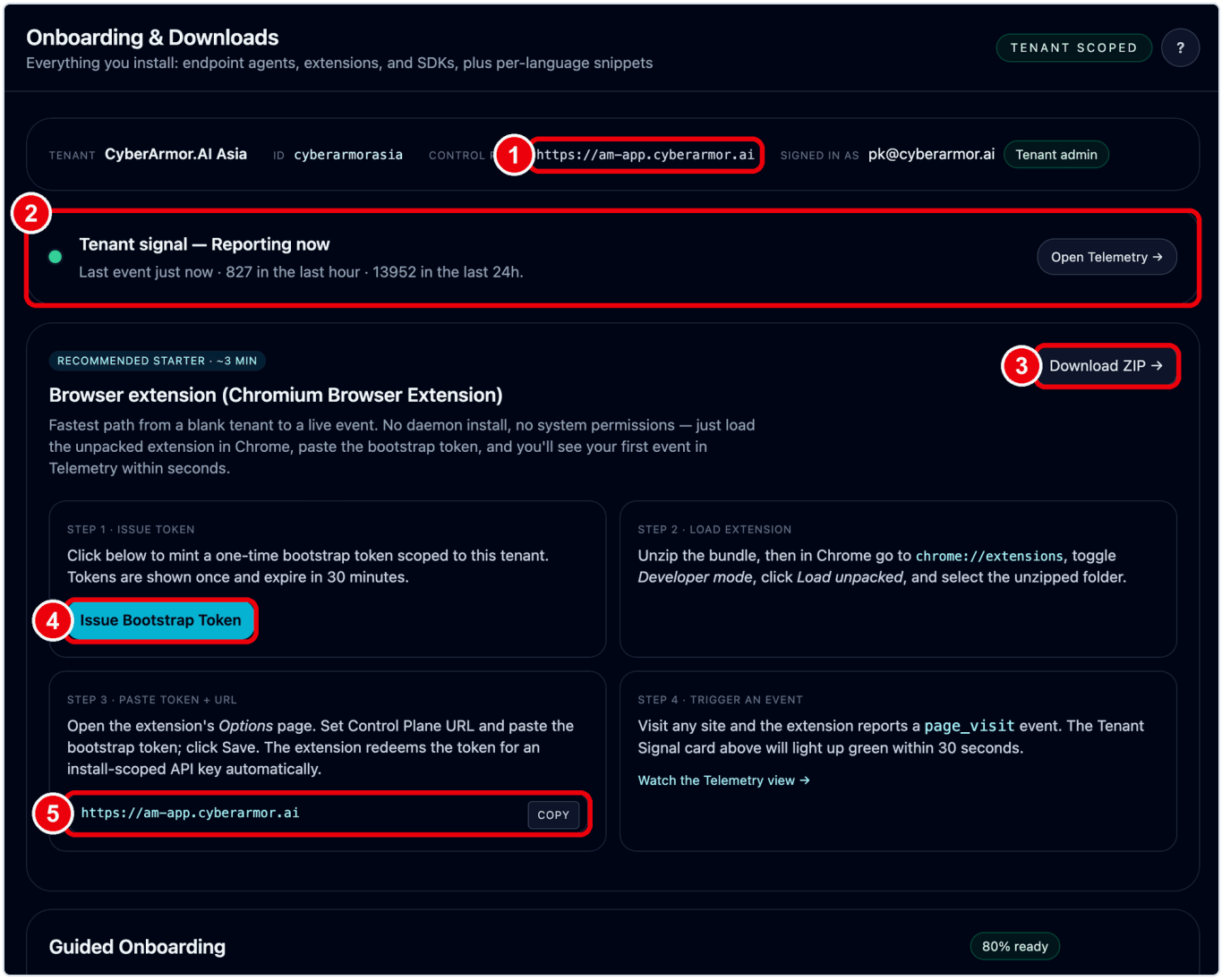
Prefer to watch? The training video *Installation: from sign-in to a protected computer* (9 minutes) shows every step of this guide on one computer. It is on the documentation site at **https://docs.cyberarmor.ai/training/customer-walkthrough/**, on **https://cyberarmor.ai/training**, and in the Customer Portal under **Support → Help & FAQ → Training videos**.

Part A. Get the installer and a token (all computers)

Step 1. Sign in to **https://am-app.cyberarmor.ai** and click **Setup & Admin → Onboarding & Downloads** in the menu.

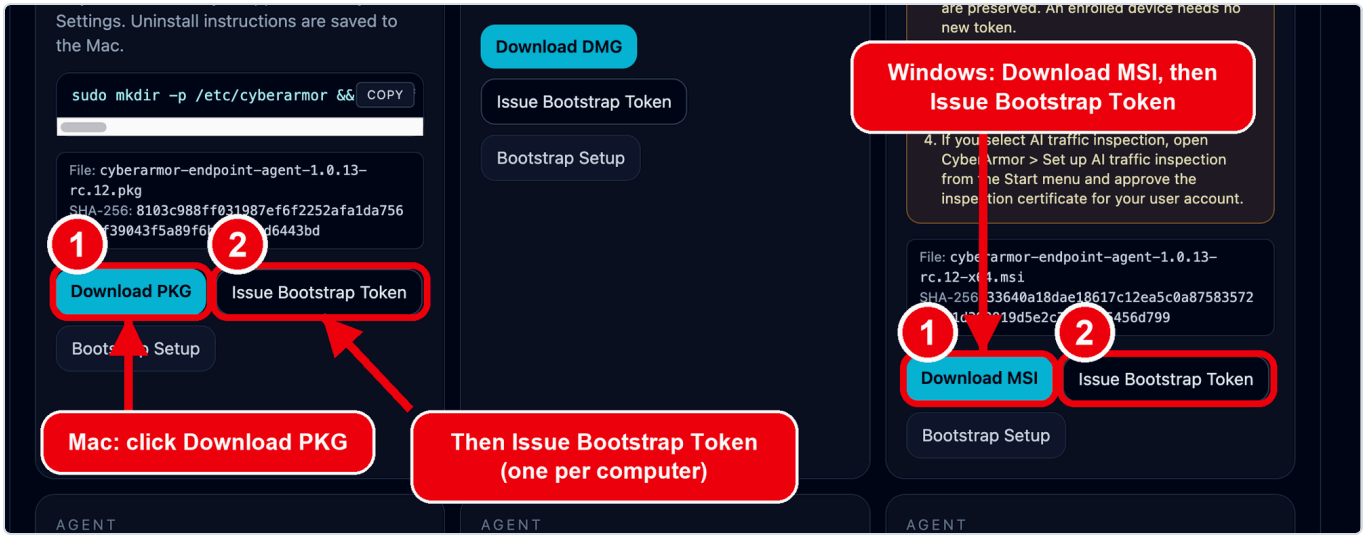
Step 2. Note two things at the top of the page:

- (1) the **Control plane** address, `https://am-app.cyberarmor.ai` ; you choose or type it during installation;
- the **ID** of your organization, for example `cyberarmorasia` ; the browser extension asks for it.



Step 3. Download the right file:

- **Chrome, Edge or Brave extension:** click **Download ZIP** → (3), in the *Recommended starter* box at the top, headed **CyberArmor.AI Protect**.
- **Mac:** scroll to the **Endpoint Agent** group. On the **CyberArmor.AI Endpoint Agent — macOS installer (PKG, signed and notarized)** card click **Download PKG**. This is for Apple silicon Macs; see the note at the top of Part C for Intel Macs. (The **CyberArmor.AI Endpoint Agent — macOS disk image (DMG)** card holds the same installer inside a disk image.)
- **Windows:** on the **CyberArmor.AI Endpoint Agent — Windows installer (MSI, beta)** card click **Download MSI**.



Step 4. On the same card, click **Issue Bootstrap Token**. The token appears at the top of the page. Click **COPY**.

- One token connects **one** computer.
- It expires after **30 minutes**: issue it just before you install.
- Treat it like a password: do not email it.

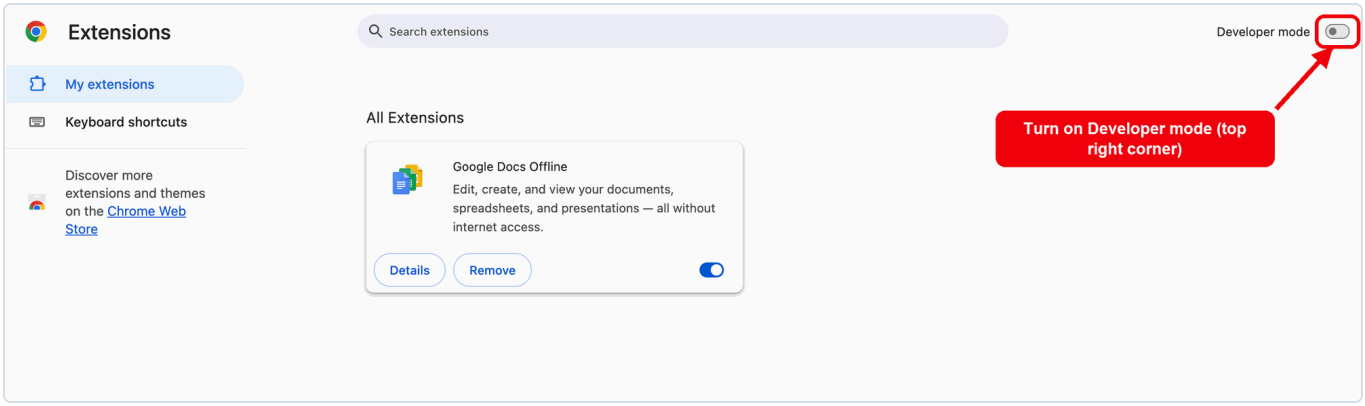


Part B. Browser extension: Chrome, Edge and Brave

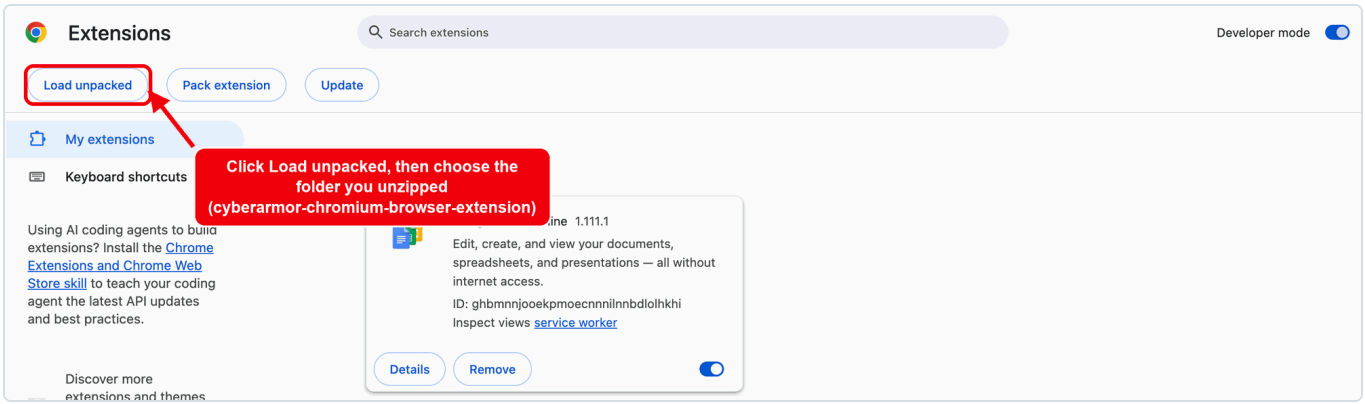
The extension is called CyberArmor.AI Protect. Its version number is shown on `chrome://extensions` *(2.3.28 or later). It is installed from the ZIP file in the portal; it has not been published in the Chrome Web Store, the Edge Add-ons store or Firefox Add-ons yet. In Microsoft Edge use* `edge://extensions`*, and in Brave* `brave://extensions`*, wherever this part says* `chrome://extensions`*.*

Step 1. Find the downloaded file `cyberarmor-chromium-browser-extension.zip` in your Downloads folder and unzip it (double-click on Mac; right-click → **Extract All** on Windows). You get a folder called **cyberarmor-chromium-browser-extension**. Keep this folder: the browser loads the extension from it.

