Anti-detect
Browser

Create an isolated browser profile for
each account in antidetect browser
and manage multiple accounts on one device securely.

2026

2026 ANTI-DETECT BROWSER INDUSTRY WHITE PAPER

指纹浏览器行业白皮书

AdsPower

跨境开店、社媒运营、广告投放，多账号早已是日常。
但只因登录在同一台电脑上，辛苦经营的账号可能一个出事，全部被封。
指纹浏览器给每个账号一个独立空间，让每一份经营都不被牵连。

Cross-border e-commerce, social media, ad campaigns
— running multiple accounts is now routine.

Yet simply sharing one computer means one flagged account can take down
all the others you've worked hard to build.

A fingerprint browser gives each account its own separate space,
so none of your work gets dragged down.

AdsPower

CONTENTS

目录

前　言 06
PREFACE.

02 11

为什么正当经营
也会被误伤

01 07

一个越来越普遍的
困境

04 19

代理 IP
与指纹浏览器

03 15

什么是
指纹浏览器

05 27

它能解决什么
不能解决什么

07 33

行业**趋势**
与展望

06 30

技术是**如何**
实现的

数据来源与参考资料 39
DATA SOURCES AND REFERENCES.

免责声明 40
DISCLAIMER.

PREFACE.

前　言

过去数年间，
一个原本主要在跨境电商与技术从业者之间流传的工具品类，正在进入更广泛的视野。
它被称为指纹浏览器。

然而，市场对这一品类的认知，明显滞后于它的实际增长。
部分使用者将其视为通用的隐私工具，部分观察者将其与灰色业务相关联，而更多人对其缺乏基本了解，往往直到自身账号因不明原因被平台判定关联、遭到限制时，才第一次接触到这一概念。

本白皮书旨在系统性地厘清指纹浏览器这一品类，
包括其定义、所解决的核心问题、主要应用场景、技术实现方式，以及评估标准。
我们希望无论读者是初次接触该领域的普通用户，还是已在使用此类工具的从业者，都能借此建立起准确而客观的认识。

Over the past few years, a category of tools that once circulated mainly among cross-border e-commerce sellers and technical practitioners has been entering wider view. It is known as the anti-detect browser, or fingerprint browser.

Yet the market's understanding of this category clearly lags behind its actual growth. Some users treat it as a general-purpose privacy tool, some observers associate it with grey-area activities, and many more have little basic understanding of it, often not encountering the concept until their own accounts are flagged as linked by a platform for unclear reasons and subsequently restricted.

This white paper aims to systematically clarify the category of fingerprint browsers, including its definition, the core problems it addresses, its main application scenarios, how it is implemented technically, and the criteria for evaluating it. Our hope is that whether the reader is a newcomer encountering this field for the first time or a practitioner already using such tools, this paper can help establish an accurate and neutral understanding.

01

一个越来越普遍的**困境**

An Increasingly Common Dilemma.

“越来越严的平台风控之下，正当经营者也被卷入其中。”

2021 年，一位跨境电商卖家登录自己的亚马逊后台，发现一家两年前注册、此后从未运营、早已降级为个人状态的店铺，被系统判定为关联账号。他没有做任何操作，账号却在某个环节被卷入了一次风控。

同一时期，另一位卖家反复申明自己的店铺从未刷单、从未操纵评论，但依然收到了平台的风险提醒。还有卖家收到封号邮件，被关联到一个他从未接触、完全陌生的店铺。

这些不是个例。它们指向一个正在变得普遍、却很少被系统讨论的问题，正当经营的用户，正在为平台风控的从严从快，承担着并不属于自己的代价。

一、当封号从个案处罚变成规模化风控

≈600

约 600 个中国品牌受影响

≈3000

约 3000 个卖家封号被封禁

>1000

超千亿元行业损失预估

任何一个大型互联网平台，都需要风控。识别欺诈、打击刷单、阻止滥用，这是平台维持秩序的正当需求，本身无可厚非。

问题出在规模上。当一个平台面对的是数以百万计的账号、每天海量的操作时，逐一人工审核变得不现实。平台转而依赖算法进行自动化识别和处置。算法效率极高，但它有一个内在的取向，为了不放过真正的违规者，它倾向于从严、从宽地划定打击范围。用行业里流传的说法，就是宁可错杀不可放过。

