CyberArmor.AI 安装指南 — Windows、Mac 与 Chrome

最后核验时间：2026-10-29。全文已对照 `main` 分支提交 1f4497db6 的代码逐节核对。步骤 9 中的证书名称读取自 `install_local_proxy.sh` 与 `install_local_proxy.ps1`（2026-10-29）；尚未在包含该更改的设备上实际看到这些对话框。D 部分（Windows）于 2026-10-29 在一台干净的 Windows 11 计算机上完整执行：使用从美国门户（app.cyberarmor.ai）下载的已签名 1.0.13-rc.15 MSI，该执行早于上述证书改名。C 部分步骤 8–11：于 2026-10-26 在一台干净的 macOS 26 虚拟机上，对接新加坡生产环境门户（am-app.cyberarmor.ai）、版本 1.0.13-rc.12，完整执行了全流程——代理安装并注册至 `cn-demo-bank` 租户，按路径授予完全磁盘访问权限，重启守护进程后 `cyberarmor-status` 报告 `[ ok ] endpoint.monitoring_health`，完成本地代理配置后报告 `CyberArmor — 已保护`，且 AI 流量检查已开启。浏览器扩展部分描述的是扩展 2.3.20。截图拍摄于 2026-10-24；如图片与正文不一致，以正文描述为准。

本指南介绍如何将一台计算机接入贵组织的 CyberArmor.AI 服务。共有三种方式，您可以在同一台计算机上同时使用多种方式：

安装内容	适用场景	耗时	是否需要计算机的管理员密码?
浏览器扩展（Chrome、Edge、Brave）	最快捷的入门方式。**仅保护您实际安装了扩展的那些浏览器配置文件**——Chrome、Edge、Brave 彼此独立，同一浏览器内的每个配置文件（Profile）也彼此独立（见 B 部分步骤 7）。	每个配置文件约 3 分钟	否
Mac 代理程序	为 Mac 提供完整防护，包括桌面端 AI 应用。	约 5 分钟	是
Windows 代理程序（测试版）	为 64 位 Windows PC 提供完整防护。	约 5 分钟	是

开始之前，您需要具备：

1. 客户门户的登录权限：**https://am-app.cyberarmor.ai**（亚洲及中东地区）或 **https://app.cyberarmor.ai**（美国）。请参阅**客户门户用户指南**第 1 节。如果贵组织运行自己的 CyberArmor.AI 服务器，凡本指南提到门户地址之处，请改用管理员或合作伙伴提供的地址。
2. 可签发安装令牌的角色：**Deployer**（部署员）、**Analyst**（分析员）或 **Tenant admin**（租户管理员）。

所有安装方式都遵循相同的三个步骤：

下载 → 获取一次性令牌 → 安装并粘贴令牌

想看视频? 培训视频《安装：从登录到受保护的计算机》（约 9 分钟）在一台计算机上演示了本指南的每一个步骤。视频位于文档站点 **https://docs.cyberarmor.ai/zh/training/customer-walkthrough/**、**https://cyberarmor.ai/training**，以及客户门户的**支持 → 帮助与常见问题 → 培训视频**。视频目前为英语（巴基斯坦）版。

A 部分：获取安装程序与令牌（所有计算机通用）

步骤 1. 登录 **https://am-app.cyberarmor.ai**，在菜单中点击**设置与管理 → 接入与下载**。

步骤 2. 请记下页面顶部的两项信息：

- （1）**控制平面**地址 `https://am-app.cyberarmor.ai`；安装过程中需要选择或输入该地址；
- 贵组织的 **ID**，例如 `cyberarmorasia`；浏览器扩展会要求填写该 ID。



步骤 3. 下载对应的文件：

- **Chrome、Edge 或 Brave 扩展：** 在页面顶部标题为 **CyberArmor.AI Protect** 的*推荐入门方式*区域点击**下载 ZIP** →（3）。
- **Mac：** 向下滚动至**终端代理**（Endpoint Agent）分组。在 **CyberArmor.AI Endpoint Agent——macOS 安装程序（PKG，已签名并经过公证）**卡片上点击**下载 PKG**。（**CyberArmor.AI Endpoint Agent——macOS 磁盘映像（DMG）**卡片提供的是装在磁盘映像中的同一安装程序。）
- **Windows：** 在 **CyberArmor.AI Endpoint Agent——Windows 安装程序（MSI，测试版）**卡片上点击**下载 MSI**。



步骤 4. 在同一张卡片上点击**签发引导令牌**。令牌会显示在页面顶部。点击**复制**。

- 一个令牌只能接入**一台**计算机。
- 令牌将在 **30 分钟**后过期：请在即将安装前再签发。
- 请像对待密码一样处理令牌：切勿通过邮件发送。

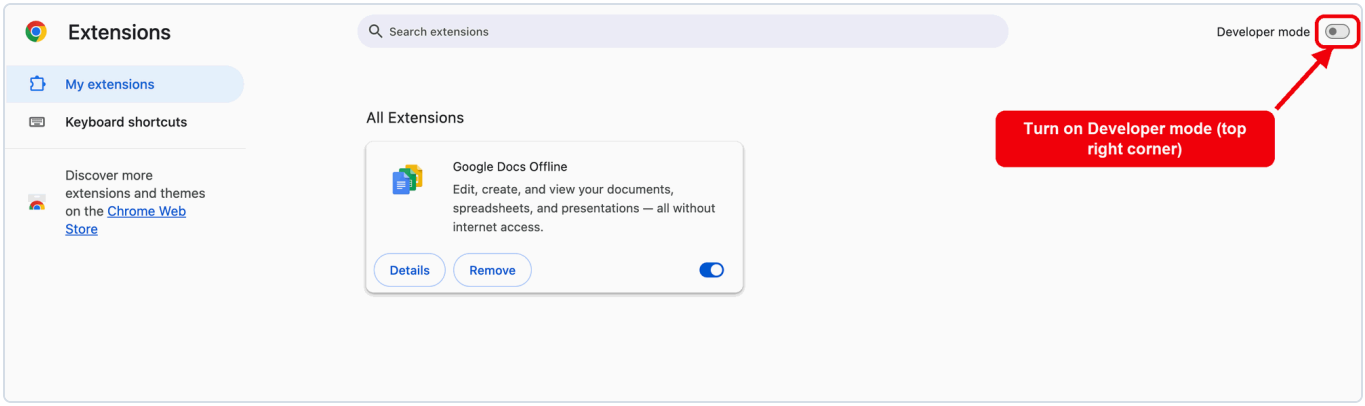


B 部分：浏览器扩展：Chrome、Edge 与 Brave

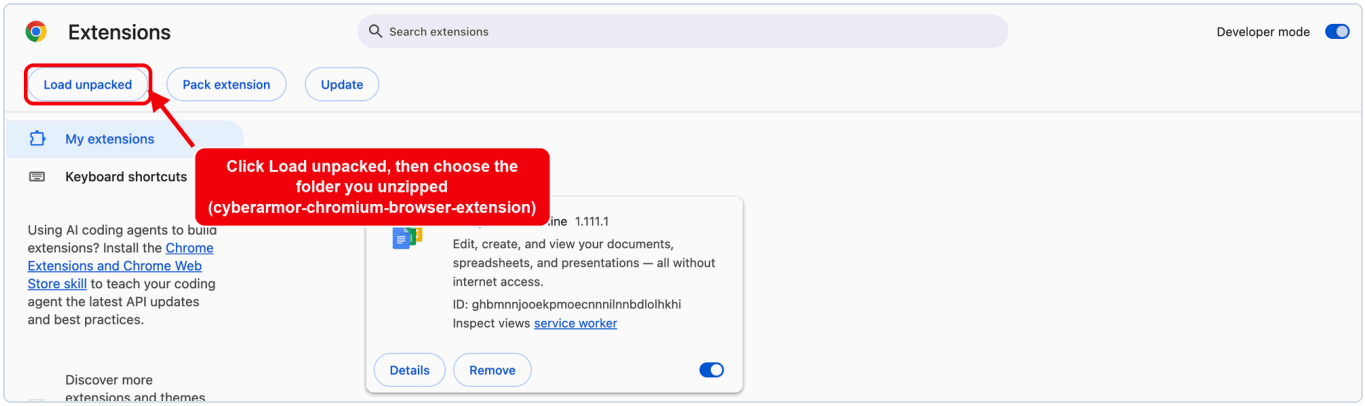
该扩展名为 CyberArmor.AI Protect，版本 2.3.20，通过门户中的 ZIP 文件安装；目前尚未在 Chrome 应用商店、Edge 加载项商店或 Firefox 附加组件网站上架。在 Microsoft Edge 中请使用 `edge://extensions`*，在 Brave 中请使用* `brave://extensions`*，替代本部分中的* `chrome://extensions`*。*

步骤 1. 在"下载"文件夹中找到已下载的 `cyberarmor-chromium-browser-extension.zip` 文件并解压（Mac 上双击即可；Windows 上右键点击 → **全部解压缩**）。解压后会得到一个名为 **cyberarmor-chromium-browser-extension** 的文件夹。请保留该文件夹：浏览器将从中加载扩展程序。

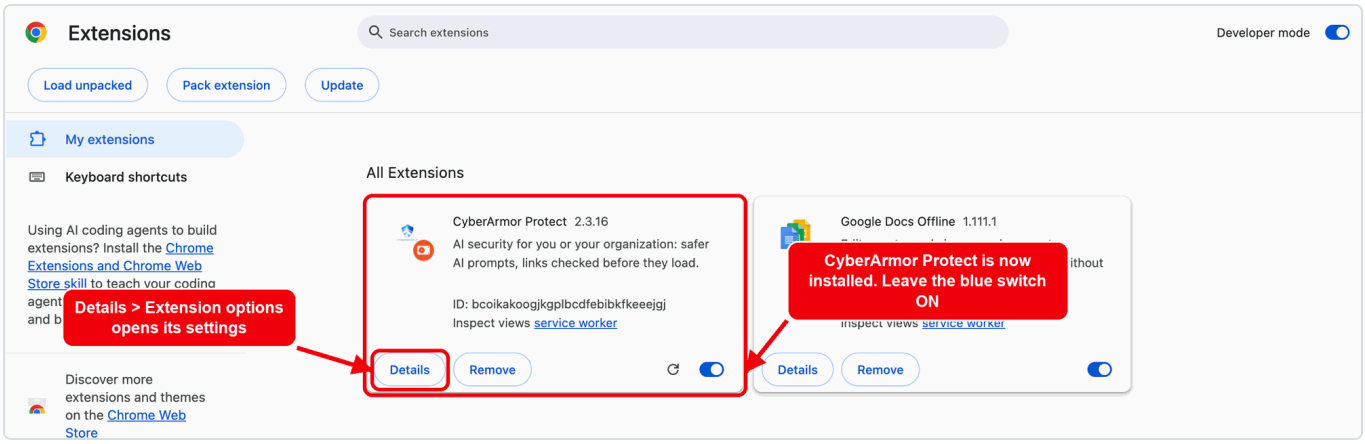
步骤 2. 在 Chrome 地址栏中输入 `chrome://extensions` 并按回车。打开右上角的**开发者模式**。



步骤 3. 界面上会出现三个新按钮。点击**加载已解压的扩展程序**，选择您刚才解压出的 **cyberarmor-chromium-browser-extension** 文件夹，然后点击**选择**。