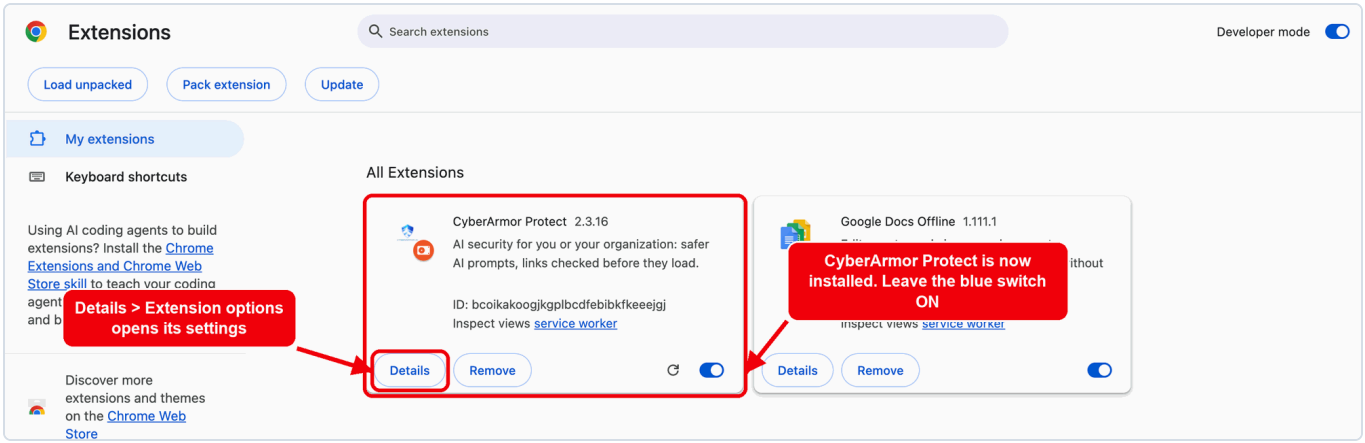
Step 2. In Chrome, type `chrome://extensions` in the address bar and press Enter. Turn on **Developer mode** (top right corner).



Step 3. Three new buttons appear. Click **Load unpacked**, then choose the **cyberarmor-chromium-browser-extension** folder you unzipped, and click **Select**.



Step 4. CyberArmor.AI Protect now appears in the list. Make sure its switch is on (blue). Click **Details**, then scroll down and click **Extension options**. Tip: click the puzzle-piece icon in the toolbar and pin **CyberArmor.AI Protect** so it is always visible.

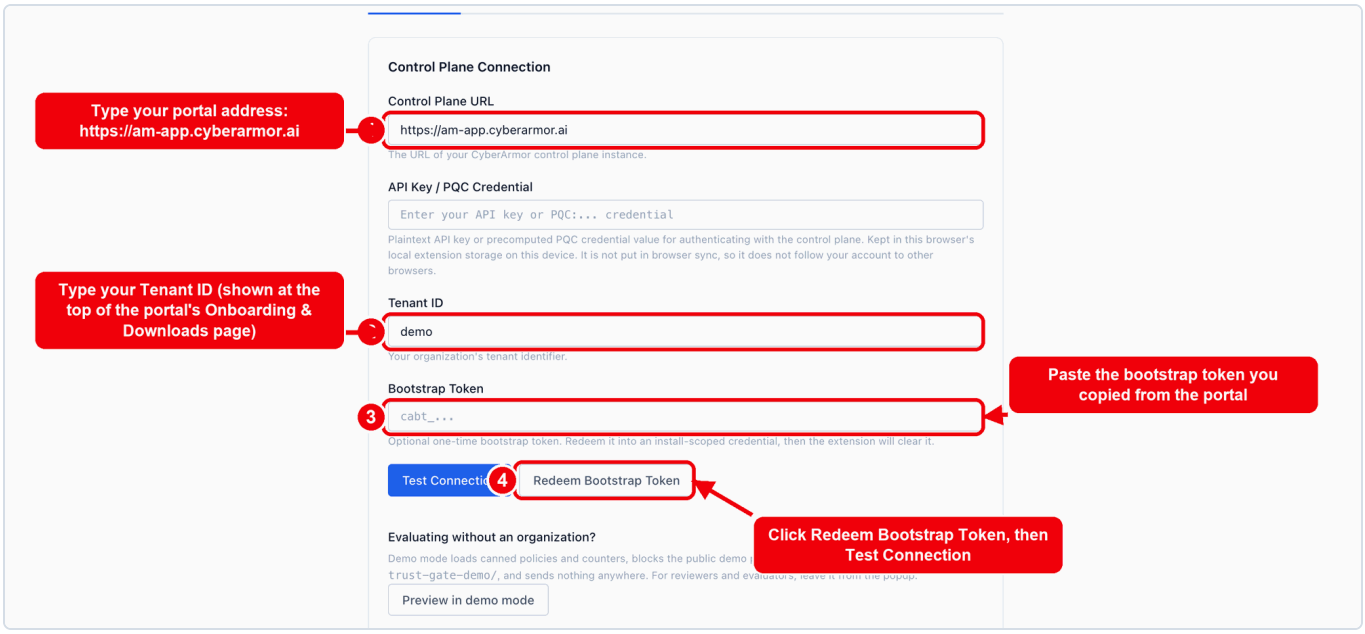


Step 5. Agree, then connect. The settings page opens on the **Protection level** tab. Click the **Connection** tab.

1. Read **Before you connect: what CyberArmor.AI Protect sends**. It lists what the extension sends once it is connected, and that it sends it only to your organization's CyberArmor.AI server: the address of each page you open (without the part after "?"), the text of prompts you send to AI services and files you upload to them when your organization's policy says so, a record of what it warned about, redacted or blocked, and this browser's enrollment identity. **Nothing is sent until you agree.** Click **I agree: connect and send this data**.
2. **Server address (required).** Nothing is filled in for you. Click **Singapore (am-app.cyberarmor.ai)** in Asia and the Middle East, or **United States (app.cyberarmor.ai)** in the United States. If your organization runs its own server, click **My organisation's server** and type its address, which starts with `https://`.

3. **Tenant ID:** type your organization ID from the portal (Part A, step 2).
4. **Bootstrap Token:** paste the token you copied (Part A, step 4).
5. Click **Redeem Bootstrap Token**. When it succeeds, click **Test Connection**.

Until you click **I agree**, the extension refuses to redeem a token, test a connection or save a server address. Your agreement is recorded in this browser only.



Step 6. Check it works. Visit any website. Within about 30 seconds, the **Tenant signal** on the portal's **Onboarding & Downloads** page turns green, and the browser appears in **Inventory** → **Endpoints**.

To see a block page on purpose, open **https://aitrustlab.org/url-trust-gate-demo/**. That site holds the URL Trust Gate demonstration pages: the attack pages on it are blocked, and `benign.html` is allowed. (These pages used to be on `app.cyberarmor.ai/url-trust-gate-demo/`. That old address now answers **410 Gone**; update any bookmark.)

Step 7. Repeat for every browser AND every browser profile

This step decides whether the extension protects you at all. Do not skip it.

A browser extension lives inside one browser, and inside that browser, inside **one profile**. Chrome treats each profile as a separate browser with its own extension list. So:

- Installing it in Chrome does nothing for Edge or Brave.
- Installing it in your work profile does nothing for your personal profile **on the same computer**.
- A profile added after you rolled the extension out has no extension until someone adds it there.

Repeat Steps 1 to 6 in **every browser your people actually use for AI, and in every profile inside it**. Added, agreed, configured and connected are all required — an extension that is present but never had **I agree** and **Redeem Bootstrap Token** completed is not protecting that profile either.

A profile without it is not partly protected. It is not protected, and nothing on that screen tells the person using it. The portal cannot list a profile it has never heard from, so an uninstrumented profile is invisible there too — absence in **Inventory** → **Endpoints** is not evidence that a profile is safe.

To check a profile quickly: switch to it, open `chrome://extensions`, and confirm **CyberArmor.AI Protect** is listed and switched on; then open its **Extension options** and confirm **Test Connection** succeeds.

This is also the reason to install the endpoint agent (Parts C and D) even where the extension is deployed everywhere today: once AI traffic inspection is set up, the agent works at the level of the machine rather than one browser profile, so AI traffic from a profile somebody created this morning is covered too. It does not see inside every application; the status page lists what is covered. Treat the extension as per-profile coverage and the agent as machine-wide coverage.

What the extension does once it is connected

What happens on a given page is decided by your organization's policies in the Customer Portal. A few behaviors are worth knowing before people meet them:

- **Block pages.** When a policy blocks a site, the extension shows a block page that names what was blocked. **Back**, and the page's **Go Back to Safety** button, return to the page you were on before the blocked one. Opening the blocked address again is blocked again.
- **A card PIN stays off sites that are not the bank's.** If your organization has a card-PIN policy (see the Customer Portal User Guide, section 7), a debit-card PIN typed next to a card number — in an AI chat or in a web form — is handled by that policy before it leaves the browser. In an AI chat, a **redact** policy removes the PIN as it is typed and a **block** policy stops the message from being sent. In a web form the form is held: a **block** policy sends nothing and names the policy; a **redact** policy empties the PIN field, masks the card number and holds the form so the person can see why. The bank's own website is the exception, and the exception comes only from bank lists, never from payment processors or card networks.
- **Private network addresses** (routers, printers, intranet apps opened by IP address) are allowed, warned about or blocked according to the tenant's **Settings** → **Private network addresses**. The extension never sends those addresses to CyberArmor.AI.

Firefox, and Firefox for Android

The portal's **CyberArmor.AI Protect — Browser extension for Firefox** card offers `cyberarmor-firefox-extension.zip`, the same extension packaged for Firefox.

- **Firefox on a computer:** open `about:debugging#/runtime/this-firefox`, click **Load Temporary Add-on**, and choose `manifest.json` inside the unzipped folder. Firefox 140 or later is required. Then follow Step 5 above. Firefox removes a temporary add-on when it restarts, so this is for evaluation; a permanent installation needs the extension's listing on Firefox Add-ons, which has not been published yet.
- **Firefox for Android:** the package supports Firefox for Android 142 or later. Firefox for Android installs extensions only from Firefox Add-ons (addons.mozilla.org), where CyberArmor.AI Protect has not been published yet. Until it is, ask your CyberArmor.AI contact how to install it on Android devices.