这种取向在一次典型事件中体现得淋漓尽致。2021 年，亚马逊对中国卖家发起了一轮大规模封号。根据多家媒体报道，在大约五个月内，亚马逊关闭了约 600 个中国品牌、封禁了约3000个卖家账号，行业损失预估超过千亿元。这轮封号的起因，是算法识别到了部分卖家的刷单和操纵评论数据，随后打击面从头部大卖家迅速扩大到中小卖家。

在这轮风控中，确实有卖家存在违规操作。但同样真实存在的，是大量被误伤的正当经营者。

二、正当经营者同样受到波及

在当时的报道中，卖家的声音大量出现。

一位卖家告诉记者，他的店铺绝对没有任何刷单和刷评论行为，但依然收到了平台的风险提醒。另一位卖家表示，自己什么违规的事都没做，却被平台判定为关联账号。前面提到那位 2019 年注册、从未运营的卖家，账号早已降级为个人状态，某天登录才发现莫名其妙被关联。

更让经营者不安的，是这种误伤的不可预测。一位卖家的话很有代表性，这次是因为刷单、礼品卡、账号关联，下一次是什么原因呢，谁也说不好下一个会不会是我，谁也不敢保证。

被误伤之后，申诉之路也并不顺畅。有卖家为了申诉去咨询服务商，得到的报价是两万五千元起步，而且申诉成功的概率并不高。对许多中小经营者来说，这意味着账号一旦被误封，挽回的成本高、希望小。

需要说明的是，指出这些问题，并不是要否定平台风控的正当性。平台有维护秩序的权利和责任。但一个客观的事实是，在规模化、算法化的风控之下，误伤是这套机制难以避免的副产品，而承担这个副产品代价的，往往是没有做错什么的普通经营者。

三、账号风险识别的三个维度：环境、网络与行为

要理解账号为什么被关联或受到限制，可以从浏览器环境、网络和操作行为三个维度来看。它们分别涉及账号通过什么设备和浏览器访问、使用什么网络，以及进行了哪些操作。

第一是浏览器环境。平台可以通过 Cookie、浏览器指纹等信息，识别账号的使用环境。例如，卖家在同一个浏览器环境中登录不同店铺，即使切换了账号，这些访问仍可能保留共同的环境特征，成为平台判断账号关系的线索。

第二是网络。平台接收到的访问请求，还带有出口 IP 等网络信息。即使不同店铺使用了独立的浏览器环境，只要共用同一个网络出口，平台看到的 IP 仍相同。此外，登录地区的异常变化、IP 过往的使用情况，也可能成为风险判断的参考。

第三是操作行为。除了环境与网络，平台还会关注账号进行了哪些操作，例如短时间内大量重复操作、异常的交易活动，或刷单、操纵评论等违规行为。这类风险需要从实际操作和业务活动中查找原因，仅更换浏览器环境或 IP 无法解决。



平台结合多信息判断风险 - 单一特征相同，不等于账号违规。

这三个维度可能共同影响平台的判断，也需要经营者分别管理。指纹浏览器用于隔离和管理不同账号的浏览器环境，代理服务用于配置网络出口，经营者则需要确保业务与操作符合平台规则。明确各自的作用，才能减少环境混用带来的干扰，也更容易在账号异常时找到排查方向。

四、这个困境已经不只属于电商

值得注意的是，账号被误判、被限制的困境，正在从跨境电商，蔓延到更多的平台和场景。

社交媒体平台对多账号的风控日趋严格，广告投放账户的连带封禁时有发生。近一两年，随着 AI 工具的普及，类似的问题也开始出现在AI产品的使用中。

以 Claude 这类 AI 服务为例，不少正常使用的用户也遇到了账号被限制或封禁的情况，其中相当一部分与使用环境、网络来源的识别有关。



*部分配图仅为视觉呈现需要，与正文论述无直接关联，亦不构成任何事实性说明



这说明，账号误封并不是某个平台的孤立问题，而是在平台普遍采用算法化风控的今天，一个跨平台、跨场景的共性现象。只要一个平台需要大规模地识别和管理账号，就存在误伤正当用户的可能。而如何在这样的环境下，保护自己正当的使用和经营不被无端波及，正在成为越来越多用户需要面对的现实问题。

指纹浏览器，正是应对这一现实问题的手段之一。它到底是什么，下一章从头讲起。

02

为什么正当经营**也会被误伤**

Why Are Legitimate Businesses Also Adversely Affected?