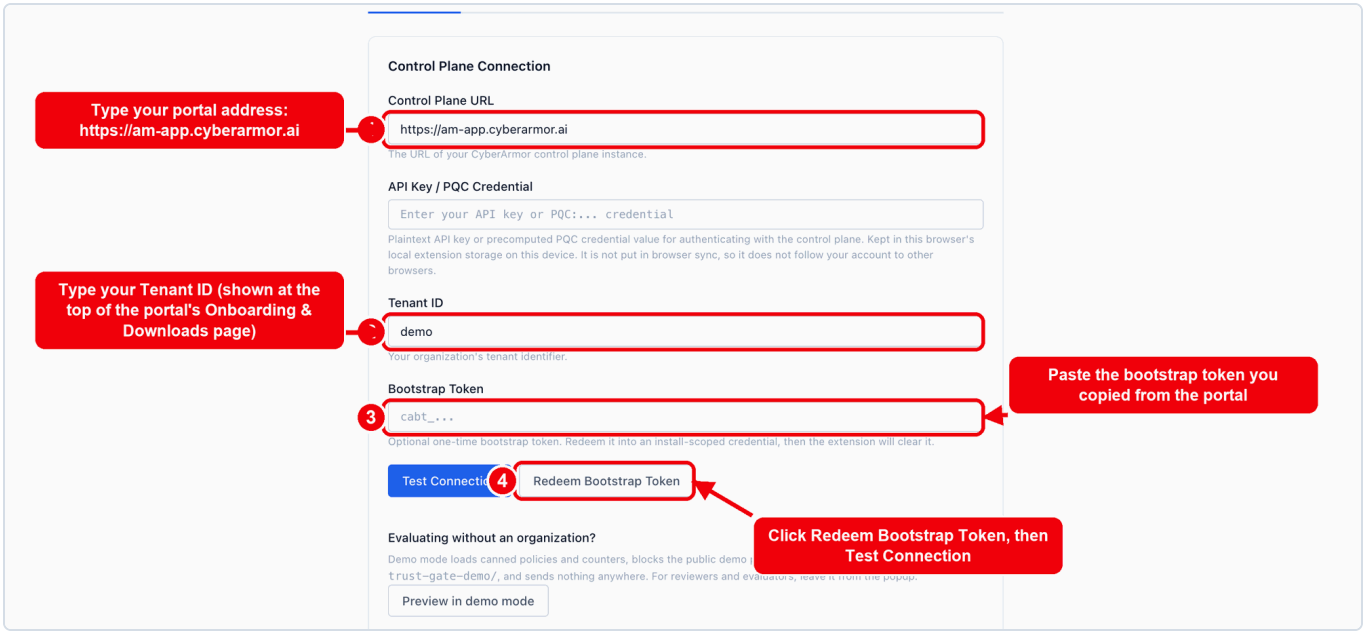
步骤 4. CyberArmor.AI Protect 随即出现在列表中。请确认其开关已开启（显示为蓝色）。点击**详情**，向下滚动并点击**扩展程序选项**。小提示：点击工具栏中的拼图图标，将 **CyberArmor.AI Protect** 固定在工具栏上，方便随时查看。



步骤 5. 先同意，再连接。 设置页面打开在**连接**（Connection）选项卡上。

1. 阅读 **Before you connect: what CyberArmor.AI Protect sends**（连接之前：CyberArmor.AI Protect 会发送哪些内容）。它列出了扩展连接后会发送的内容，并说明这些内容只发送到贵组织的 CyberArmor.AI 服务器：您打开的每个页面的地址（不含"?"之后的部分）、在组织策略要求时您发送给 AI 服务的提示词文本和上传给它们的文件、扩展所警告、脱敏或拦截的记录，以及本浏览器的注册身份。**在您同意之前，什么都不会发送。**点击 **I agree: connect and send this data**（我同意：连接并发送这些数据）。
2. **Server address (required)**（服务器地址，必填）。该字段不会预先填写。在亚洲及中东地区点击 **Singapore (am-app.cyberarmor.ai)**，在美国点击 **United States (app.cyberarmor.ai)**。如果贵组织运行自己的服务器，请点击 **My organisation's server**，并输入以 `https://` 开头的服务器地址。
3. **Tenant ID**（租户 ID）：输入您在门户中查到的组织 ID（A 部分步骤 2）。
4. **Bootstrap Token**（引导令牌）：粘贴您此前复制的令牌（A 部分步骤 4）。
5. 点击 **Redeem Bootstrap Token**（兑换引导令牌）。兑换成功后，点击 **Test Connection**（测试连接）。

在您点击同意之前，扩展会拒绝兑换令牌、测试连接或保存服务器地址。您的同意只记录在本浏览器中。



步骤 6. 验证是否生效。 访问任意网站。约 30 秒内，门户**接入与下载**页面上的**租户信号**会变为绿色，该浏览器也会出现在**资产清单 → 终端**中。

如需主动查看一次拦截页面，请打开 **https://aitrustlab.org/url-trust-gate-demo/**。该站点存放 URL Trust Gate 演示页面：其中的攻击页面会被拦截，`benign.html` 则会放行。（这些页面以前位于 `app.cyberarmor.ai/url-trust-gate-demo/`，该旧地址现在返回 **410 Gone**；请更新书签。）

步骤 7. 在每一个浏览器、每一个浏览器配置文件中重复一遍

这一步决定了扩展到底能不能起到保护作用，请不要跳过。

浏览器扩展只存在于某一个浏览器之中，并且只存在于该浏览器的**某一个配置文件（Profile）**之中。Chrome 把每个配置文件都当作独立的浏览器，各自管理自己的扩展列表。因此：

- 在 Chrome 中装好，对 Edge 或 Brave 没有任何作用。
- 在工作配置文件中装好，对**同一台电脑上**的个人配置文件没有任何作用。
- 在您完成部署之后新建的配置文件，在有人手动为它安装之前，是没有扩展的。

请在**员工实际用于 AI 的每一个浏览器、以及其中的每一个配置文件**中重复步骤 1 至 6。「装上、同意、配置好、连接成功」缺一不可——扩展虽然在列表里，但从未完成**同意**与**兑换引导令牌**，同样不能保护该配置文件。

没有安装扩展的配置文件，不是「保护得少一些」，而是完全没有保护；并且那个界面上不会有任何提示告诉使用者这一点。 门户也无法列出一个从未上报过的配置文件，因此未部署的配置文件在门户中同样是不可见的——**资产清单 → 终端**中没有出现，并不能证明某个配置文件是安全的。

快速检查某个配置文件的方法：切换到该配置文件，打开 `chrome://extensions`，确认 **CyberArmor.AI Protect** 在列表中且开关已打开；再打开其**扩展程序选项**，确认**测试连接**可以成功。

这也正是即使已在所有浏览器中部署了扩展、仍然需要安装终端代理（C、D 部分）的原因：在设置好 AI 流量检查之后，终端代理是在整台机器的层面工作，而不是只在某一个浏览器配置文件里，因此某位员工今天早上才新建的配置文件所产生的 AI 流量同样会被覆盖。它并不能看到每一个应用程序的内部；具体覆盖范围以状态页为准。请把扩展理解为「按配置文件生效的覆盖范围」，把终端代理理解为「整机生效的覆盖范围」。

扩展连接后会做什么

某个页面上具体发生什么，由贵组织在客户门户中设定的策略决定。以下几种行为，建议在员工遇到之前先了解：

- **拦截页面。** 当策略拦截某个站点时，扩展会显示一个说明被拦截内容的页面。按**返回**，或点击页面上的 **Go Back to Safety**（返回安全页面）按钮，都会回到被拦截页面之前的那个页面。再次打开被拦截的地址仍会被拦截。
- **银行卡 PIN 码不会离开银行以外的站点。** 如果贵组织设有银行卡 PIN 码策略（见客户门户用户指南第 7 节），在银行卡号旁边输入的借记卡 PIN 码——无论是在 AI 聊天中还是在网页表单中——都会在离开浏览器之前按该策略处理。在 AI 聊天中，**redact**（脱敏）策略会在输入时移除 PIN 码，**block**（拦截）策略会阻止该消息发送。在网页表单中，表单会被暂扣：拦截策略不会发送任何内容，并显示策略名称；脱敏策略会清空 PIN 码字段、遮盖卡号并暂扣表单，让使用者看到原因。银行自己的网站是例外，而且例外只来自银行清单，绝不来自支付机构或银行卡组织。
- **私有网络地址**（通过 IP 地址打开的路由器、打印机、内网应用）会按照租户**设置 → 私有网络地址**中的选择放行、警告或拦截。扩展绝不会把这些地址发送给 CyberArmor.AI。

Firefox 与 Android 版 Firefox

门户中的 **CyberArmor.AI Protect——适用于 Firefox 的浏览器扩展**卡片提供 `cyberarmor-firefox-extension.zip`，即为 Firefox 打包的同一扩展（2.3.20）。

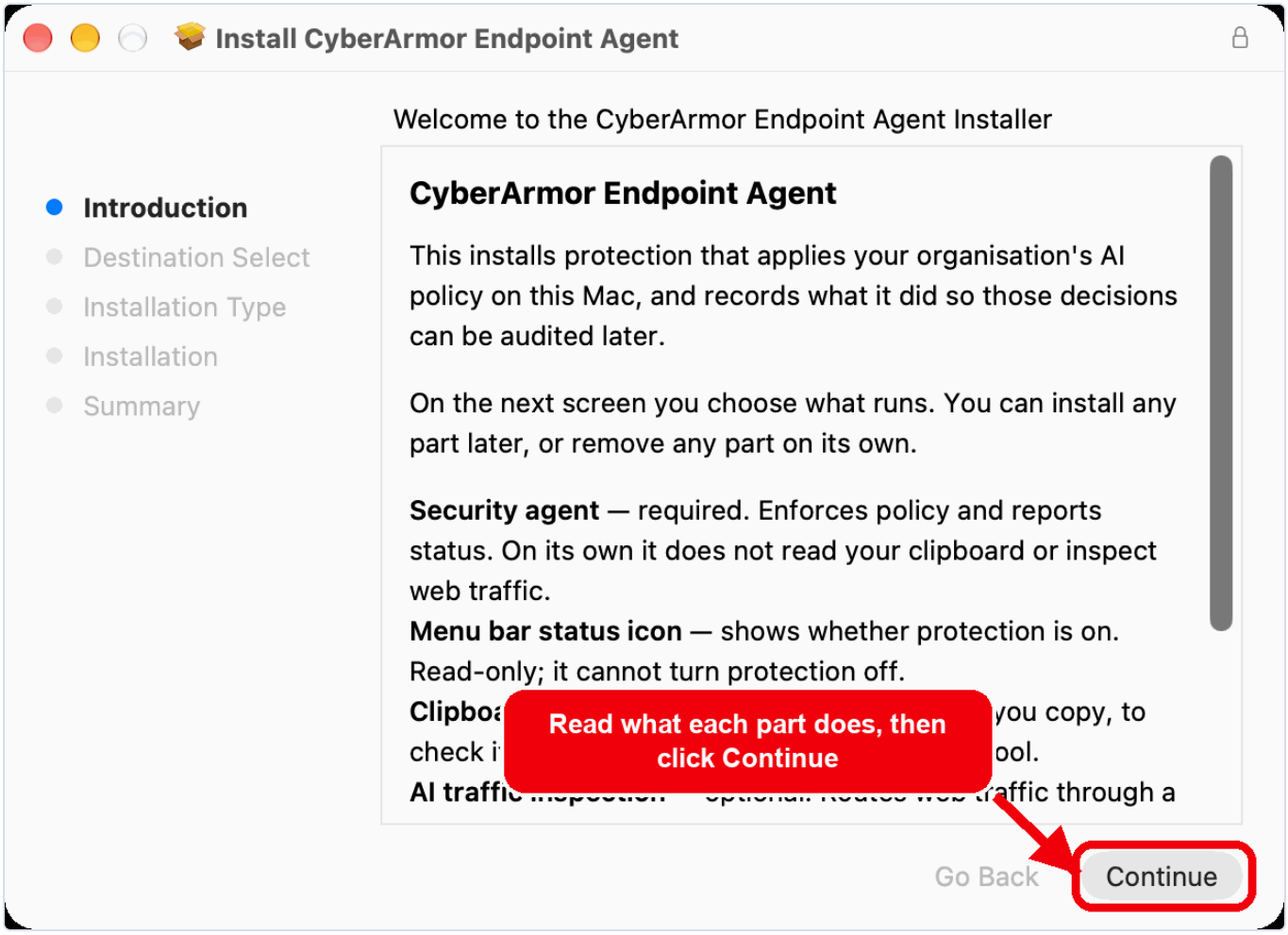
- **电脑上的 Firefox：** 打开 `about:debugging#/runtime/this-firefox`，点击**临时载入附加组件**，选择解压后文件夹中的 `manifest.json`，然后按上面的步骤 5 操作。Firefox 重启时会移除临时附加组件，因此这种方式仅适用于评估；永久安装需要该扩展在 Firefox 附加组件网站上架，目前尚未上架。
- **Android 版 Firefox：** 2.3.20 扩展包支持 Android 版 Firefox 142 及更高版本。Android 版 Firefox 只能从 Firefox 附加组件网站（addons.mozilla.org）安装扩展，而 CyberArmor.AI Protect 尚未在该网站上架。在上架之前，请向您的 CyberArmor.AI 联系人咨询如何在 Android 设备上安装。