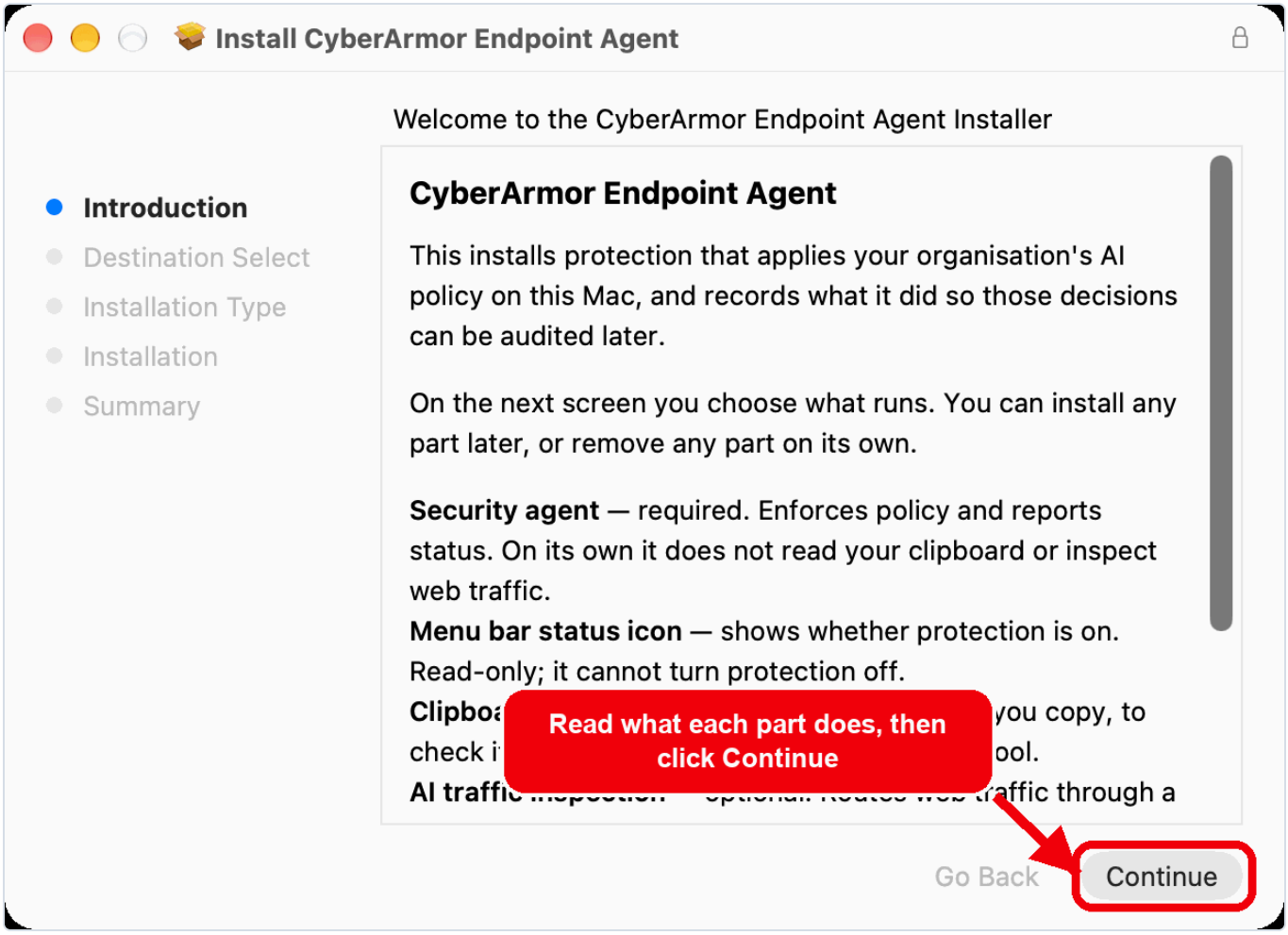
Code editors: the **Browser, IDE & Office** group also offers extensions for VS Code, Cursor and Kiro as `.vsix` files, each with its install command on the card. They are not covered in this guide.

Part C. Mac

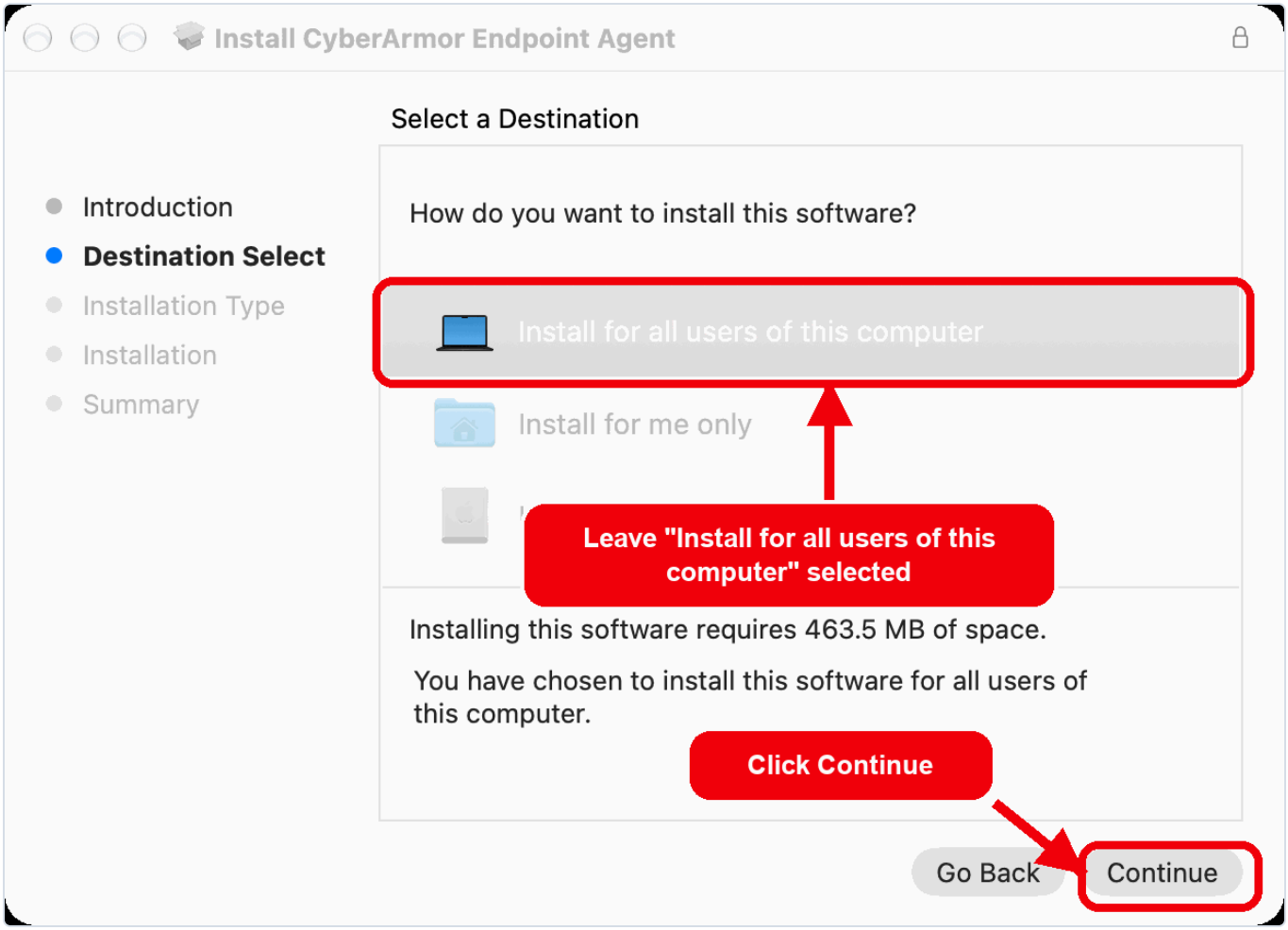
macOS 12 or later on a Mac with Apple silicon (M1 or later). The current installer does not run on Intel Macs: Apple menu → About This Mac shows which chip you have. On an Intel Mac, use the Download PKG for Intel Macs button on the same card if it is shown (the last version built for Intel), or ask your CyberArmor.AI contact. You need the password of an administrator account on the Mac.

Step 1. Find `cyberarmor-endpoint-agent.pkg` in your Downloads folder and double-click it. The installer is signed and notarized by Apple, so it opens without warnings.

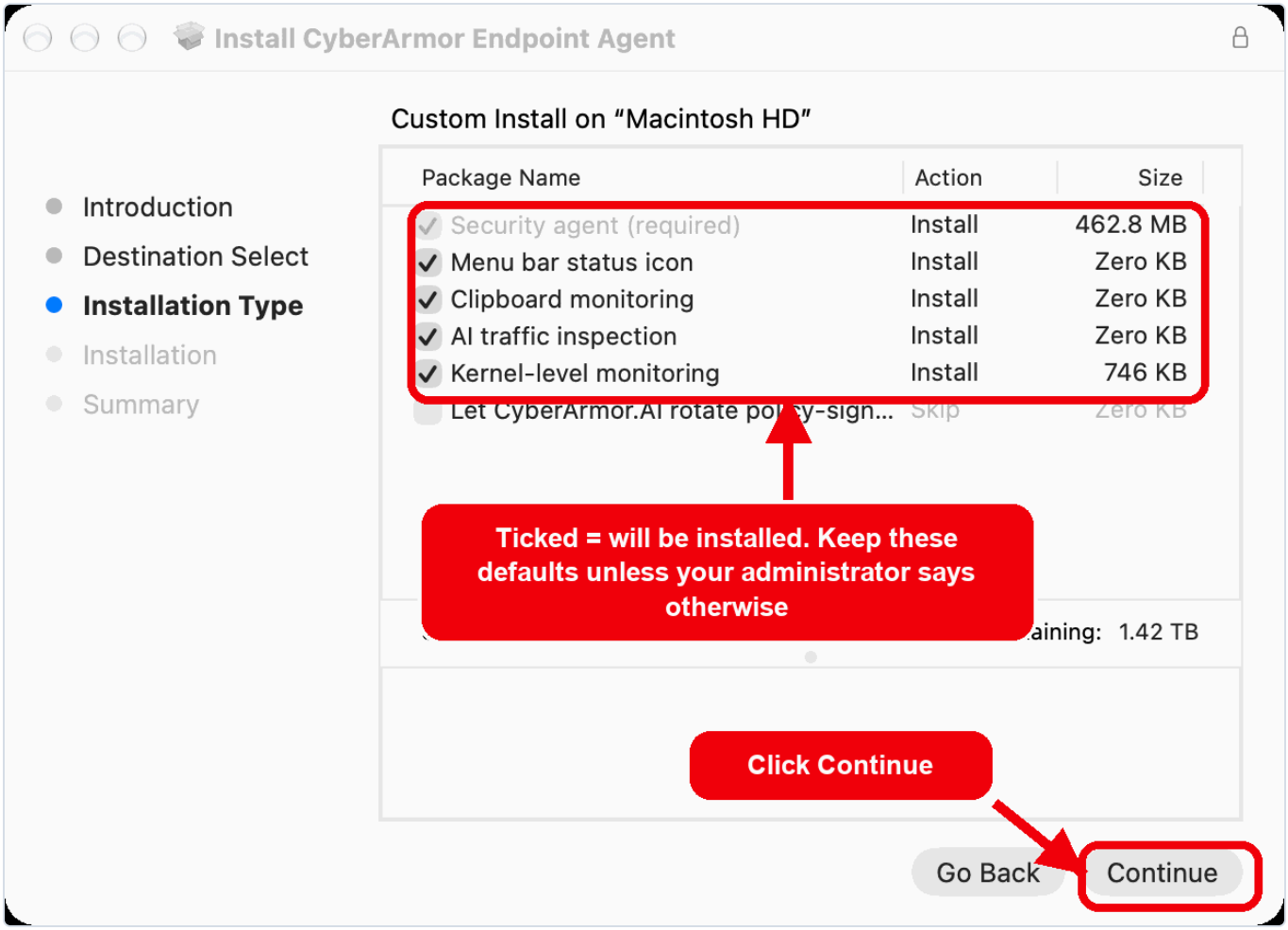
Step 2. The **Introduction** page explains each part of the software. Read it and click **Continue**. The **License** page follows: read the agreement, click **Continue**, then **Agree**.