“平台风控在效率和精确之间倾向效率，误伤就成了难以避免的副产品。”

上一章描述了正当用户被误伤的现象。这一章要回答的是，为什么会这样。 理解了平台风控的底层逻辑，也就理解了指纹浏览器存在的必要性。

一、多账号运营，本身是正当的商业需求

在讨论误伤之前，需要先厘清一个前提，多账号运营是不是正当的。

在很多真实的商业场景里，一个经营主体需要同时运营多个账号，这是再正常不过的经营方式。一家跨境电商公司在不同平台、不同站点开设多家店铺，覆盖不同的市场和品类；一个出海品牌的社媒团队，分别运营面向不同国家、不同语言的官方账号；一个广告代理商，为不同的客户管理各自独立的投放账户。这些都是合规的、普遍的、有实际商业价值的运营行为。

多账号运营是有边界的。正当的多账号，指向的是真实、独立的业务需求，比如不同的市场、不同的品牌、不同的客户。它与那种用大量虚假账号进行刷单、操纵评论、批量滥用的行为，有本质区别。前者是把生意做大、做规范的正常手段，后者才是平台风控真正要打击的对象。

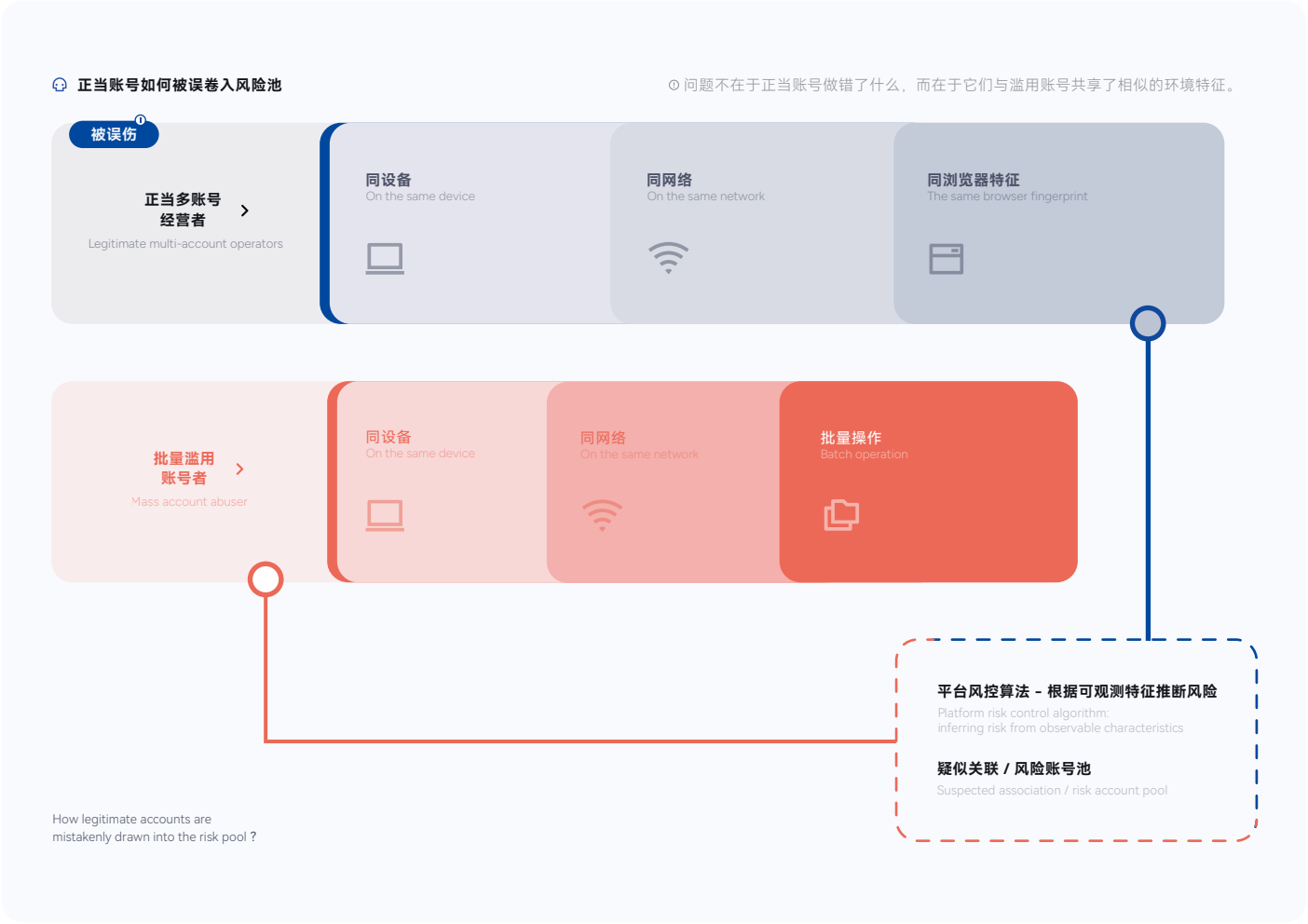
问题在于，平台的算法未必总能准确区分这两者。

二、平台风控的逻辑，是从特征推断风险

平台风控的核心，是通过一系列可观测的特征，去推断一个账号背后的风险。这些特征包括操作环境、注册信息、行为模式等。当多个账号在某些特征上表现出相似性时，算法就可能推断它们之间存在关联，进而判断是否构成风险。

这套逻辑在打击真正的滥用时是有效的。批量注册的虚假账号，往往会共用相同的设备、IP、注册信息，这些共性正是算法识别它们的依据。

但同样的逻辑，也会误伤正当用户。一个正常的多账号运营者，如果在同一台电脑、同一个网络下管理自己名下的多个账号，那么这些账号在环境特征上天然就是相似的。在算法眼里，这种相似性与批量滥用账号的相似性，可能并没有本质区别。于是，正当的多账号运营，就有可能被算法误判为需要打击的关联滥用。