C 部分：Mac

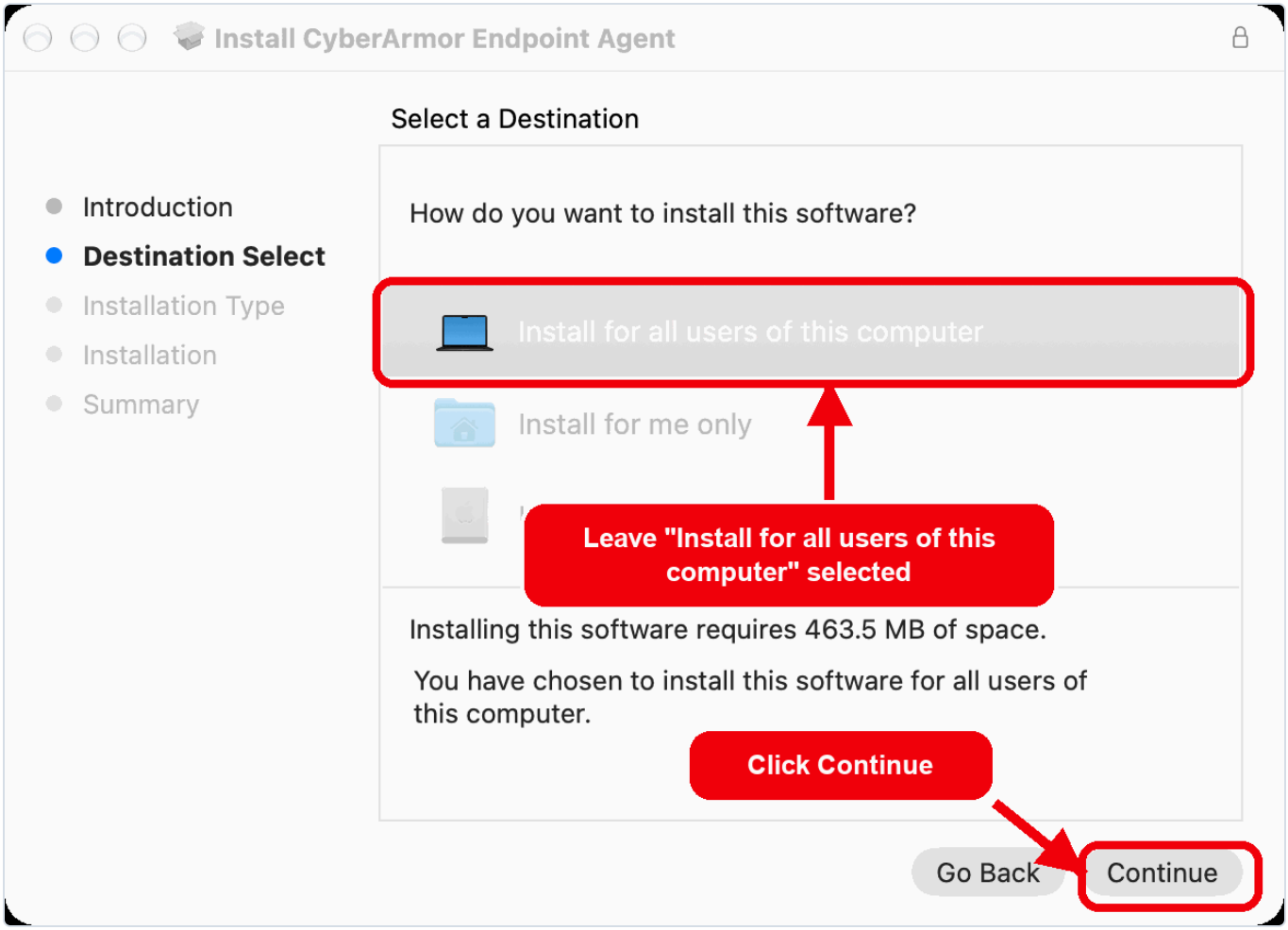
适用于搭载 Apple 芯片或 Intel 芯片的 macOS。您需要该 Mac 上管理员账户的密码。

步骤 1. 在"下载"文件夹中找到 `cyberarmor-endpoint-agent.pkg` 并双击打开。该安装程序已由 Apple 签名并公证，因此打开时不会出现警告。

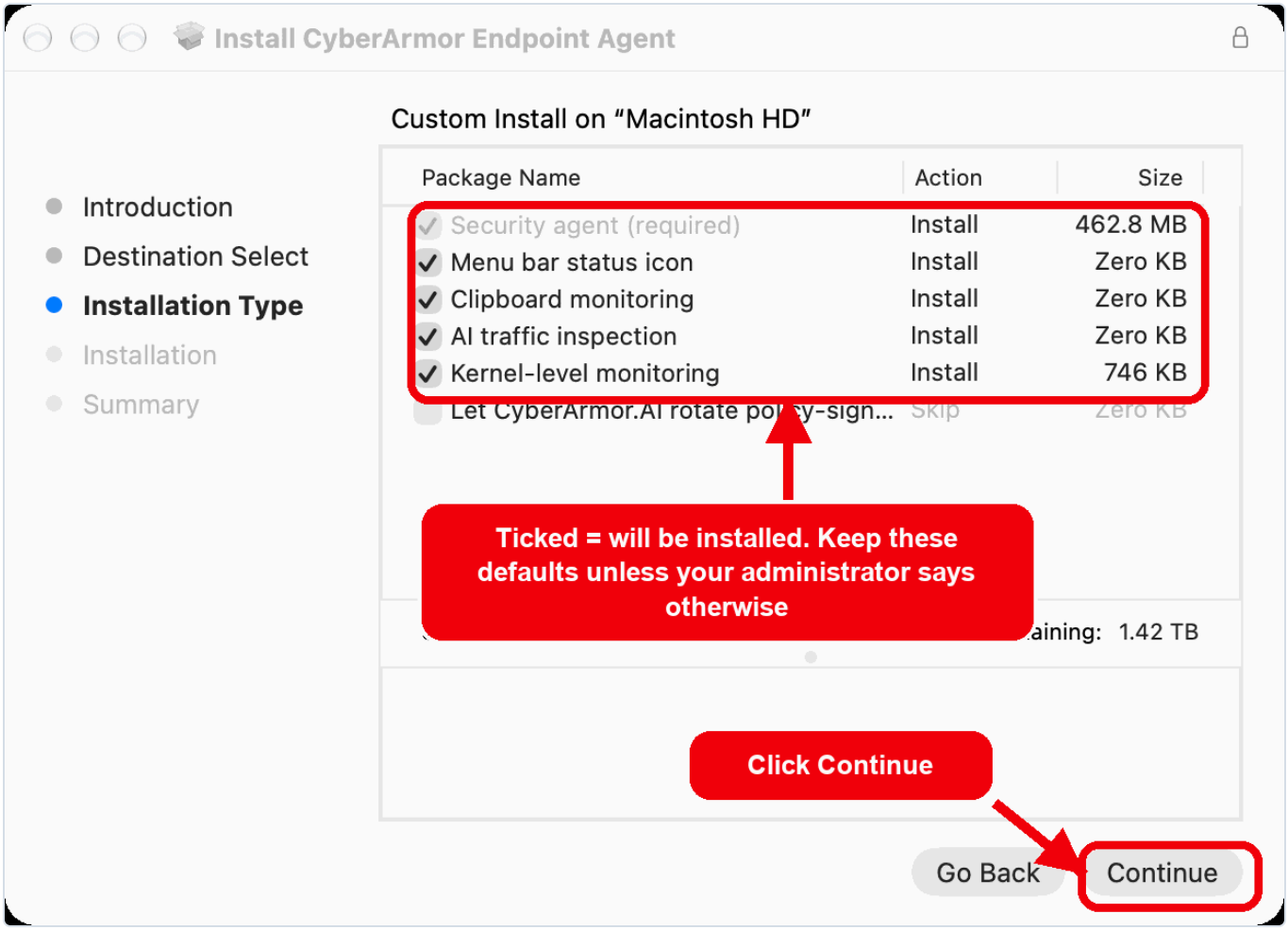
步骤 2. **简介**页面会说明软件各个组成部分的功能。阅读后点击**继续**。



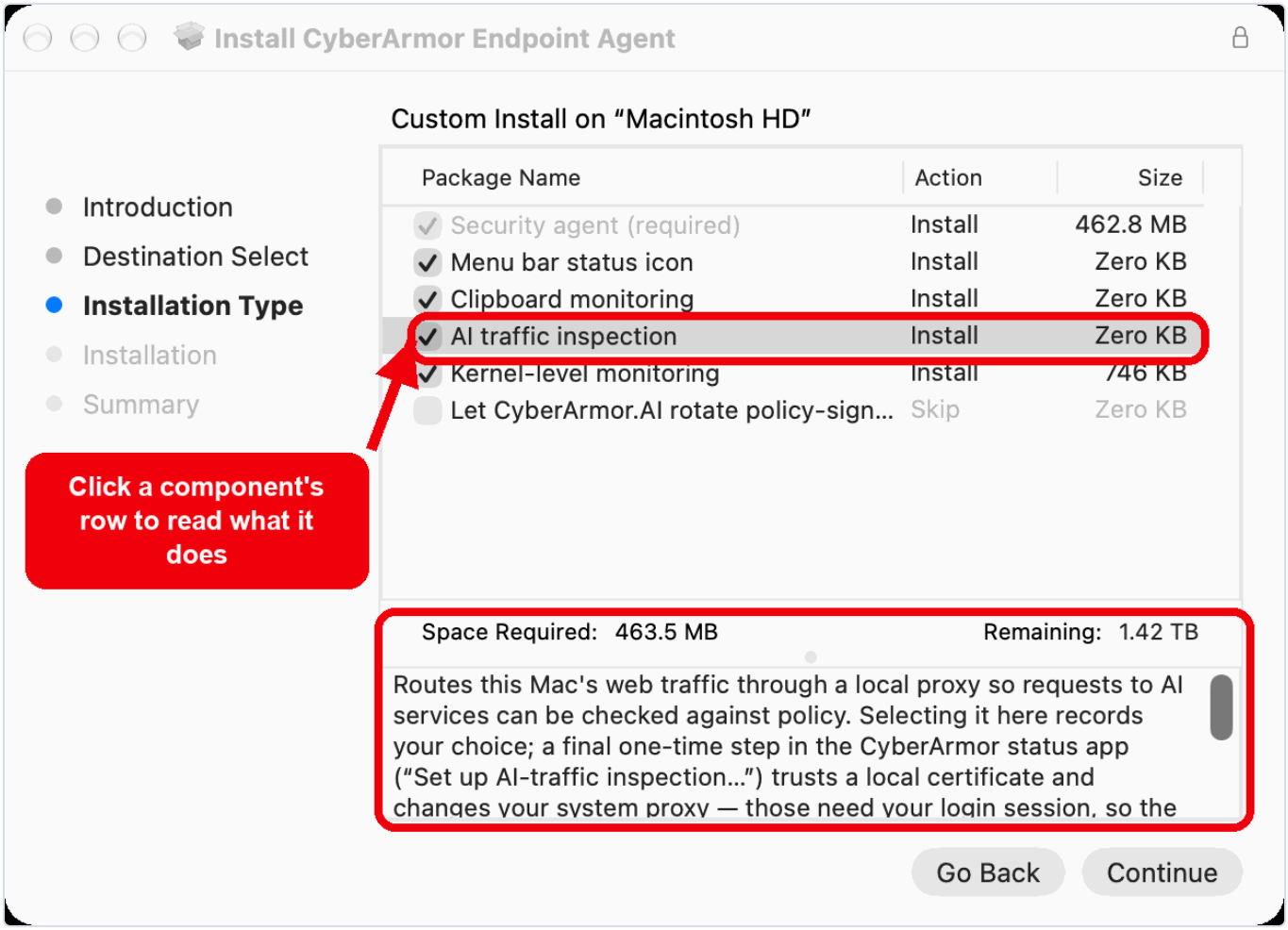
步骤 3. 在**选择安装目标**页面，保持选中**为本计算机的所有用户安装**，然后点击**继续**。（部分 Mac 会跳过此页面。）