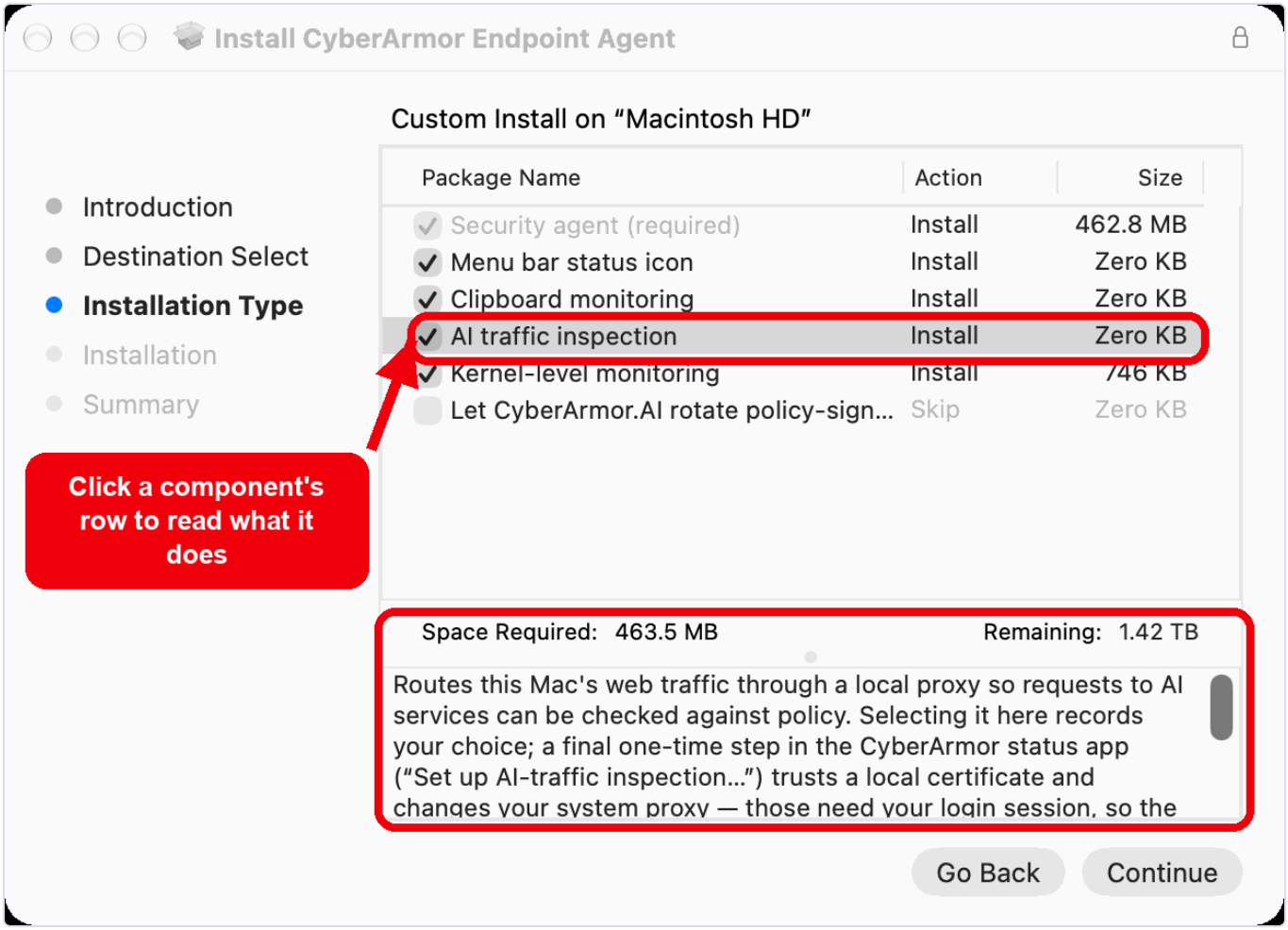
Step 3. On **Select a Destination**, leave **Install for all users of this computer** selected and click **Continue**. (Some Macs skip this page.)



Step 4. Components. Installation Type offers **Install**, which installs every part listed below. You do not need to choose anything. To leave a part out, click **Customize**: the parts appear as a list, as in the picture, and a tick means it will be installed.



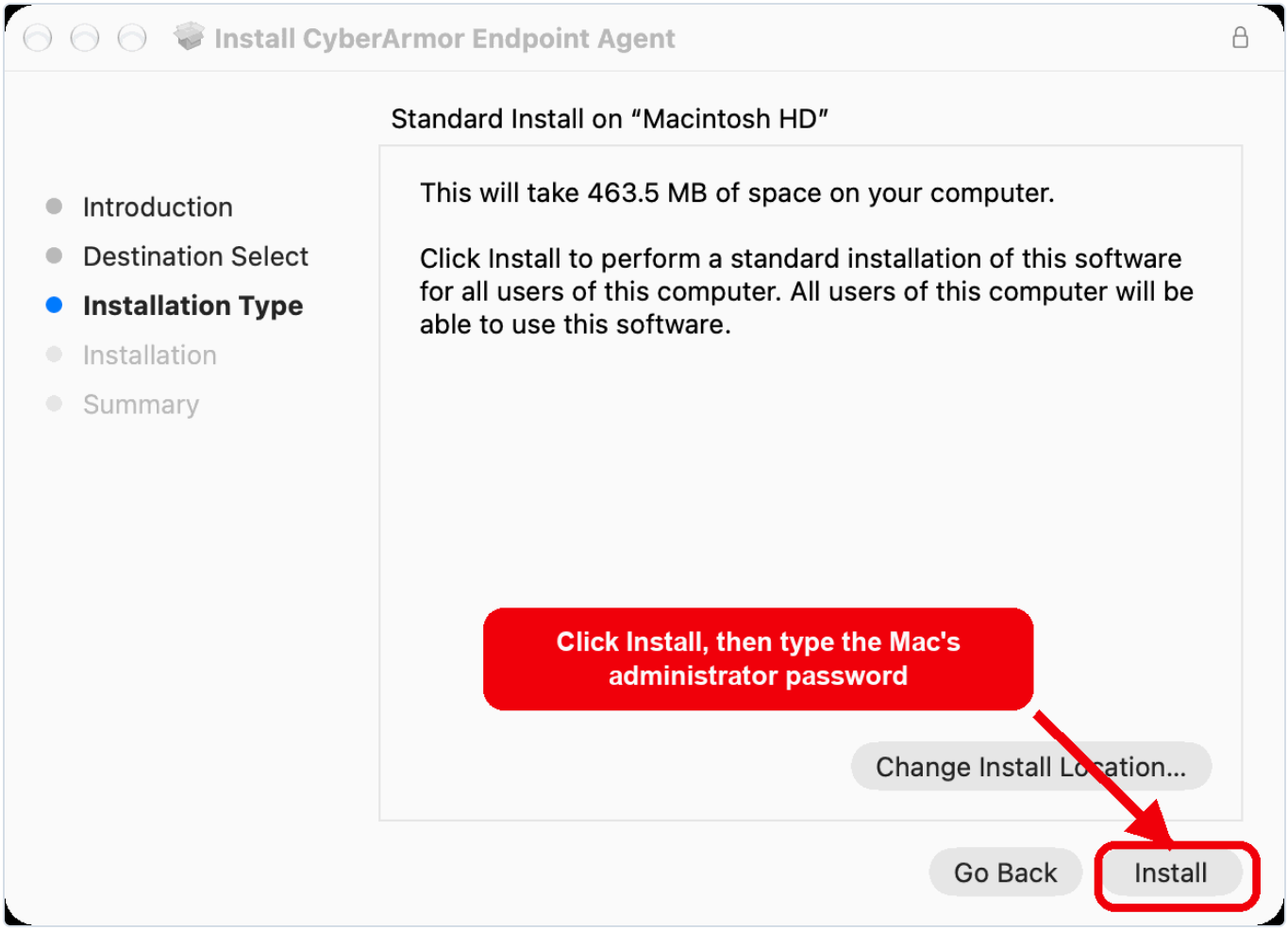
In that list, click a row (not its tick box) to read what it does in the box underneath.



Component	Ticked at first?	What it does
Security agent (required)	Always	The background service that applies your organization's AI policy and reports this Mac's status.
Menu bar status icon	Yes	Shows in the menu bar whether protection is on. It cannot turn protection off.
Clipboard monitoring	Yes	Checks what you copy for sensitive data, and redacts or clears it according to policy.
AI traffic inspection	Yes	Checks web requests to AI services. Needs one extra step after installing (step 10).
Kernel-level monitoring	Yes	Sees desktop AI apps and the files they read. Needs your approval after installing (step 8).
Let CyberArmor.AI rotate policy-signing keys for this device through your organization's signed weekly posture	No	Leave unticked unless your administrator tells you otherwise.

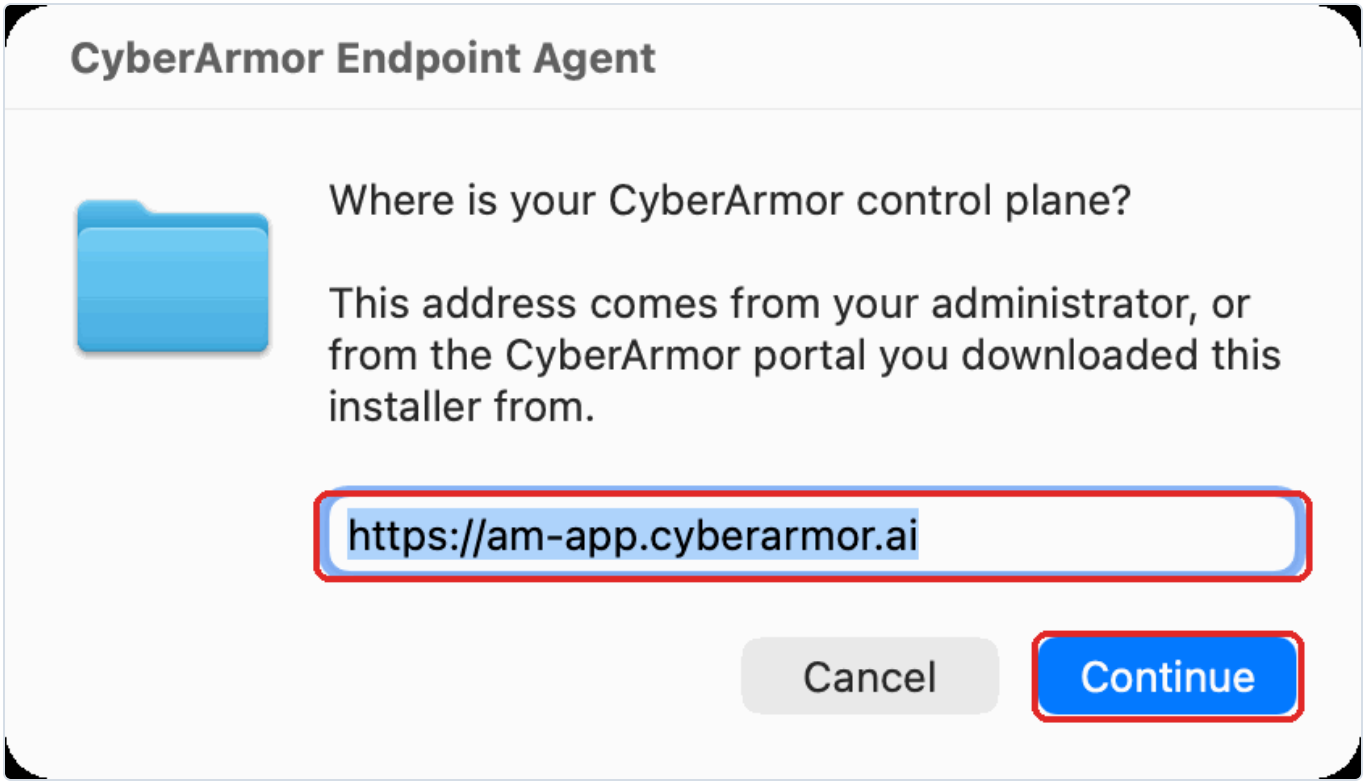
Keep the defaults unless your administrator says otherwise.

Step 5. Click **Install**, then type the Mac's administrator password and click **Install Software**.