这就是问题的核心。误伤的根源，不在于用户做错了什么，而在于平台的风控在效率和精确之间，选择了前者。算法用统一的、粗放的标准去筛查海量账号，宁可扩大打击面，也不愿放过真正的违规者。正当用户与滥用者共享了某些表面特征，就被卷入了同一张网。

三、连坐效应，让风险进一步放大

平台风控还有一个特点，会让误伤的后果被放大，这就是连坐。

一旦某个账号被判定存在问题，与它共享过环境特征的其他账号，往往会被一并处置。前一章提到的案例中，有卖家的多个店铺因为曾经关联到一个被封的账号而全部被波及，也有卖家的美国站被封后，欧洲站随之被关联封停。



对一个正当经营者来说，连坐意味着风险的高度集中。他名下所有共用过环境的账号，实际上被绑定成了一个命运共同体。任何一个账号出问题，都可能危及全部。这种结构性的脆弱，是很多经营者在账号被封之后才痛切意识到的。

四、从这里，引出了环境隔离的需求

把上面的逻辑连起来，一个自然的结论浮现出来。

正当的多账号运营者，面临的核心风险，是自己名下的多个账号因为共享环境特征，被算法误判为关联，进而被连坐处置。那么，降低这一风险的合理方式，就是让每个账号运行在相互独立的环境中，使它们在平台的识别体系里，呈现为彼此无关的独立主体。

这正是指纹浏览器所要解决的问题。它的作用，不是帮助用户去做违规的事，而是让用户正当的、本就相互独立的业务，在技术层面也真正相互独立，从而避免因为环境共享而被误判、被连坐。

那么，指纹浏览器具体是什么，它又是如何实现环境隔离的，下一章正式展开。

03

什么是
指纹浏览器

What Is An
Anti - detect Browser?