步骤 4. 选择组件。 **安装类型**页面列出了各个组件。带勾号表示该组件将被安装。



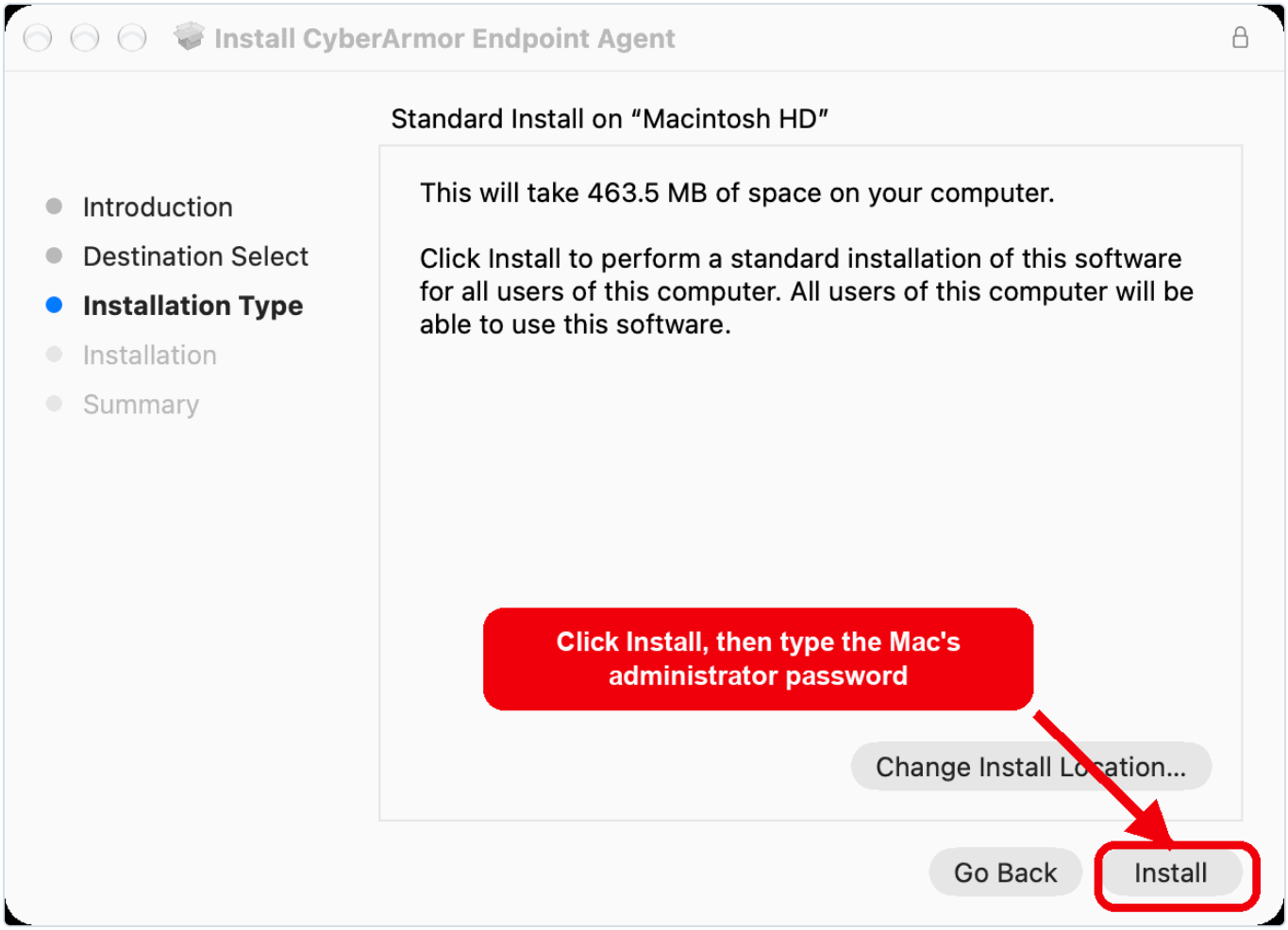
点击组件所在的行（而非其勾选框），可在下方的说明框中阅读该组件的功能说明。



组件	默认是否勾选?	功能说明
安全代理程序（必需）	始终勾选	后台服务，负责执行贵组织的 AI 策略并上报本机状态。
菜单栏状态图标	是	在菜单栏中显示防护是否已启用。该图标无法关闭防护。
剪贴板监控	是	检查您复制的内容中是否包含敏感数据，并按策略进行脱敏或清除。
AI 流量检查	是	检查发往 AI 服务的网络请求。安装后需要额外完成一个步骤（步骤 10）。
内核级监控	是	可识别桌面端 AI 应用及其读取的文件。安装后需要您手动授权（步骤 8）。
允许 CyberArmor.AI 通过贵组织每周签名的安全态势轮换本设备的策略签名密钥	否	除非管理员另行要求，否则请保持不勾选。