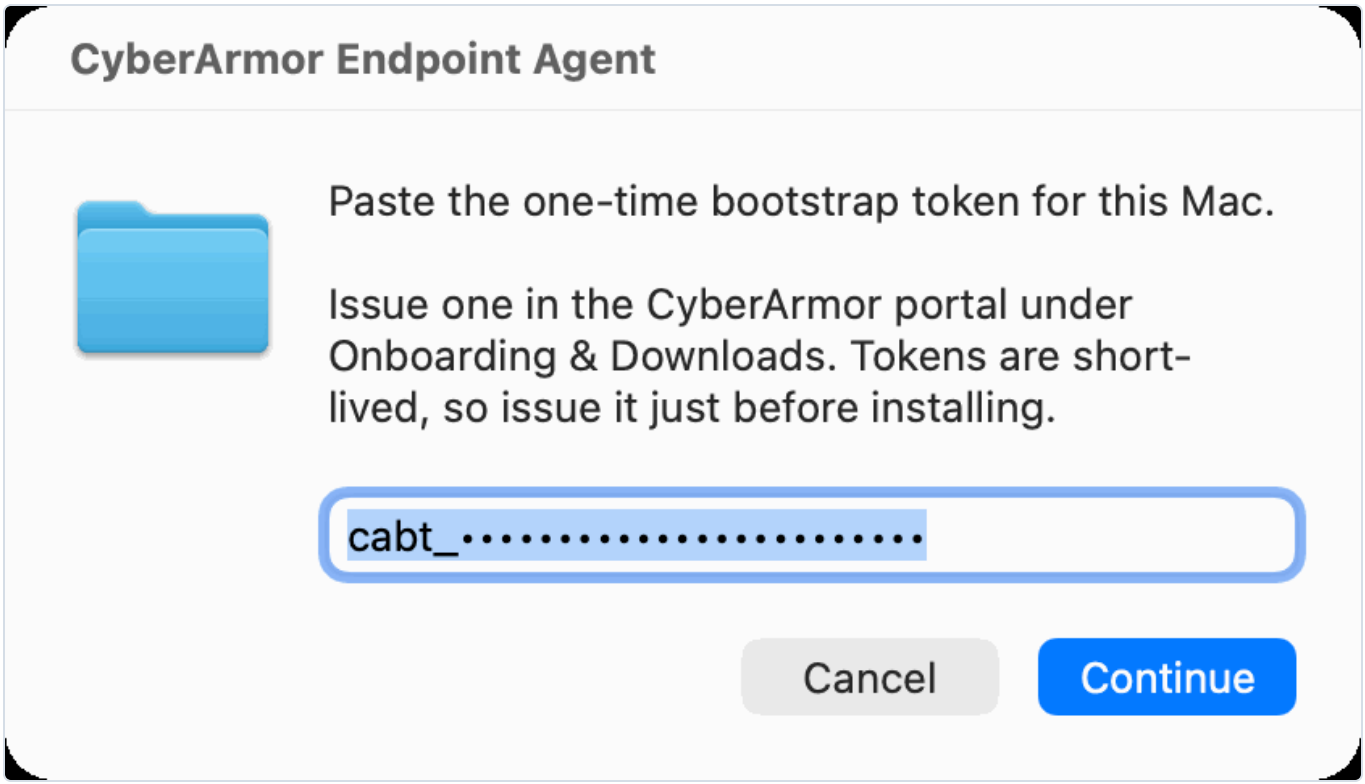


Step 6. Connect to your organization. During installation, three questions pop up, each titled `CyberArmor Endpoint Agent`.

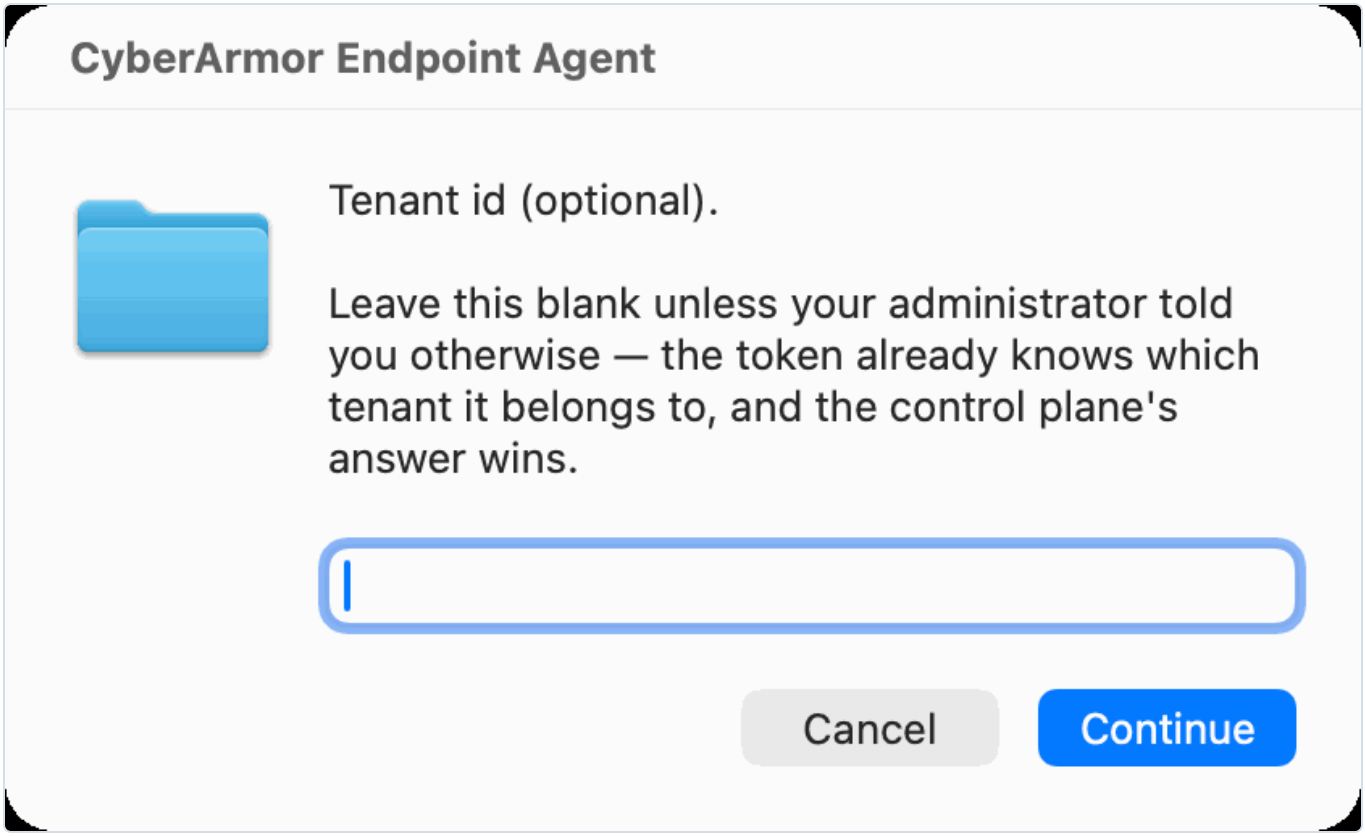
1. **The server.** `Which CyberArmor server does this Mac report to?` has three buttons and nothing pre-selected: **United States (app.cyberarmor.ai)**, **Singapore (am-app.cyberarmor.ai)** and **My organisation's server**. In Asia and the Middle East click **Singapore**. **My organisation's server** asks one more question, your own server's address, which must start with `https://`. (The picture shows the earlier installer, which had a box to type in.)



2. **Paste the one-time bootstrap token for this Mac.** Paste the token from Part A, step 4 and click **Continue**.



3. **Tenant id (optional).** Leave it empty and click **Continue**: the token already knows your organization.



If the token was mistyped or has expired, the installer offers **Try Again**, **Install Without Enrolling** or **Cancel Install**. Issue a fresh token in the portal and choose **Try Again**.

Step 7. Wait for **The installation was successful** (usually 1–3 minutes), then click **Close**. A CyberArmor.AI shield appears in the menu bar.

Step 8. Approve kernel-level monitoring (only if you kept it selected). macOS will not switch it on until you approve it: open **System Settings** → **General** → **Login Items & Extensions**, find the CyberArmor.AI extension, and turn it **on**.

Step 9. Grant Full Disk Access. Do this whether or not you kept kernel-level monitoring. Without it the agent cannot read your Documents, Downloads and Desktop folders, so files saved there are never scanned.

macOS lists the *program* the agent runs as, not the product name, so there is no "CyberArmor.AI" entry to switch on. Add the agent's own Python binary by path:

1. Open **System Settings** → **Privacy & Security** → **Full Disk Access**.
2. Click **+** at the bottom of the list, and enter your Mac password when asked.
3. Press ⇧⌘**G**, type `/usr/local/cyberarmor/.venv/bin/` and press Return.
4. Select **python3**, click **Open**, and make sure its switch is **on**.
5. Restart the agent, because the new permission does not reach the process that is already running: `sudo launchctl kickstart -k system/ai.cyberarmor.endpoint`
6. Confirm it worked by asking the agent: `/usr/local/cyberarmor/cyberarmor-status`. Under **Monitors**, `endpoint.monitoring_health` should read `[ ok ]` and name the folders it is watching.

Check it that way rather than running the disk-access test yourself from a Terminal window. macOS attributes a file request to the program that is *responsible* for it, which for anything you launch from Terminal is Terminal — so the test can report a failure while the agent itself is reading those folders perfectly well. The agent runs under launchd and is responsible for its own requests, so its report is the one that reflects reality.

If a `python3` entry is already switched on, it is not necessarily ours: other software installs its own copy of Python, and the switch belongs to whichever binary was added. Add the path above regardless.

Step 10. Finish AI traffic inspection (only if you kept it selected). Click the CyberArmor.AI shield in the menu bar and choose **Finish setting up protection…**. Enter your Mac password when asked; this trusts a local certificate and turns on the local proxy. One or two of the dialogs say **security** rather than CyberArmor.AI, because macOS names the system tool making the change rather than the application that asked for it.

Step 11. Check it works. Click the shield: the first line should read `CyberArmor — Protected`. If your organization allows pausing, a row below reads `AI apps and websites: on`, followed by how many of the Mac's network connections go through it, for example `(3 of 5 network connections)`. If the first line reads `CyberArmor — Partly on`, the reason is on the lines beneath it. The Mac also appears in the portal under **Inventory** → **Endpoints**, with health **Healthy**, within a few minutes.

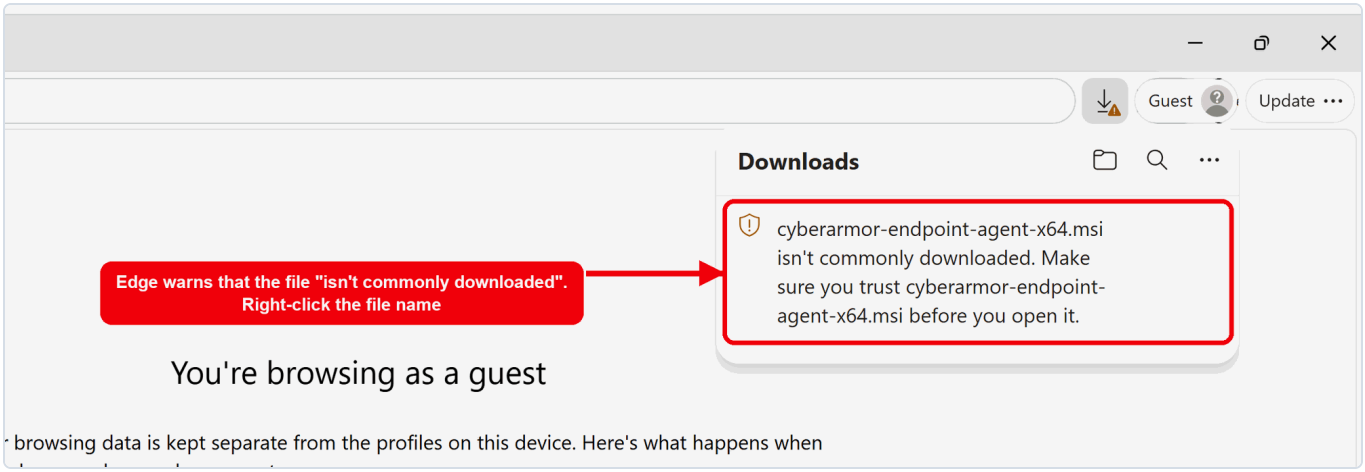
Fleet installation (IT teams): the Mac card in the portal has a copyable Terminal command that writes the server address, tenant and token to a settings file the installer reads, and runs the installer without questions, which is suitable for device-management tools. Paste the token in place of `<paste-token-here>`.

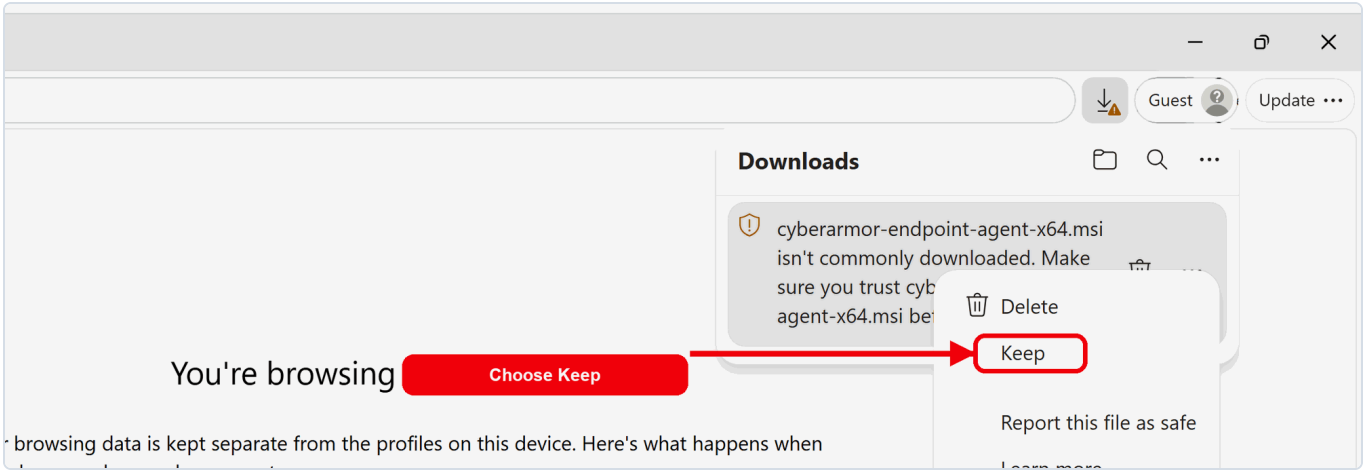
Uninstalling: the installer's last page, and the instructions it saves on the Mac, name the uninstall command, `/usr/local/bin/cyberarmor-uninstall`. Run it as your own user, not with `sudo`: it asks for administrator rights once.