“它的核心
是隔离，
让本就独立的
业务真正独立。”

一、先理解浏览器指纹

要理解指纹浏览器，需要先理解浏览器指纹。

当用户打开一个网站时，浏览器会主动向网站传递一系列用于正常渲染页面的信息，包括操作系统、浏览器版本、屏幕分辨率、显卡型号、字体列表、时区、语言等。单独看每一项都很普通，但当数十项参数组合在一起时，就构成了一个具有高度唯一性的标识。这个标识被称为浏览器指纹。通俗地说，它相当于浏览器在网络上的一张脸。

这张脸的独特性已被多项研究证实。电子前哨基金会的研究显示，在约 47 万个浏览器样本中，84% 具有唯一的指纹配置。后续在更大样本上的研究，也得出了接近九成乃至更高的唯一性比例。这意味着，即便用户更换了账号、密码，只要浏览器指纹不变，平台依然能够识别出这些操作来自同一环境。

“浏览器指纹

由哪些信息组成？”

多种信息信号组合 = **唯一身份特征**

01 操作系统　02 浏览器版本　03 屏幕分辨率

01+02+03

04

04 显卡 / WebGL

05

05 字体列表

06 时区　07 语言

06+07

08+09

08 插件 / 扩展　09 Canvas 渲染特征

10

10 Cookie / 本地储存

这浏览器指纹正是平台进行环境关联的重要依据之一。多个账号如果共享了相同的浏览器指纹，在平台看来，就是同一张脸在操作，关联也就随之而来。

二、指纹浏览器的定义

在此基础上，指纹浏览器的定义就清晰了。

指纹浏览器是一类能够创建多个相互独立浏览器环境的工具。每一个环境都拥有自己独立、稳定且真实的浏览器指纹，在平台的识别体系中呈现为不同的设备与使用主体。

它的核心价值，是隔离，而非隐藏。它让原本可能共享同一张脸的多个账号，各自拥有独立的身份。对一个正当的多账号运营者而言，这意味着他名下的每个账号，都能运行在一个相互独立的环境里，从而降低因环境共享而被误判关联、被连坐处置的风险。



三、一个更贴近用户的理解

如果说传统的定义偏技术，那么从用户的角度，指纹浏览器可以这样理解。

它是正当经营者为自己的多个独立业务，建立相互隔离的运行空间的工具。正如一家公司会为不同的部门、不同的项目设立相互独立的办公室，避免彼此干扰，指纹浏览器为不同的线上账号提供了相互独立的浏览器环境，让它们不会因为挤在同一个空间里，而被误认为是同一个主体。

理解了这一层，也就能理解为什么把指纹浏览器简单等同于灰色工具是不准确的。它的存在，回应的是一个真实而正当的需求，即让本就相互独立的业务，在技术上也真正独立，不被平台的粗放风控无端波及。

04

代理 IP 与
指纹浏览器

Proxy IPs and Fingerprint Browsers

“账号运营，
既需要独立的浏览器环境，
也需要妥善管理网络出口。”

一、什么是代理 IP

当用户打开一个网站时，网站接收到的连接通常带有一个来源 IP 地址。常见的 IPv4 地址由四组数字组成，例如“203.0.113.10”（示例地址），这个地址可以理解为本次访问的网络出口。同一办公室里的多台电脑，可能通过同一个公网 IP 访问网站，因此 IP 与具体设备、账号并非一一对应。

日常所说的代理 IP，通常是指通过代理服务访问网站时使用的出口 IP。配置代理后，访问请求先经过代理服务器，再由它转发给目标网站。对于经代理转发的连接，网站通常看到的是代理的出口 IP。



例如，一家面向美国市场经营的跨境电商企业，如果业务需要通过美国网络访问平台，可以配置美国地区的代理，由相应的网络出口承载访问请求。这类需求既可能出现在店铺的日常运营中，也可能用于查看自有独立站面向当地访客的页面与配送信息。