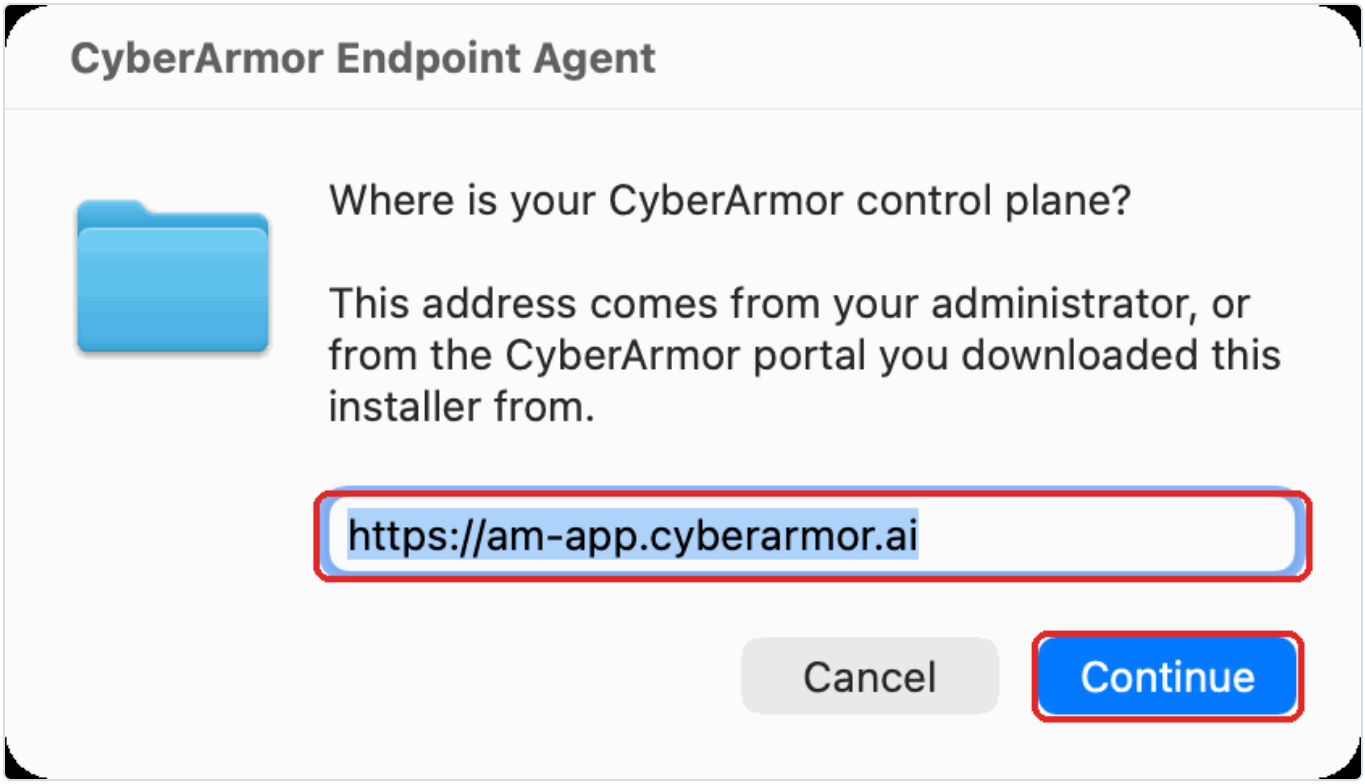
除非管理员另有说明，请保持默认设置，然后点击**继续**。

步骤 5. 点击**安装**，输入该 Mac 的管理员密码，然后点击**安装软件**。

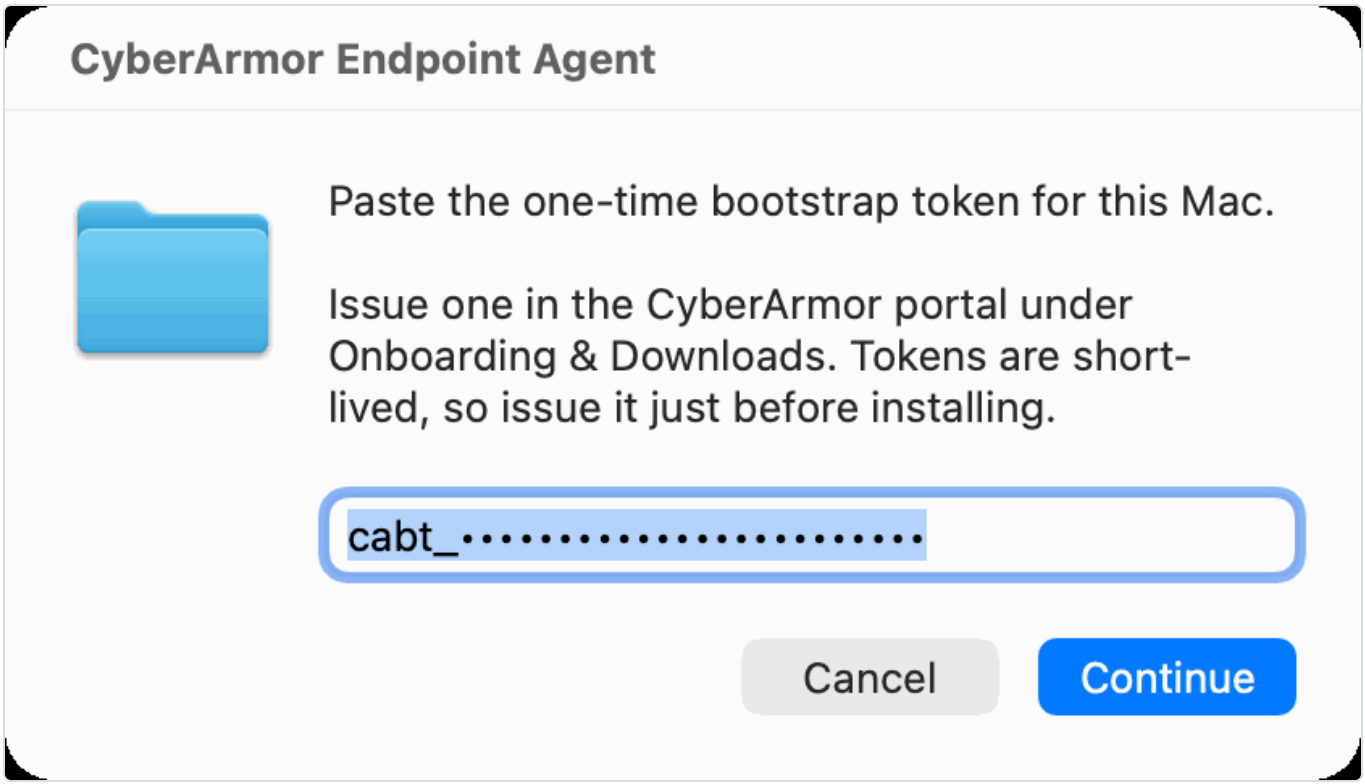


步骤 6. 接入贵组织。 安装过程中会弹出三个问题，标题均为 `CyberArmor Endpoint Agent`。

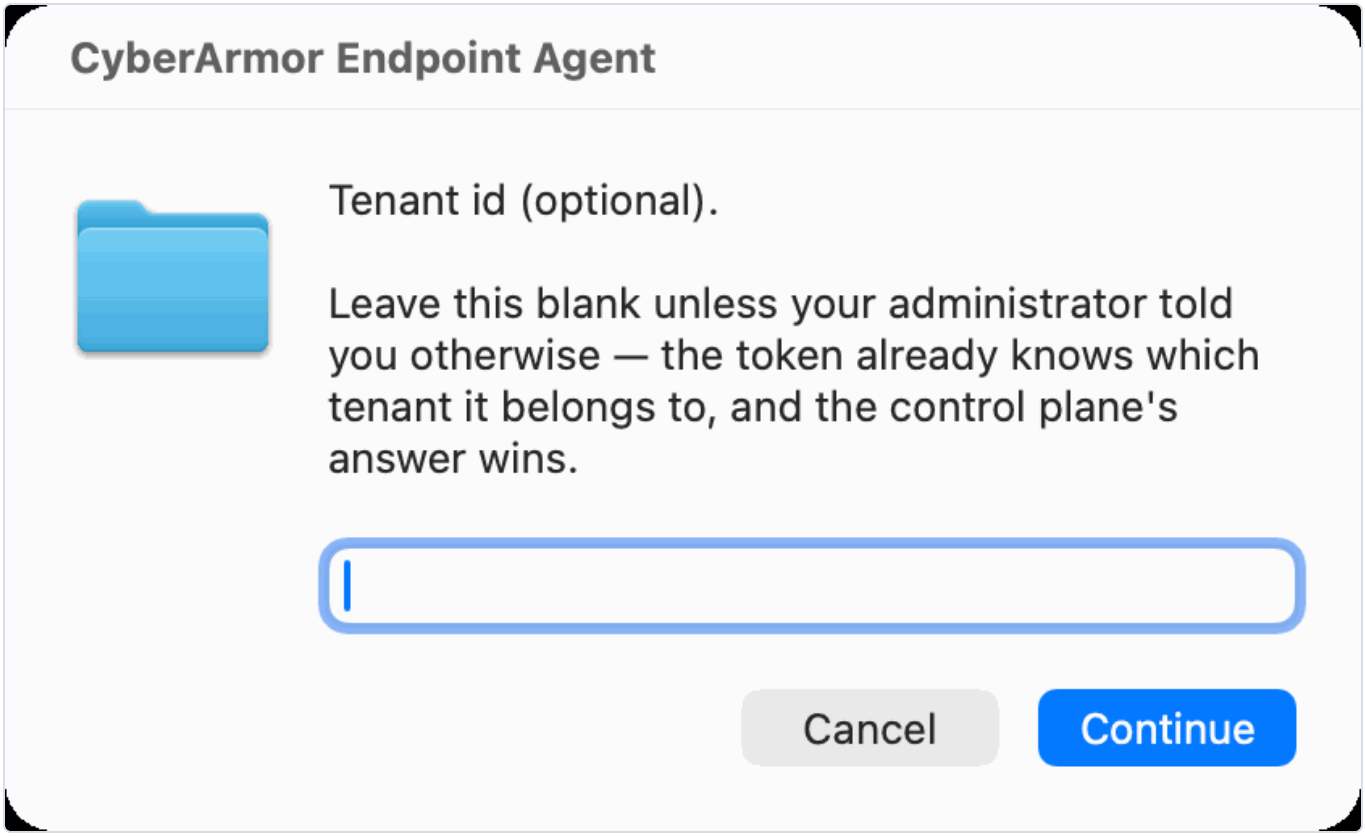
1. **服务器。** 第一个问题取决于安装程序的版本：- **1.0.13-rc.15 版本**询问 `Where is your CyberArmor control plane?`（您的控制平面地址是什么？），输入框中显示 `https://app.cyberarmor.ai`。**在亚洲及中东地区，请将其改为** `https://am-app.cyberarmor.ai`，然后点击**继续**。- **2026-10-28 之后构建的版本**询问 `Which CyberArmor server does this Mac report to?`（这台 Mac 向哪台服务器上报？），提供三个按钮且均未预选：**United States (app.cyberarmor.ai)**、**Singapore (am-app.cyberarmor.ai)** 和 **My organisation's server**。在亚洲及中东地区请点击 **Singapore**。选择 **My organisation's server** 时，需要输入以 `https://` 开头的自有服务器地址。



2. **粘贴本机的一次性引导令牌。** 粘贴 A 部分步骤 4 中获取的令牌，然后点击**继续**。



3. **租户 ID（可选）。** 请留空并点击**继续**：令牌本身已包含贵组织的信息。



如果令牌输入有误或已过期，安装程序会提供 **Try Again**（重试）、**Install Without Enrolling**（不注册直接安装）或 **Cancel Install**（取消安装）三个选项。请在门户中签发新的令牌，然后选择**重试**。

步骤 7. 等待出现**安装成功**提示（通常需要 1–3 分钟），然后点击**关闭**。菜单栏中会出现 CyberArmor.AI 盾牌图标。

步骤 8. 授权内核级监控（仅当您保留了该组件时需要）。macOS 在您授权之前不会启用该功能：打开**系统设置** → **通用** → **登录项与扩展**，找到 CyberArmor.AI 扩展并将其**开启**。

步骤 9. 授予完全磁盘访问权限。 无论是否保留内核级监控，都需要完成此步骤。未授予时，代理无法读取您的「文稿」「下载」和「桌面」文件夹，保存在这些位置的文件不会被扫描。

macOS 在此列表中显示的是代理所运行的**程序**，而非产品名称，因此**没有名为 CyberArmor.AI 的条目可供开启**。请按路径添加代理自带的 Python 程序：

1. 打开**系统设置** → **隐私与安全性** → **完全磁盘访问权限**。
2. 点击列表底部的 **+**，按提示输入您的 Mac 密码。
3. 按 **⇧⌘G**，输入 `/usr/local/cyberarmor/.venv/bin/` 并回车。
4. 选择 **python3**，点击**打开**，并确认其开关处于**开启**状态。
5. 重启代理，因为新授予的权限不会作用于已在运行的进程：`sudo launchctl kickstart -k system/ai.cyberarmor.endpoint`
6. 通过代理自身的报告来验证：运行 `/usr/local/cyberarmor/cyberarmor-status`，在 **Monitors** 一节中，`endpoint.monitoring_health` 应显示 `[ ok ]`，并列出它正在监控的文件夹。

请使用上述方式验证，而不要自行在「终端」中运行磁盘访问检测程序。macOS 会把文件访问请求归属于**发起该请求的责任进程**；凡是从「终端」启动的程序，责任进程都是「终端」本身——因此即使代理本身能够正常读取这些文件夹，该检测仍可能报告失败。代理由 launchd 启动，对自己的请求负责，所以它给出的报告才反映真实情况。

如果列表中已有一个 `python3` 条目处于开启状态，它未必是本产品的：其他软件也会安装自己的 Python，该开关属于当初被添加的那个程序。无论如何，请按上述路径添加。

步骤 10. 完成 AI 流量检查配置（仅当您保留了该组件时需要）。点击菜单栏中的 CyberArmor.AI 盾牌图标，选择**设置 AI 流量检查…**。按提示输入您的 Mac 密码；此操作将信任一份本地证书并启用本地代理。其中一两个对话框显示的名称是 **security** 而非 CyberArmor.AI，这是因为 macOS 显示的是执行该变更的系统工具，而不是发起请求的应用程序。所信任的证书名为 **CyberArmor.AI Local Proxy CA**。如果这台 Mac 是用 1.0.13-rc.15 或更早版本的代理程序完成设置的，再次运行此操作会替换其旧证书（名为 **mitmproxy**）：先信任新证书，待代理使用新证书运行后再移除旧证书。完成后请打开一个新的“终端”窗口。

步骤 11. 验证是否生效。 点击盾牌图标，应显示 `CyberArmor — Protected`（已保护），以及一行 `AI-traffic inspection: on`（AI 流量检查已开启），后面注明本机有多少个网络服务经由它转发。几分钟内，该 Mac 也会出现在门户的**资产清单** → **终端**页面中，健康状态显示为**健康**（Healthy）。

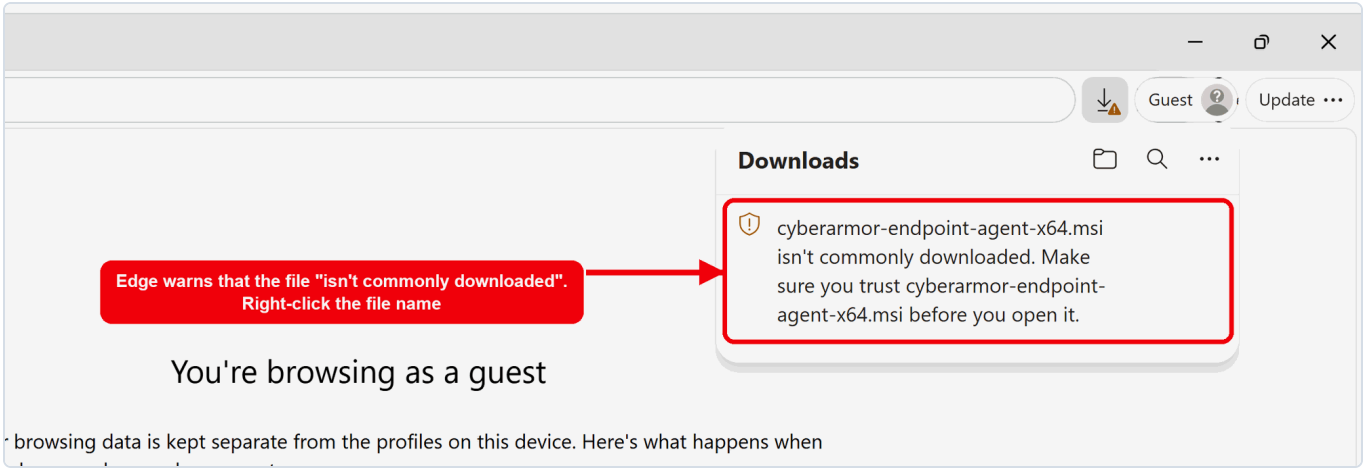
批量安装（IT 团队）： 门户中的 Mac 卡片提供一条可复制的终端命令，该命令会将服务器地址、租户和令牌写入安装程序读取的设置文件，并以无交互方式运行安装程序，适合配合设备管理工具使用。请用令牌替换命令中的 `<paste-token-here>`。

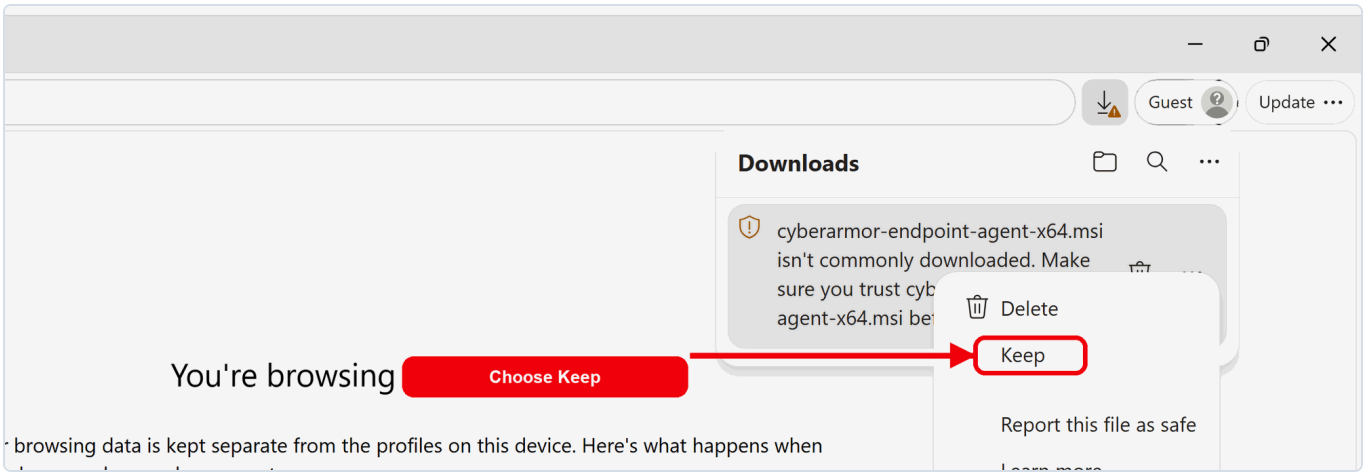
卸载： 安装程序的最后一页及其保存在本机的说明中写明了卸载命令 `/usr/local/bin/cyberarmor-uninstall`。请以您自己的用户身份运行，不要加 `sudo`：它只会请求一次管理员权限。