Part D. Windows (beta)

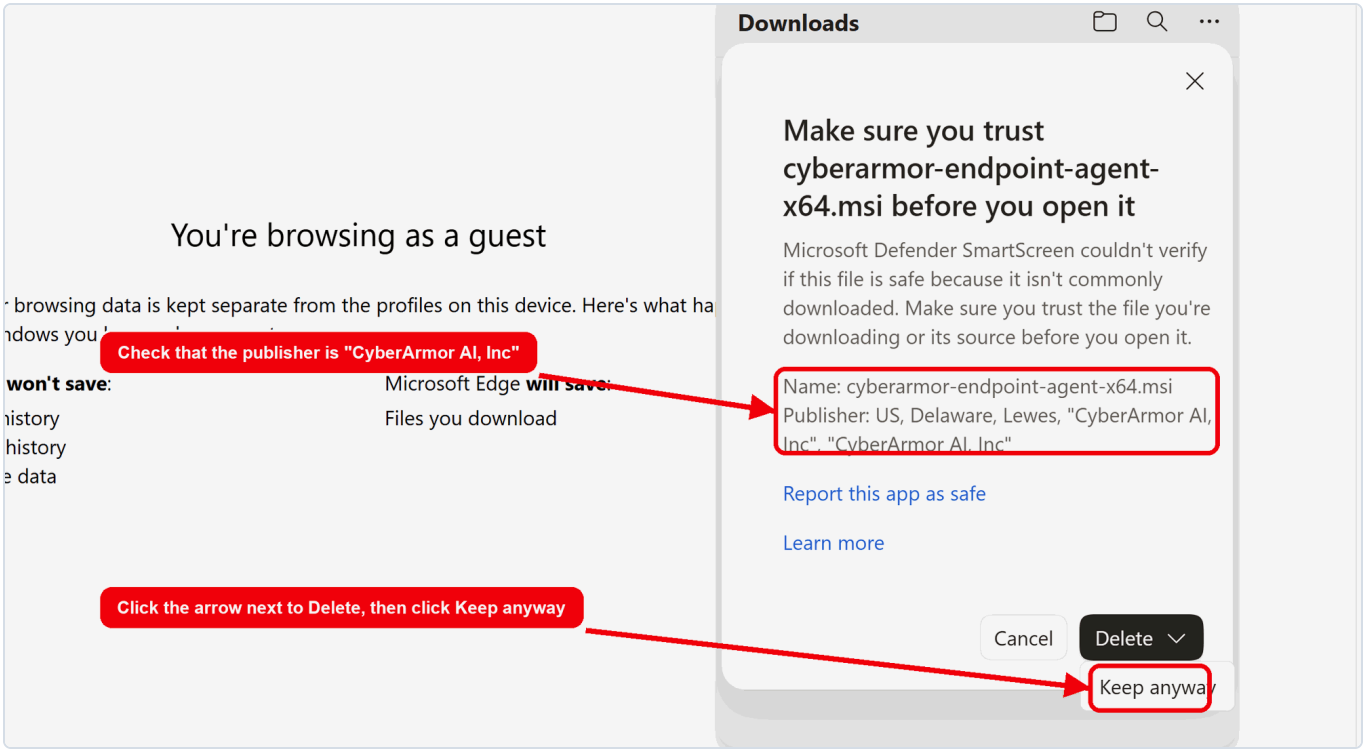
64-bit Windows; our testing is on Windows 11. You need an administrator account on the PC. The pictures show Microsoft Edge.

Step 1. Download the MSI. In our test on 2026-10-29, Edge downloaded the signed MSI from the portal without any warning. If your browser does warn that the file "isn't commonly downloaded", this is expected for a new installer: right-click the file name in the **Downloads** panel and choose **Keep**.

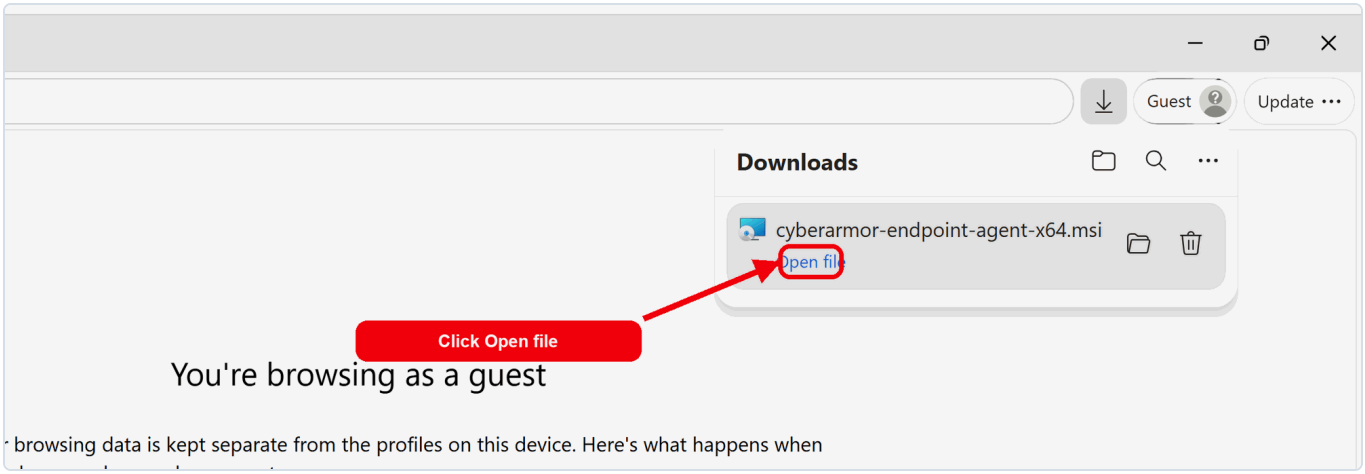




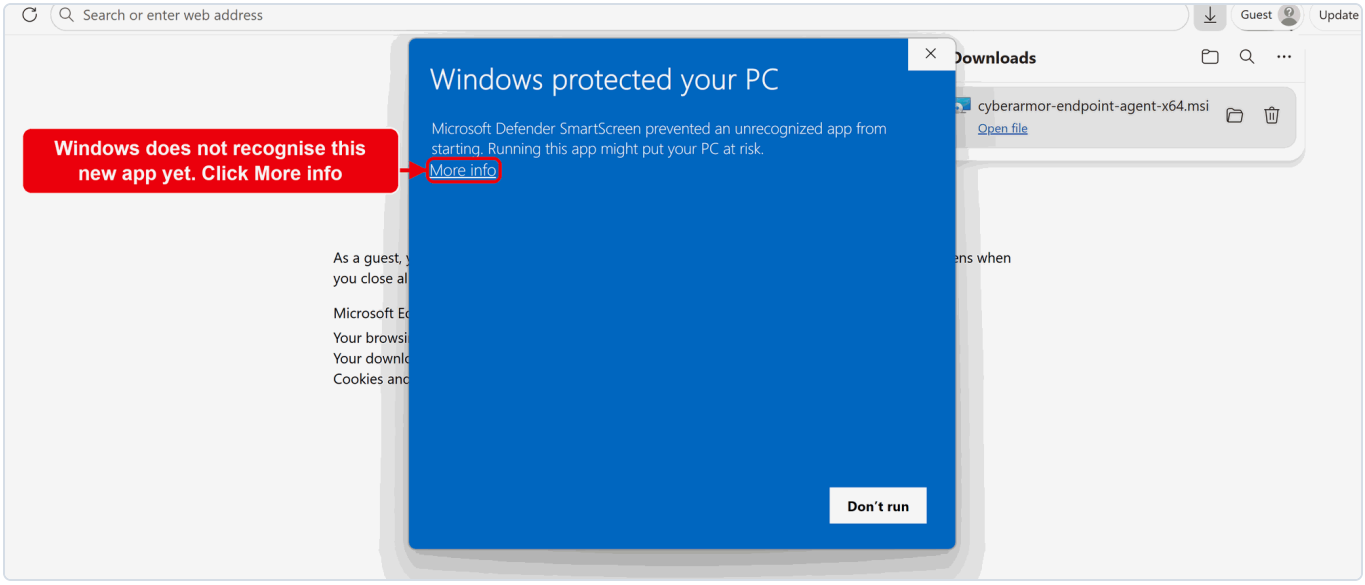
If Edge then asks you to make sure you trust the file, check that the publisher says **CyberArmor AI, Inc**, click the small arrow next to **Delete** and choose **Keep anyway**.



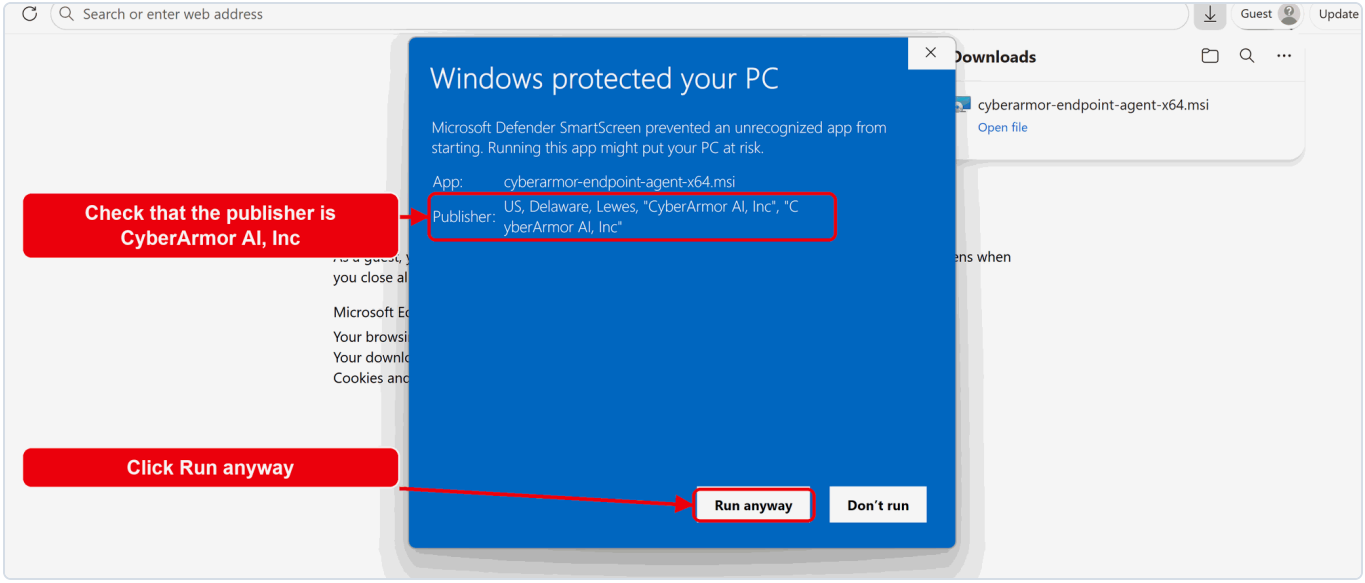
Step 2. Click **Open file**, or double-click the MSI in your Downloads folder.