二、网络管理，从单个店铺开始

对跨境经营者而言，即使只运营一家店铺，也不能忽略网络环境。海外平台对卖家的审核，既涉及经营主体和注册资料，也涉及登录地区与网络使用情况。因此，从开店到日常运营，卖家都需要关注网络是否符合业务需求，以及登录时使用的网络是否发生变化。

2025 年 1 月，新浪财经刊载的《TikTok “封号潮”背后：被抛弃的底层卖家》一文提到，部分 TikTok Shop 卖家和服务商反映，店铺受限可能与共用 IP、IP 过往的不当使用记录，以及登录网络和设备的变化有关。

网络安全研究也提供了相应的观察。Cloudflare 在 2025 年的一项研究中发现，在其评估范围内，由运营商通过地址转换技术（CGNAT）让多个用户共用出口的 IP，受到访问频率限制的频率约为其他 IP 的 3 倍。这意味着，共用出口的用户更容易遇到访问请求受限的情况。



因此，浏览器环境与网络出口需要分别管理。指纹浏览器负责隔离和管理 Cookie、登录状态等浏览器环境信息；代理服务则用于配置和管理网络出口。经营者可以根据实际业务需要配合使用两者，单独更换 IP 并不会自动隔离浏览器内的数据。

三、代理 IP 的常见类型，分别是什么意思

挑选代理服务时，经常会看到“住宅”“静态”“独享”等名称。它们回答的是不同的问题。a

网络从哪里来？住宅代理使用住宅宽带网络的出口；数据中心代理使用机房服务器的出口；移动代理使用移动运营商网络的出口。

出口会不会变化？静态代理通常在约定服务期内保持同一个出口 IP；动态代理则按服务规则更换出口，部分可以在一段时间内保持不变。
是否与其他客户共用？独享代理通常指约定服务期和范围内由一个客户使用；共享代理则允许多个客户使用同一出口或资源。但是独享也不意味着这个 IP 过去从未被别人使用。

“看懂

代理名称的三个纬度。”

01

网络**从哪里来?**

- **住宅代理** → 住宅宽带
- **数据中心代理** → 机房服务器
- **移动代理** → 移动网络

02

出口**会不会变化?**

- **静态代理** → 服务期内保持同一种
- **动态代理** → 按规则更换，可暂时保持

03

是否**与他人共用?**

- **独享代理** → 约定期内单一客户使用
- **共享代理** → 多个客户公用出口或资源

这些名称可以组合。例如，“静态住宅代理”表示它属于住宅网络类型，同时出口相对固定；但是否独享，还需要另外确认。

四、选择代理服务，重点看什么

不同业务对代理的要求有所不同。日常维护店铺，首先要看连接是否顺畅，能否支持商品上传、订单处理等工作。如果业务需要长期保持同一出口，还应确认 IP 的保持时间、续费方式和更换条件。连接稳定与 IP 固定是两回事，需要分别评估。

检查自有电商网站在不同国家的页面展示，则更关注代理是否支持这些国家，以及能否按需切换。选择代理时，应结合实际用途评估，不能仅凭类型名称判断好坏

此外，还需要了解网络资源的来源与授权、是否独享、流量和时长如何计费，以及认证信息和访问日志如何处理。明确这些条件，才能判断服务是否适合长期使用。

Source and Copyright

来源与**版权**

• 所需国家，按需切换



连接稳定 ≠ IP 固定

IP **保持**

• 时间 • 续费 • 更换

IP

IP Retention

从
业务需求
出发

Starting From
Business
Requirements

连接**质量**

Connection Quality

Regional Coverage

地区**覆盖**

• 所需国家，按需切换

数据**保护**

Data Protection

使用与
计费

• 访问顺畅

• 独享 / 共享

• 流量 / 时长

Usage and Billing

"选择代理服务，**重点看什么**。"

五、代理与浏览器环境的一体化管理

从单个店铺的日常维护，到多个店铺的团队协作，代理配置都需要与具体业务保持清楚的对应关系。哪个环境使用哪个代理、服务何时到期、连接是否正常，都是运营中需要持续掌握的信息。