D 部分：Windows（测试版）

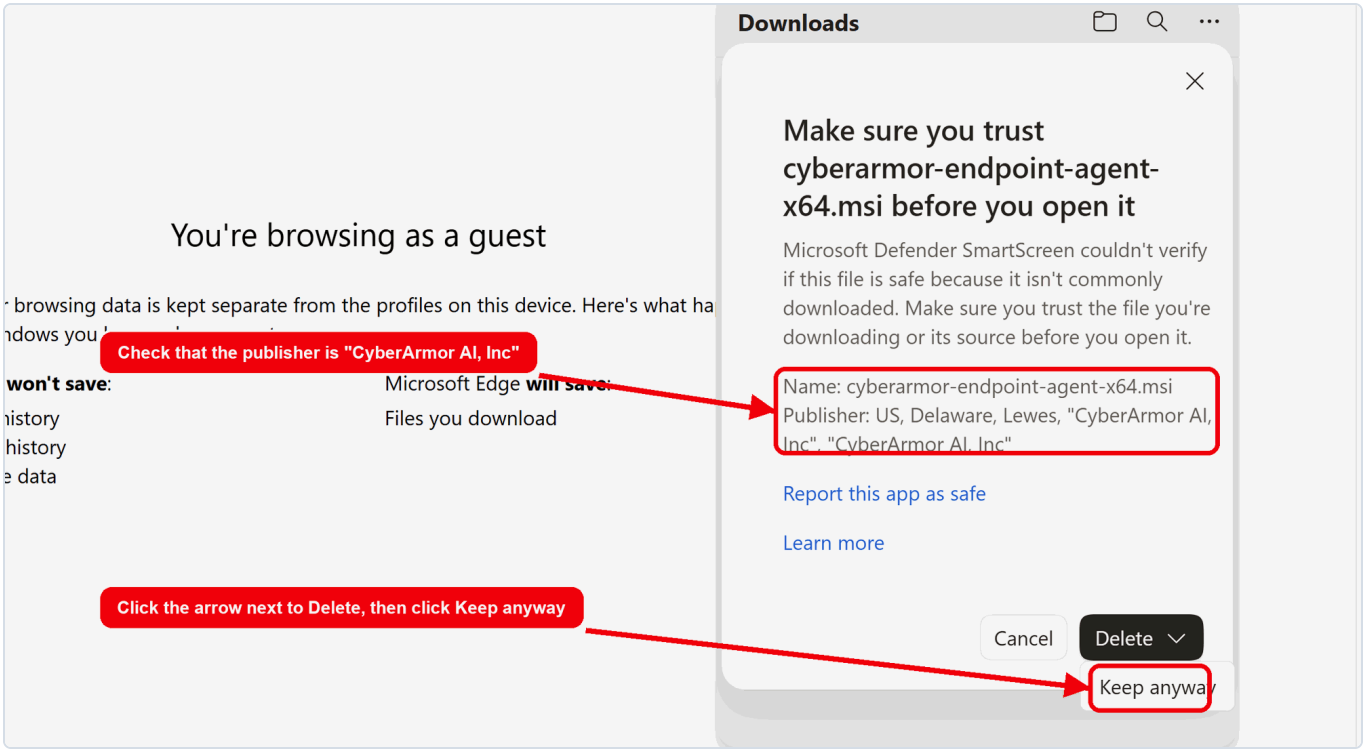
适用于 64 位 Windows；我们的测试环境为 Windows 11。您需要该 PC 上的管理员账户。图中展示的是 Microsoft Edge。

步骤 1. 下载 MSI。 2026-10-29 实测时，Edge 从门户下载已签名的 1.0.13-rc.15 MSI 未出现任何警告。如果您的浏览器提示该文件"不是常用的下载内容"，这对于新的安装程序属于正常现象：在**下载**面板中右键点击文件名，选择**保留**。

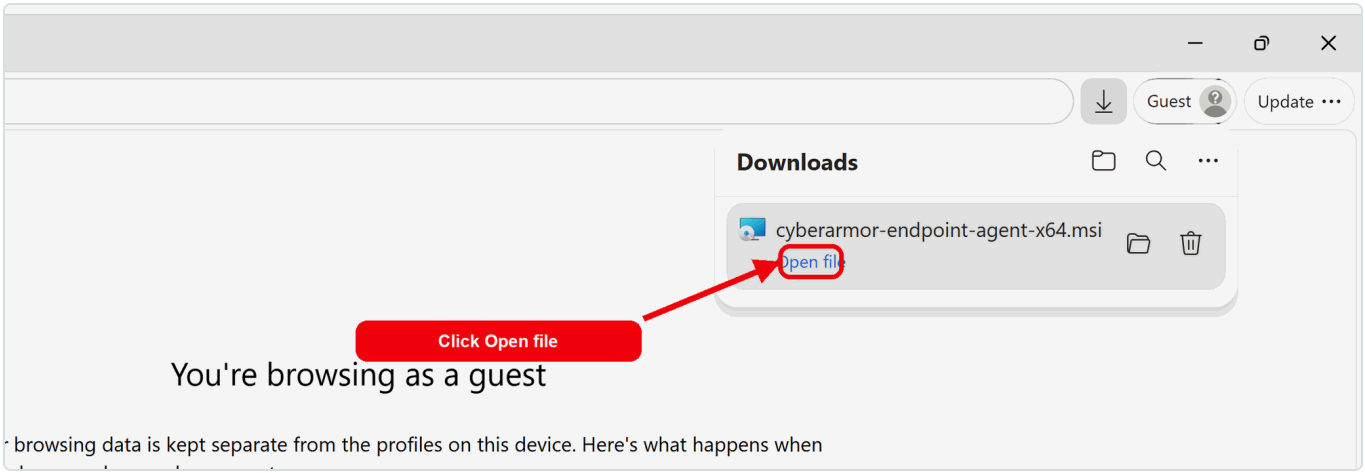




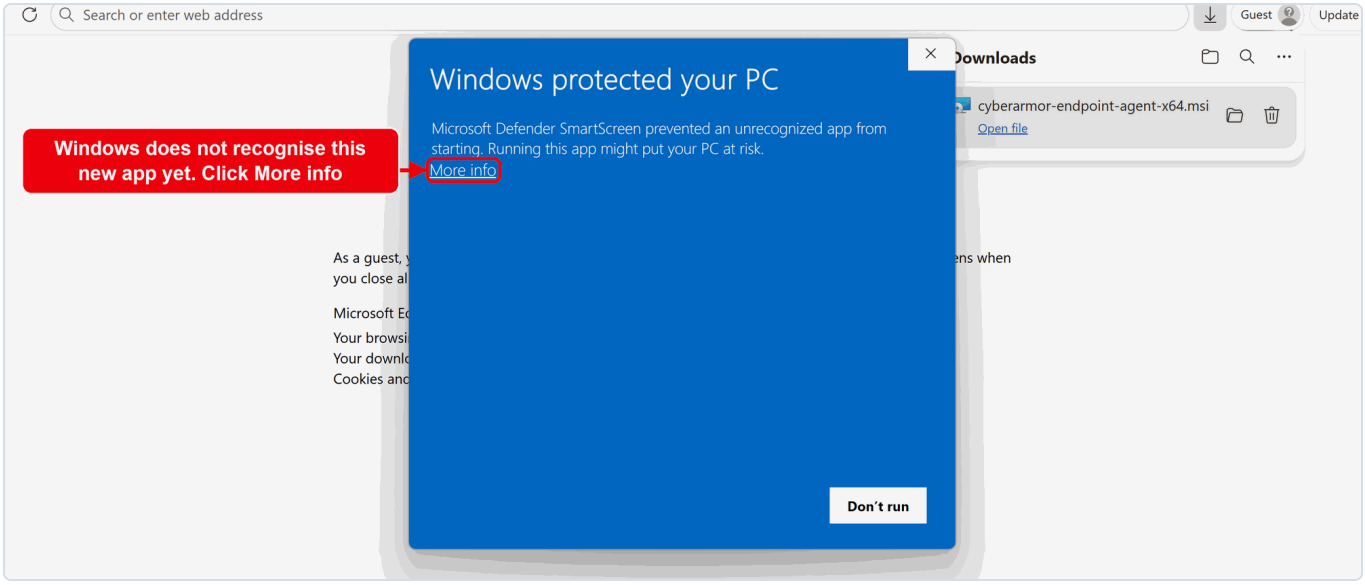
如果 Edge 接着要求您确认信任该文件，请核对发布者是否为 **CyberArmor AI, Inc**，然后点击**删除**旁边的小箭头，选择**仍然保留**。