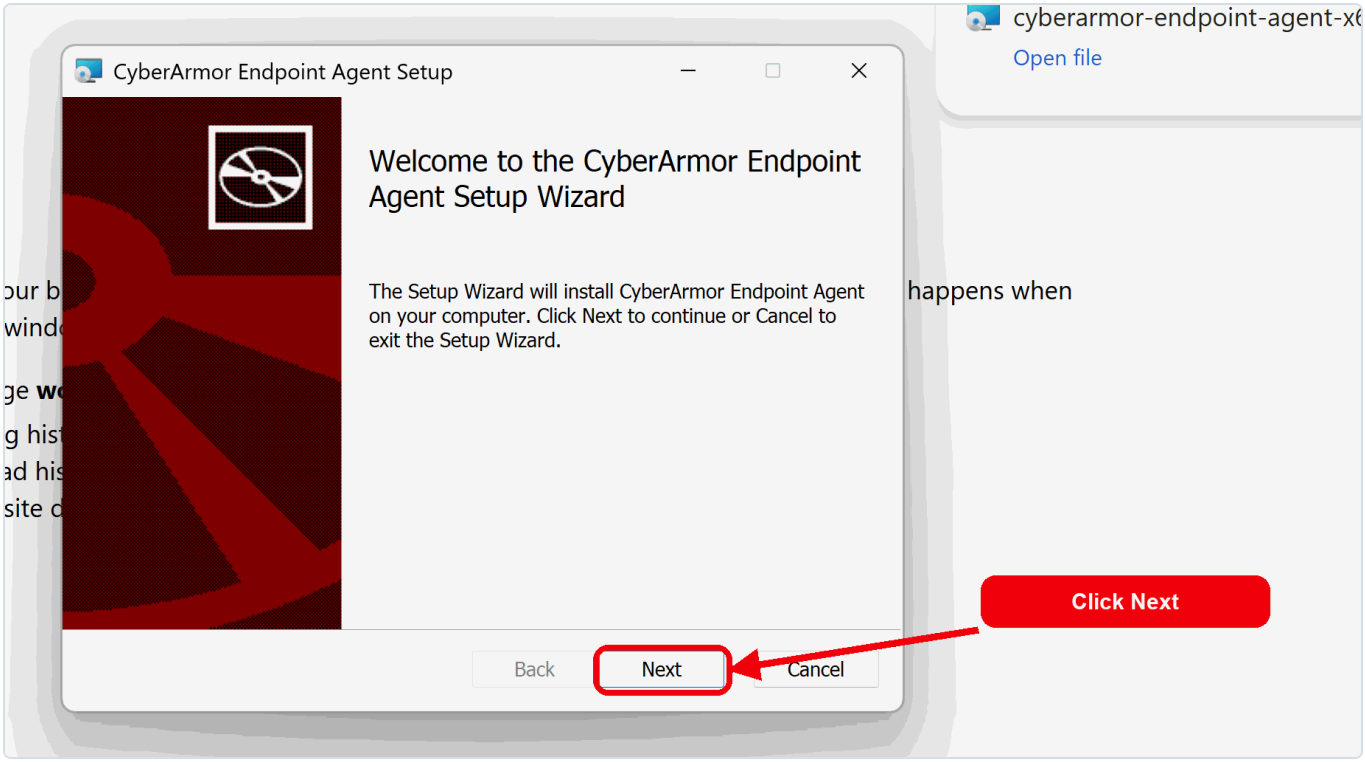
Step 3. If "Windows protected your PC" appears. SmartScreen may show this blue screen for apps it has not seen many times yet. It did not appear on 2026-10-29, but it can. If it does, click **More info**...



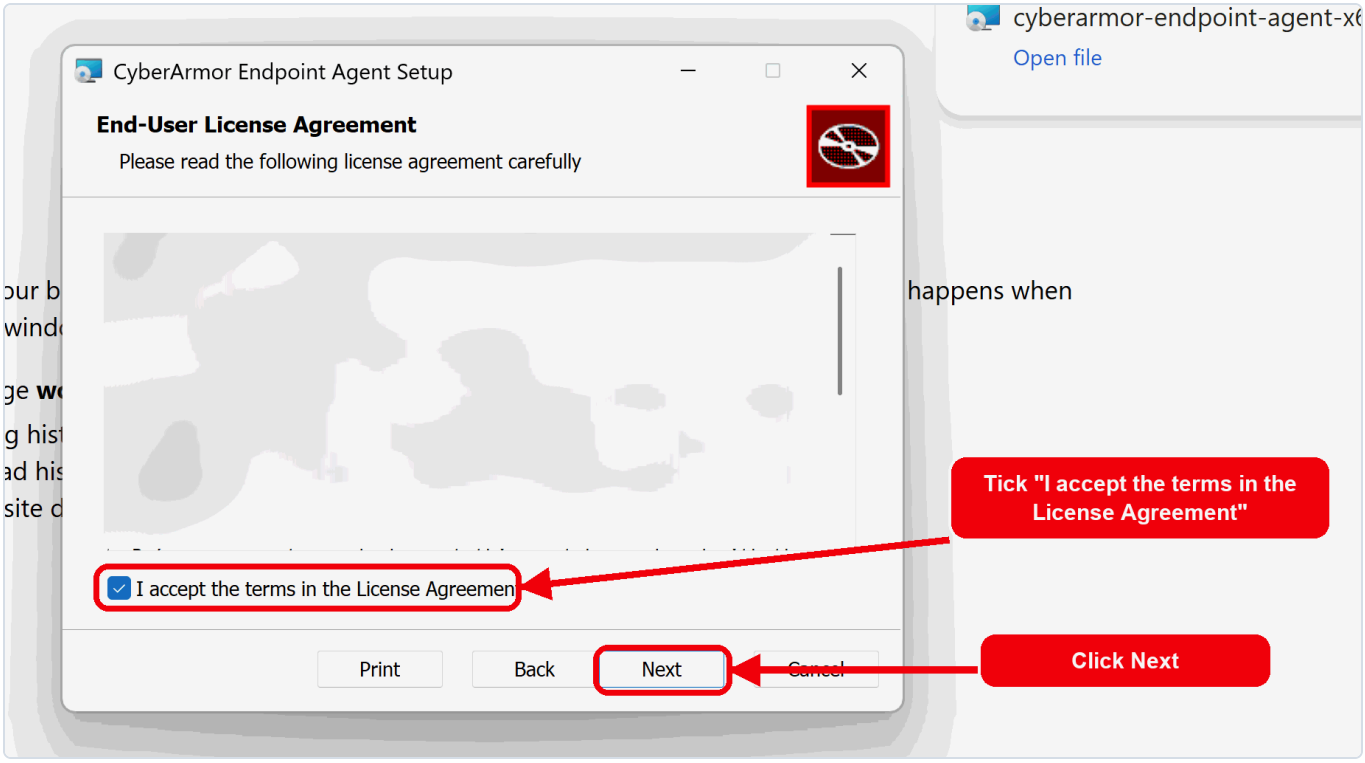
...check that the publisher is **CyberArmor AI, Inc**, and click **Run anyway**.



Step 4. Welcome. The `CyberArmor Endpoint Agent Setup` wizard opens. Click **Next**.



Step 5. License. Accept the license agreement and click **Next**.

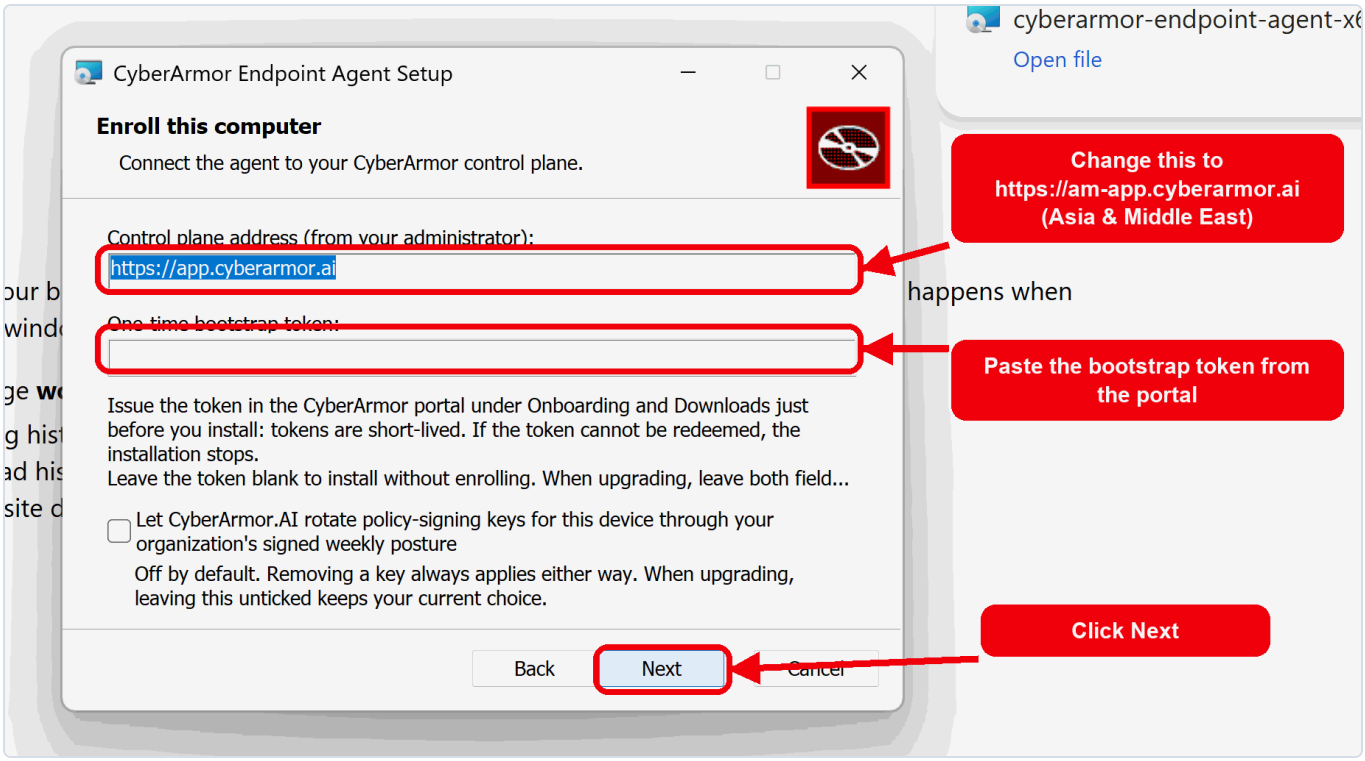


Step 6. Enroll this computer. `Which CyberArmor server does this computer report to?` has three choices and nothing pre-selected: **United States (app.cyberarmor.ai)**, **Singapore (am-app.cyberarmor.ai)** and **My organisation's server** (type its `https://` address in the box below it). The installer will not continue without a server.