以 AdsPower 为例，产品内集成了静态数据中心代理、静态 ISP 住宅代理和动态住宅代理的购买与管理入口。用户可以为相应的浏览器环境配置代理，将店铺的登录状态、浏览器配置与网络连接放在同一工作流程中管理，减少重复填写、核对信息和交接遗漏。

代理 IP 与指纹浏览器分别承担网络出口配置和浏览器环境隔离的作用，共同支持店铺的日常运营。这种配合的价值，在于让业务的运行条件更清楚、更可控。

05

它能解决什么
不能解决什么

What Can It Solve, And What Can't It Solve?

“它保护的
是正当经营者
的正常业务。”

关于指纹浏览器，市场上存在不少夸大的宣传，仿佛它是应对一切账号问题的万能钥匙。这种认知是有害的，它既误导用户，也扭曲了这个品类的真实价值。
这一章想诚实地厘清它的能力边界。

一、它能解决的，环境关联导致的误判与连坐

指纹浏览器真正擅长解决的，是第一章所说的环境关联问题。

通过为每个账号提供独立、真实、一致的浏览器环境，它能够有效降低多个账号因为共享设备、网络、浏览器特征而被平台误判为关联的风险。对于正当的多账号运营者来说，这意味着他名下的账号不再是一个因环境共享而绑定的命运共同体，而是相互独立的个体，一个账号的问题不会轻易连坐到其他账号。

这是指纹浏览器最核心、也最有价值的作用。



二、它不能解决的，行为层面的风险

但指纹浏览器不是万能的。

如第一章所述，平台的风控除了环境关联，还有行为判定。如果一个账号本身的操作行为触发了平台的风控模型，比如异常的操作节奏、被标记的动作、或注册信息本身的问题，那么再好的环境隔离，也无法改变这些行为特征。一个在刚注册阶段就因行为特征被限制的账号，问题不在环境，指纹浏览器对此无能为力。

换句话说，指纹浏览器解决的是不因环境被误伤的问题，而不是可以随意操作而不被发现的问题。它保护的是正当经营者的正常业务，而不是为违规操作提供庇护。

三、边界之外的部分

厘清这个边界，对理解这个品类本身有意义。

指纹浏览器解决的是环境层面的问题，而账号能否稳健经营，最终仍取决于操作本身是否合规。环境隔离是一层技术保障，让正当的业务不因环境共享而被误伤，但它替代不了合规经营本身。把它当成规避一切规则的万能工具，是一种误读。

对这个品类而言，边界的清晰同样重要。夸大工具的能力，用万能的话术去包装它，短期或许有效，长期却会模糊它真正的价值。一个走向成熟的行业，其标志之一，恰恰是能够清楚地说明工具能做什么、不能做什么。

06

技术是**如何实现的**

How Is The Technology Implemented?

“衡量一款产品，关键看它能否维持环境的真实与一致。”

理解了指纹浏览器的价值与边界，这一章简要介绍它在技术上如何实现独立而真实的浏览器环境。
这部分面向对技术感兴趣的读者，也是判断一款产品优劣的基础。

一、两条技术路线

面对平台的指纹采集，指纹浏览器的技术实现主要有两条路线。

第一条是参数注入。它在网页加载前，通过一段脚本对浏览器暴露的接口进行修改，返回设定的参数值。这条路线实现相对快捷，但由于修改发生在较表层的位置，容易被采集方识别出修改痕迹，且多项参数之间的一致性较难保证。

第二条是内核级修改。它从浏览器底层入手，直接修改浏览器内核中相关接口的实现，使采集到的信息从源头上即为设定值。由于修改发生在底层，这条路线生成的指纹更难被识别为人为修改，各项参数也能实现更好的一致性。随着平台采集与校验技术的升级，内核级路线正逐渐成为行业的主流方向。



二、一致性，比参数数量更重要

在技术实现中，一个容易被忽视但至关重要的概念是一致性。

指纹浏览器的目标，不是让一个环境看起来与众不同，而是让它看起来像一台真实、普通、自洽的设备。这意味着环境中的各项参数必须相互匹配，不能出现逻辑矛盾。一个声称位于某地区的环境，其时区、语言与网络归属地应当彼此对应；一个声称使用某型号硬件的环境，其渲特征也应与之相符。