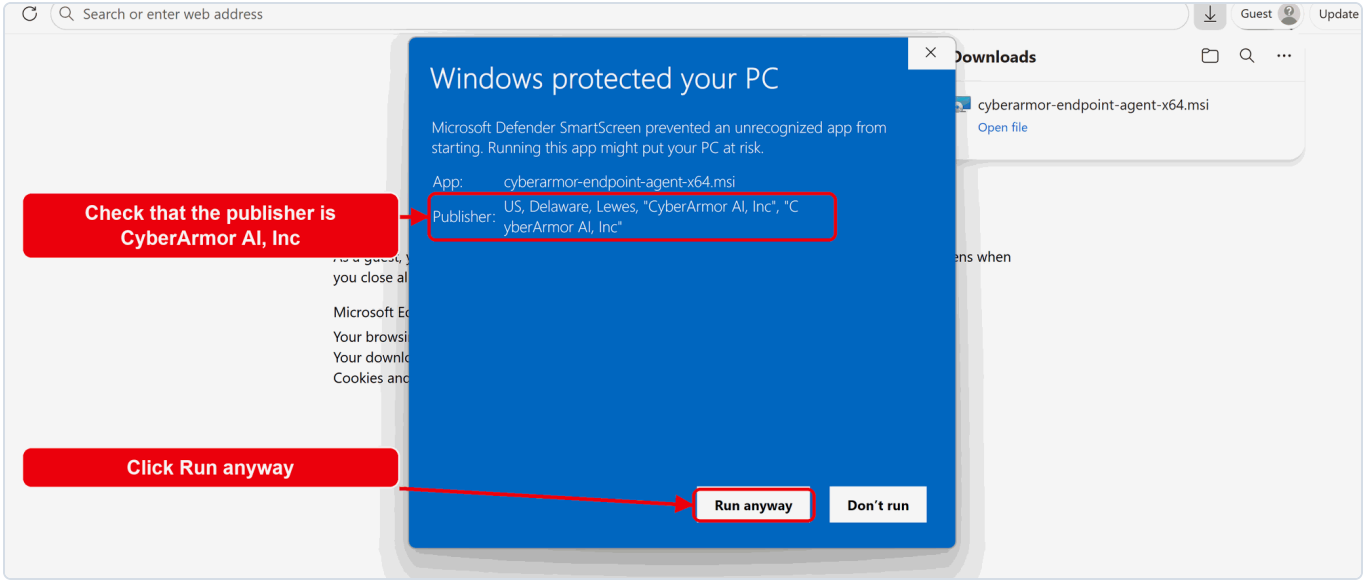
步骤 2. 点击**打开文件**，或在"下载"文件夹中双击该 MSI。



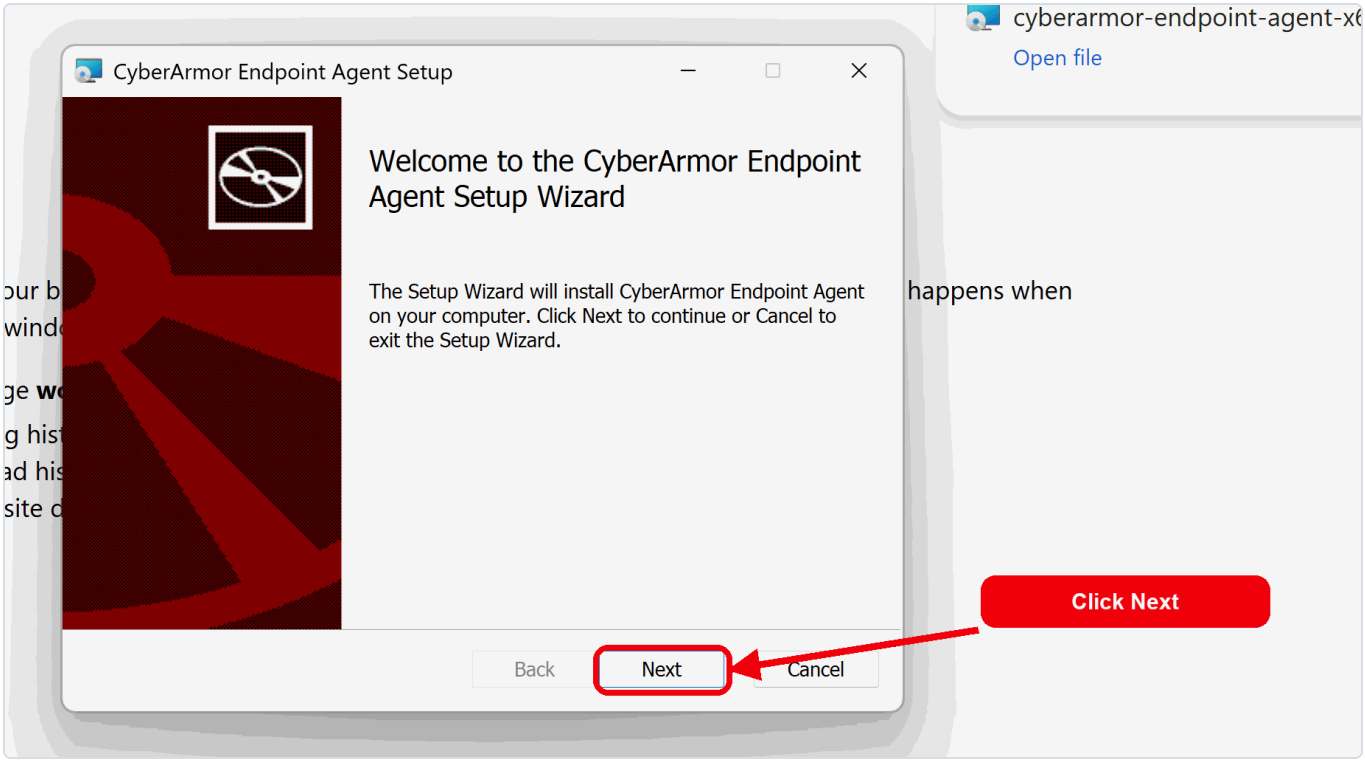
步骤 3. 如果出现"Windows 已保护你的电脑"。 对于尚未被广泛使用的新应用，SmartScreen 可能显示这个蓝色界面。2026-10-29 实测时没有出现，但仍有可能出现。如果出现，请点击**详细信息**……



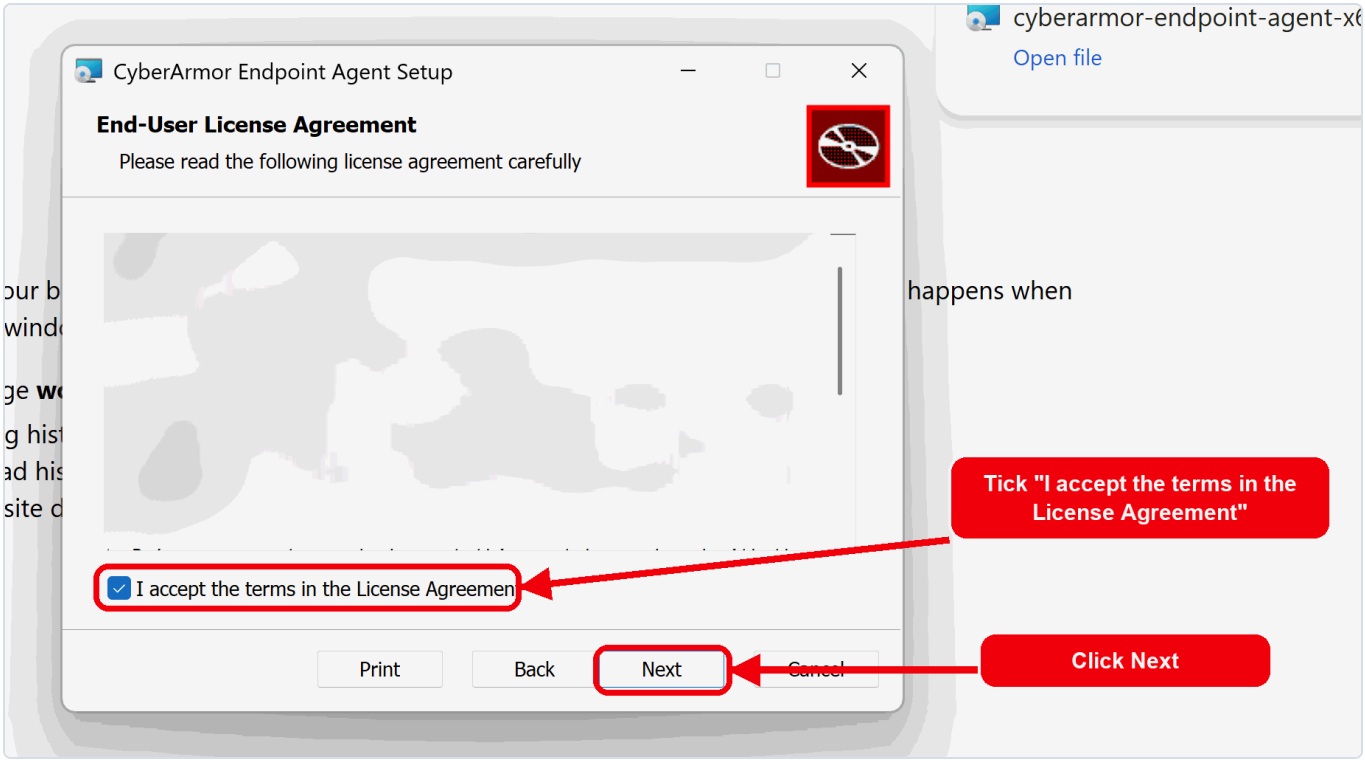
……核对发布者是否为 **CyberArmor AI, Inc**，然后点击**仍要运行**。



步骤 4. 欢迎。 `CyberArmor Endpoint Agent Setup` 安装向导随即打开。点击**下一步**。



步骤 5. 许可协议。 接受许可协议，然后点击**下一步**。



步骤 6. 注册本计算机（Enroll this computer）。 该页面取决于安装程序的版本：

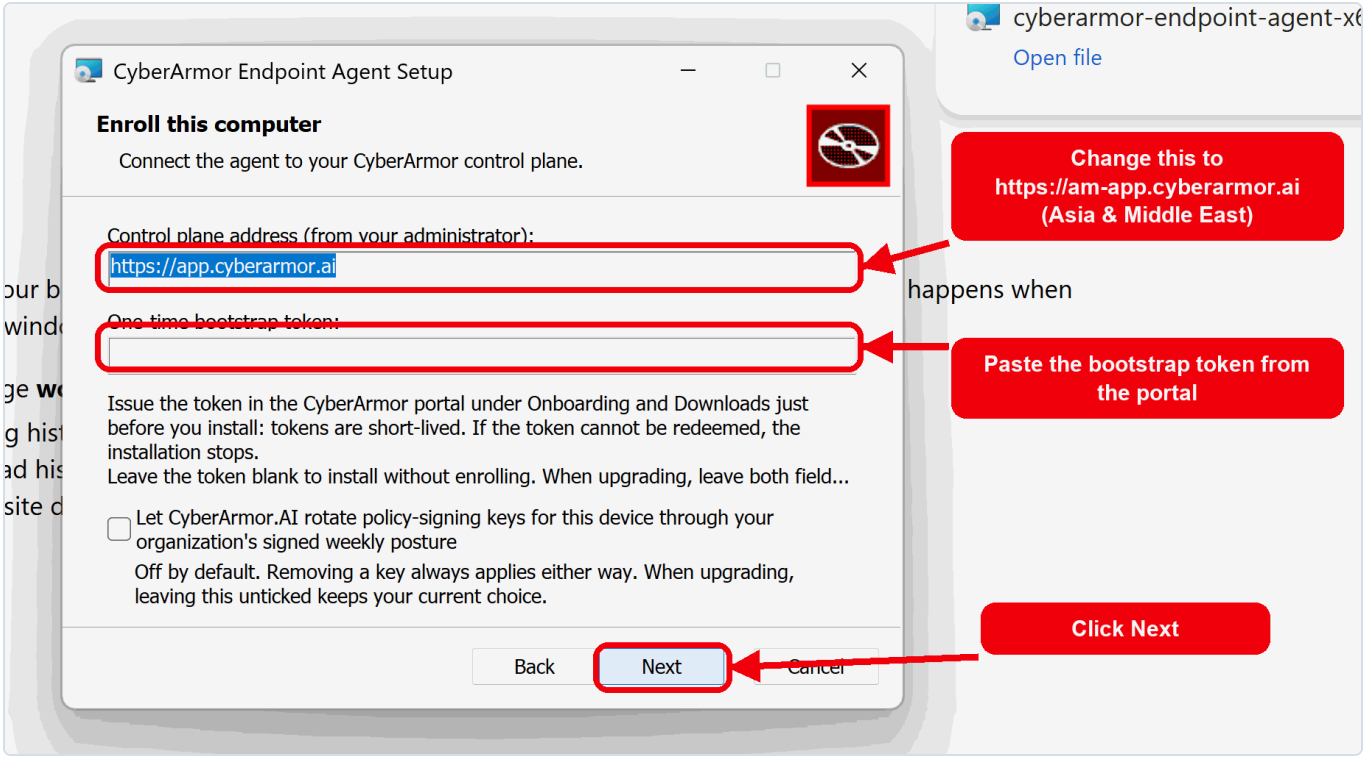
- **1.0.13-rc.15 版本： 控制平面地址**输入框中已填入 `https://app.cyberarmor.ai`。**在亚洲及中东地区，请将其改为** `https://am-app.cyberarmor.ai`。

- **2026-10-28 之后构建的版本**询问 `Which CyberArmor server does this computer report to?`（这台计算机向哪台服务器上报？），提供三个选项且均未预选：**United States (app.cyberarmor.ai)**、**Singapore (am-app.cyberarmor.ai)** 和 **My organisation's server**（在其下方的输入框中填写以 `https://` 开头的地址）。不选择服务器，安装程序不会继续。