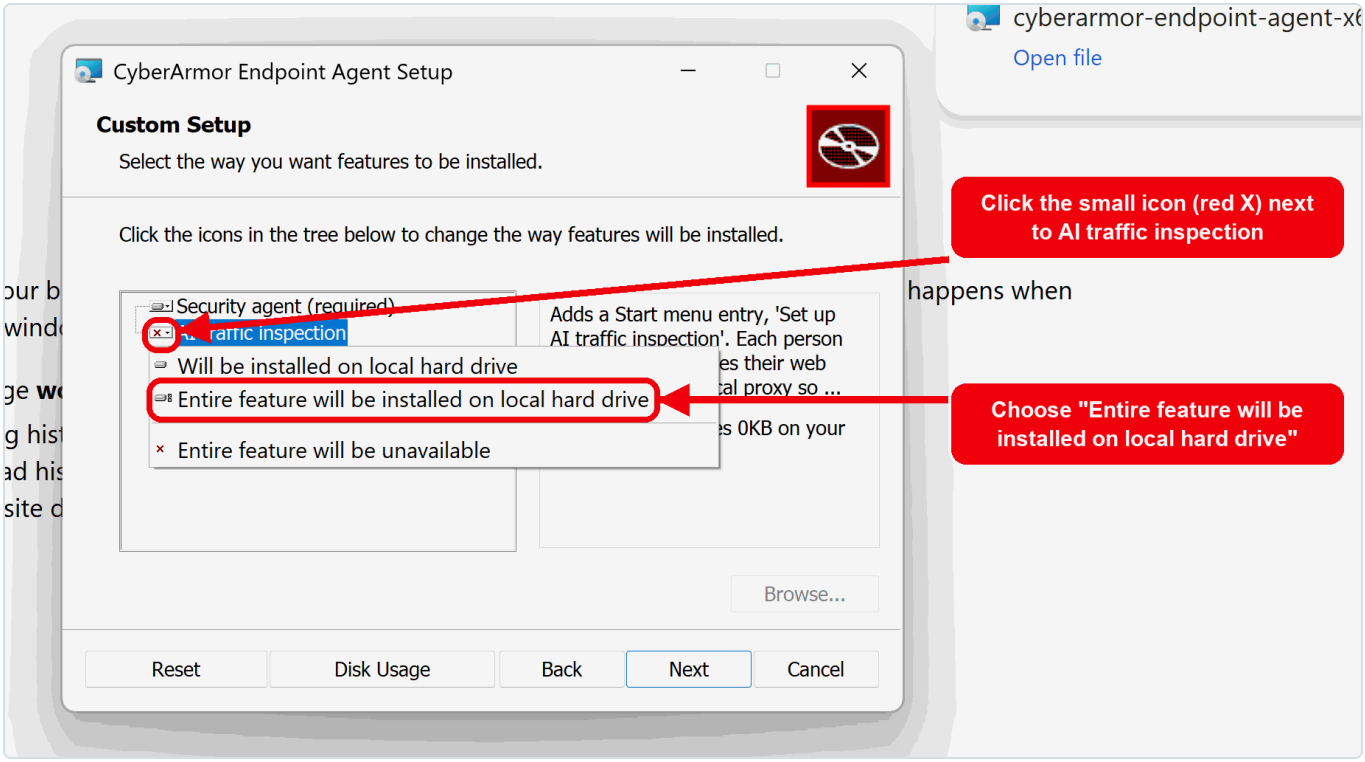
Then:

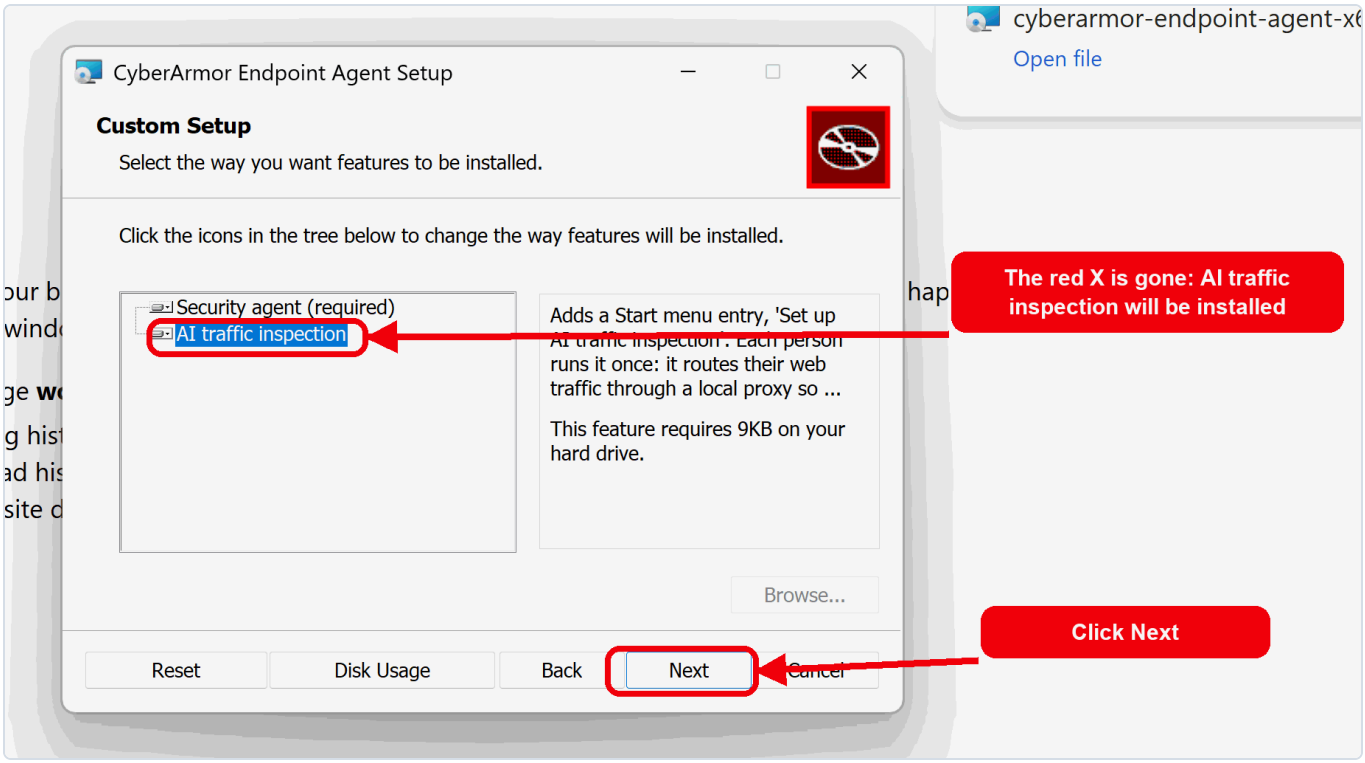
- **One-time bootstrap token:** paste the token from Part A, step 4.
- Leave the box about rotating policy-signing keys unticked unless your administrator tells you otherwise.

Click **Next**.

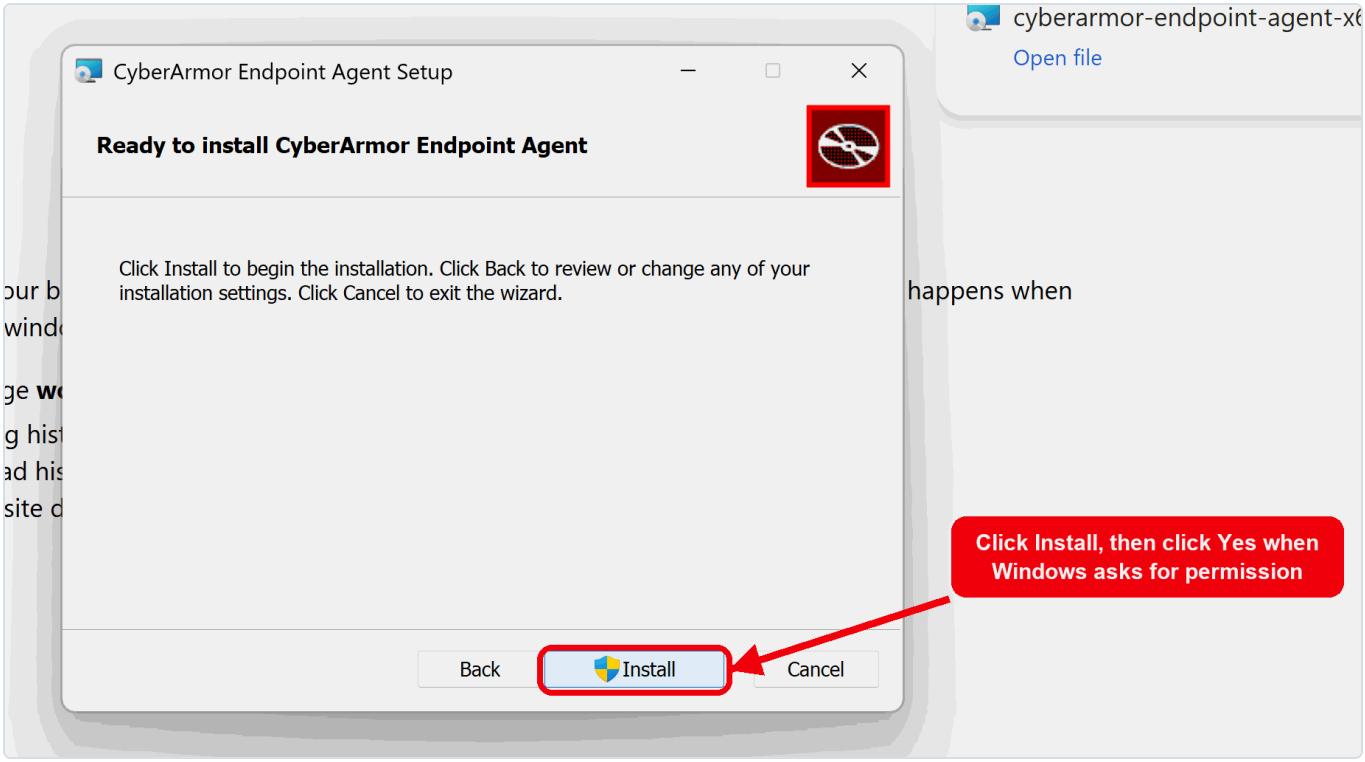


Step 7. Nothing to choose. After **Next** the installer goes straight to **Ready to install**. Every protection is installed, including **AI traffic inspection**. To leave a part out, click **Back** once on that page: **Custom Setup** opens, where **Security agent (required)** is fixed and **AI traffic inspection** can be switched off, or on again, from the small icon next to it. The two pictures below show Custom Setup; you will not see it unless you click **Back**.





Step 8. Install. Click **Install**, then click **Yes** when Windows asks whether to allow changes (User Account Control). Installation takes 1–3 minutes; click **Finish** at the end.



Step 9. Finish AI traffic inspection. Open the **Start menu**, find **Set up AI traffic inspection** (in the `CyberArmor` folder) and run it. A **CyberArmor.AI** box explains the certificate: click **OK**. Click **Yes** when Windows asks to allow changes, and **Yes** again when it asks you to trust the certificate issued by **CyberArmor.AI Local Proxy CA**. A final box says whether setup finished. The account must be a local administrator. Each person who signs in to this PC does this once. (The 1.0.18 installer has no first box and no final box: it opens a console window and asks only about the certificate.) On a PC set up with an agent from 1.0.13-rc.15 or earlier, running it again replaces the older certificate, named **mitmproxy**: Windows asks to trust the new one, then asks once more to delete the old one; click **Yes** both times.

Step 10. Check it works. In the portal, open **Inventory** → **Endpoints**. On 2026-10-29 the PC appeared with health **Healthy** within a minute of the installation, and about 4 minutes later its row showed AI traffic **Enforced** and **Filter set up for** this organization.

The CyberArmor.AI tray icon is in the notification area. Windows usually puts it in the overflow: click **^** next to the clock to see it. If it is not there, run `CyberArmor Status (Windows)` from the `CyberArmor` folder in the Start menu.

Upgrading later: run the newer MSI as administrator and leave the enrollment fields empty. Do not uninstall first and do not issue a new token: the existing connection is kept.

Unattended installation (IT teams): the MSI takes `CONTROL_PLANE_URL`, `BOOTSTRAP_TOKEN` and `ACCEPT_EULA=YES` on the `msiexec` command line. Without a server address it refuses a new installation rather than guess one.

If something goes wrong

What you see	What to do
The token is refused or "expired"	Tokens last 30 minutes and work once. Issue a new one in the portal and try again.
The installer cannot reach the server	Check the address is exactly `https://am-app.cyberarmor.ai` (Asia and Middle East) or `https://app.cyberarmor.ai` (United States), or your own server's address, and that the computer can open that address in a browser.
The extension's buttons do nothing	Click **I agree: connect and send this data** first: nothing connects until you do.

What you see	What to do
The device does not appear in Endpoints	Wait 5 minutes and refresh. If it is still missing, open the menu-bar or tray icon and use **Copy all details**, then send them to your administrator.
Back on a block page keeps showing the block page	Update the extension to the current version; earlier versions could loop back to the blocked page.
Websites stop loading on a Mac after installing	Choose **Pause protection…** from the menu-bar icon (if your organization allows pausing), then contact your administrator.
Websites stop loading on a Windows PC after setting up AI traffic inspection	Contact your administrator. Removing the **AI traffic inspection** feature (**Settings** → **Apps**, then **Modify** on `CyberArmor Endpoint Agent`) restores the proxy settings of the person removing it.
Anything else	In the portal, open **Support** → **Help & FAQ**, or watch the installation video listed at the top of this guide.