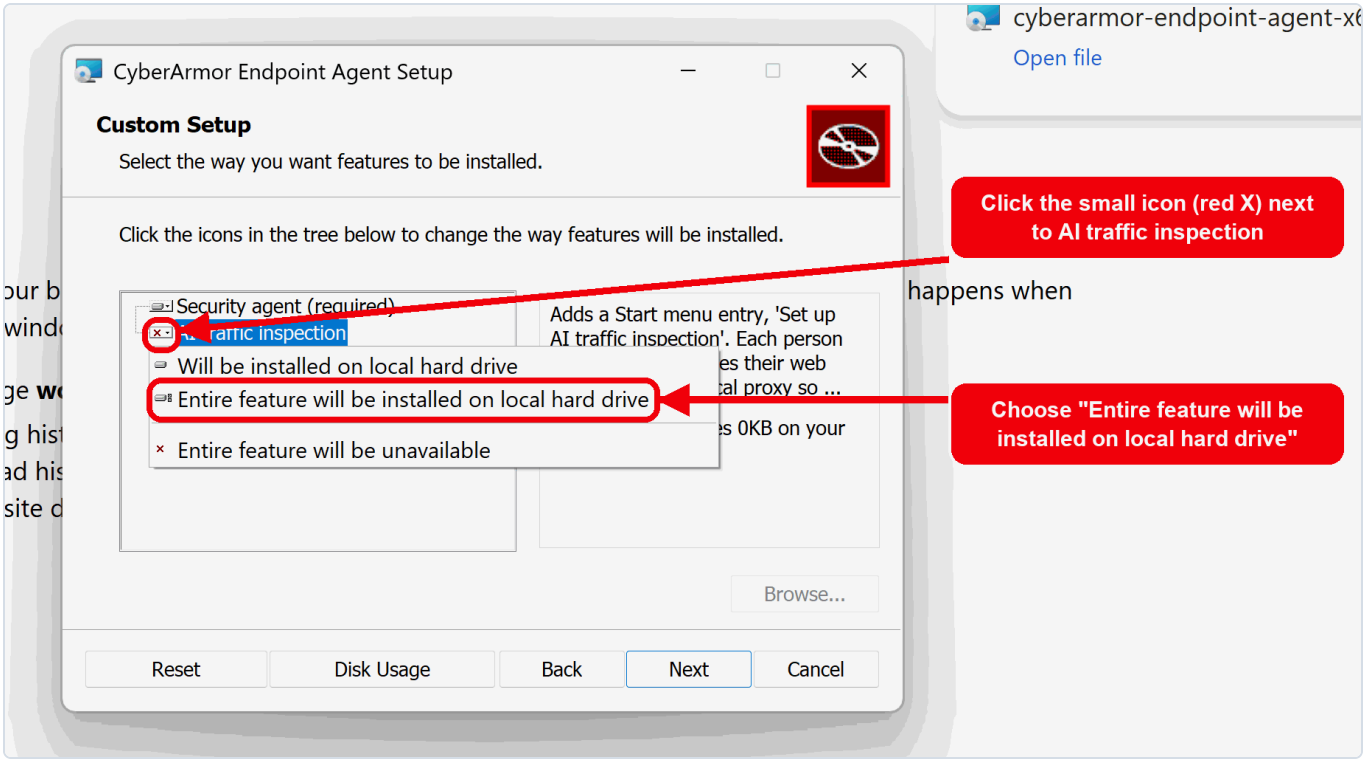
然后：

- **一次性引导令牌：** 粘贴 A 部分步骤 4 中获取的令牌。
- 除非管理员另行要求，否则请保持"轮换策略签名密钥"选项不勾选。

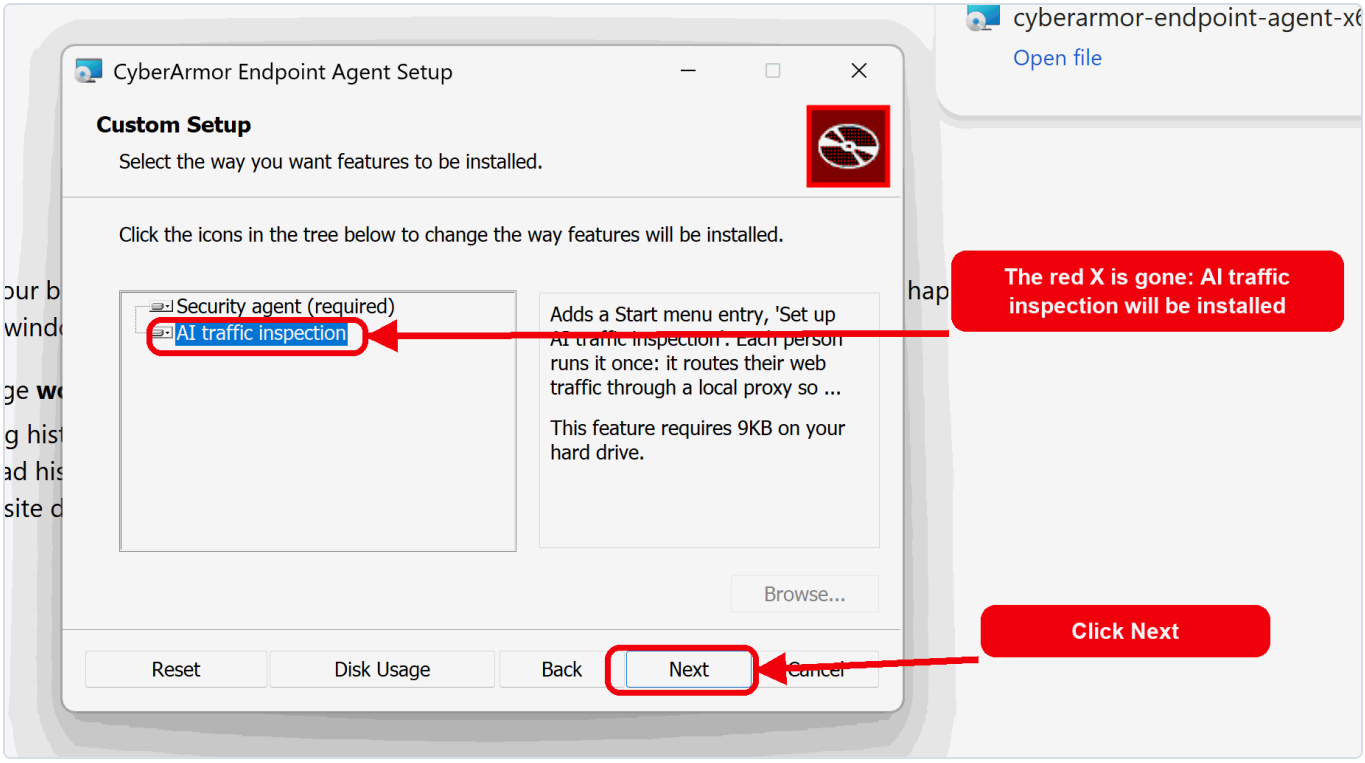
点击**下一步**。



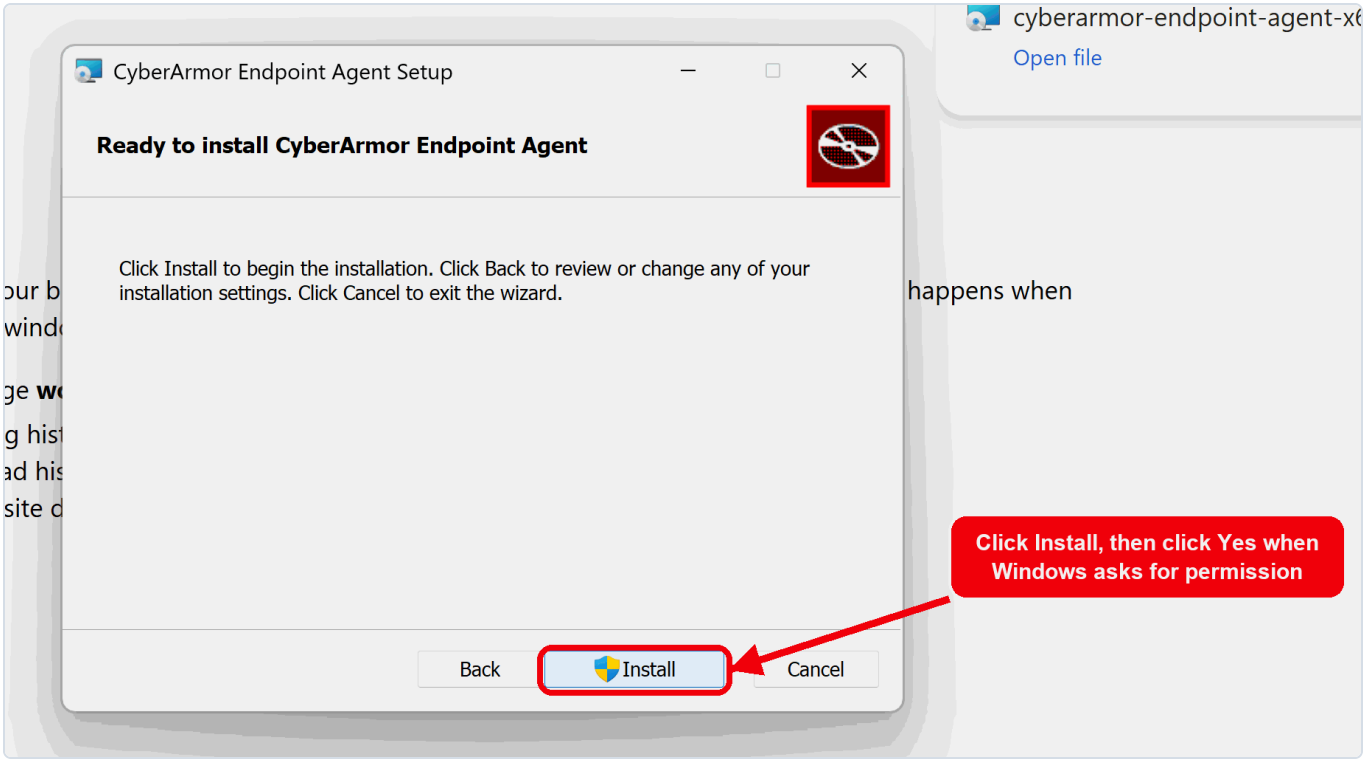
步骤 7. AI 流量检查。 在**自定义安装**界面，**Security agent (required)**（安全代理程序，必需）始终会被安装。请确认 **AI traffic inspection**（AI 流量检查）也会被安装：点击其旁边的小图标，选择**整个功能将安装在本地硬盘上**。（从 1.0.13-rc.15 版本起该功能默认选中；更早的安装程序会将其显示为红色 X，表示未启用。）



点击**下一步**。



步骤 8. 安装。 点击**安装**，当 Windows 询问是否允许更改时（用户账户控制）点击**是**。安装耗时 1–3 分钟；完成后点击**完成**。



步骤 9. 完成 AI 流量检查配置。 打开**开始菜单**，在 `CyberArmor` 文件夹中找到**设置 AI 流量检查**并运行。当 Windows 要求您信任由 **CyberArmor.AI Local Proxy CA** 颁发的证书时，点击**是**。登录该 PC 的每位用户均需执行一次此操作。如果这台 PC 是用 1.0.13-rc.15 或更早版本的代理程序完成设置的，再次运行会替换旧证书（名为 **mitmproxy**）：Windows 先要求您信任新证书，然后再询问一次是否删除旧证书；两次均点击**是**。

步骤 10. 验证是否生效。 在门户中打开**资产清单** → **终端**。2026-10-29 实测时，安装完成后一分钟内该 PC 即出现，健康状态为**健康**（Healthy）；约 4 分钟后，该行显示 **AI traffic**（AI 流量）为 **Enforced**（已强制），**Filter set up for**（过滤器所属组织）为本组织。

CyberArmor.AI 托盘图标位于通知区域，Windows 通常把它放在溢出区：点击时钟旁边的 **^** 即可看到。如果没有，请运行开始菜单 `CyberArmor` 文件夹中的 `CyberArmor Status (Windows)`。

后续升级： 以管理员身份运行较新版本的 MSI，并将注册输入框保持留空。请勿先卸载，也不要签发新令牌：现有连接会被保留。

无人值守安装（IT 团队）： MSI 可在 `msiexec` 命令行中接受 `CONTROL_PLANE_URL`、`BOOTSTRAP_TOKEN` 和 `ACCEPT_EULA=YES`。没有服务器地址时，它会拒绝全新安装，而不会自行猜测地址。

如果遇到问题

您看到的现象	应对方法
令牌被拒绝或提示"已过期"	令牌有效期为 30 分钟且仅可使用一次。请在门户中签发新令牌后重试。
安装程序无法连接服务器	请检查地址是否完全准确：`https://am-app.cyberarmor.ai`（亚洲及中东地区）、`https://app.cyberarmor.ai`（美国）或贵组织自有服务器的地址，并确认该计算机能够在浏览器中打开此地址。
扩展的按钮没有反应	请先点击 **I agree: connect and send this data**（我同意）：在您同意之前，扩展不会进行任何连接。
设备未出现在"终端"页面中	请等待 5 分钟后刷新。如果仍未出现，请打开菜单栏或托盘图标，使用 **Copy diagnostics**（复制诊断信息），然后将信息发送给管理员。
在拦截页面按"返回"仍停留在拦截页面	请将扩展更新到 2.3.20 或更高版本；更早的版本可能会循环回到被拦截的页面。

您看到的现象	应对方法
Mac 安装完成后网站无法加载	请从菜单栏图标暂停 AI 流量检查（如果贵组织允许暂停），然后联系管理员。
Windows PC 设置 AI 流量检查后网站无法加载	请联系管理员。移除 **AI 流量检查**功能（**设置** → **应用**，在 CyberArmor.AI 代理上选择**修改**）会恢复执行移除操作的那位用户的代理设置。
其他任何问题	请在门户中打开**支持** → **帮助与常见问题**，或观看本指南开头列出的安装视频。