如果各项参数相互矛盾，即便每一项单独看都被精心修改过，整体反而会因为不自洽而更容易被识别为异常。因此，衡量一款指纹浏览器，不应只看它能修改多少项参数，更应看它能否在所有参数之间维持真实的一致性。这也是判断产品优劣的一个关键标准。

在这一点上，采用内核级技术路线的产品通常更具优势。以行业中的实践为例，AdsPower 采用 C++ 内核级开发，在浏览器内核层面实现指纹的模拟与管理，以此保证环境的真实性与参数的一致性，并持续跟进主流浏览器的版本迭代。这一案例的意义，在于说明成熟的指纹浏览器，比拼的已不是参数的数量，而是底层技术能力与环境一致性的持续投入。

07

行业**趋势**
与展望

Industry Trends And Outlook.

“能够提供真实、可控、
独立浏览器环境的能力，
其价值不会消退，
反而会随着场景的扩展
而愈发重要。”

最后一章，把视野从产品本身，扩展到这个品类正在发生的变化。

一、账号误封，是一个跨平台的长期问题

回到本白皮书的起点。正当用户被平台风控误伤，不是某个平台、某个时期的偶然现象，而是平台普遍采用算法化风控之后的一个结构性问题。

只要一个平台需要大规模地识别和管理账号，就存在为了效率而牺牲精确、进而误伤正当用户的可能。这个问题在跨境电商领域表现得最为突出，但正在向更多场景蔓延。社交媒体的多账号风控、广告账户的连带封禁，乃至新兴的 AI 工具使用场景，都出现了类似的现象。以 Claude 这类 AI 服务为例，一部分正常使用的用户也遇到了账号被限制的情况，其中不少与使用环境、网络来源的识别有关。

这意味着，对独立、稳定、真实的浏览器环境的需求，不会随着某一次封号潮的平息而消失，而是一个长期存在、且不断扩展到新场景的需求。

二、AI 智能体，正在赋予这个品类新的角色

一个更值得关注的趋势是，AI 智能体的兴起，正在重新定义浏览器环境的价值。

近一两年，互联网的流量结构正在发生显著变化。越来越多的自动化程序和 AI 智能体，开始在真实网页上自主完成任务，从信息检索到表单填写，乃至交易操作。多家安全机构的数据都显示，来自 AI 智能体的自动化流量正在快速增长。

“AI驱动流量

正在快速进入主流网络流量。”

AI智能体 / 爬虫（Bot / Crawler / Agent ）

流量占比快速上升

10.1%

2025 月 8 月

2.6%

2025 月 1 月

▪ DataDome **数据**

AI bot **和** Crawer 流量占其网络中已验证机器人

流量比例从 2025 月 1 月的 **2.6 %**升至 8 月的 10.1% 以上

约 8 个月流量比例增长近 4 倍

OpenAI Crawlers 单月请求接近 17 亿次

▪ HUMAN Security **数据**

2025 年 AI 驱动的机器人流量同比增长 23.51% / 远超人类流量的 3.10%

+23.51%

AI - driven / bot traffic

+3.10%

人类流量（human traffic）

AI 驱动流量占比上升，意味着网页访问正在从“人操作浏览器”，逐渐扩展到“智能体操作浏览器”

改变网站识别、风控和访问管理的压力结构。

而这些智能体要在真实网页上稳定运行，就必须处在一个真实、一致、不被误判为异常的浏览器环境中。这恰恰是指纹浏览器多年积累的核心能力。

由此，指纹浏览器的角色，正在从面向多账号管理的工具，向 AI 智能体时代的运行环境基础设施延伸。这是一个尚在早期、但空间广阔的方向。

“指纹浏览器
的角色正在演进。”

从“管理多个账号”
到“**承载多个智能体在真实网页中稳定运行**”



跨境电商 / E-commerce

多账号隔离 / Multiple account isolation

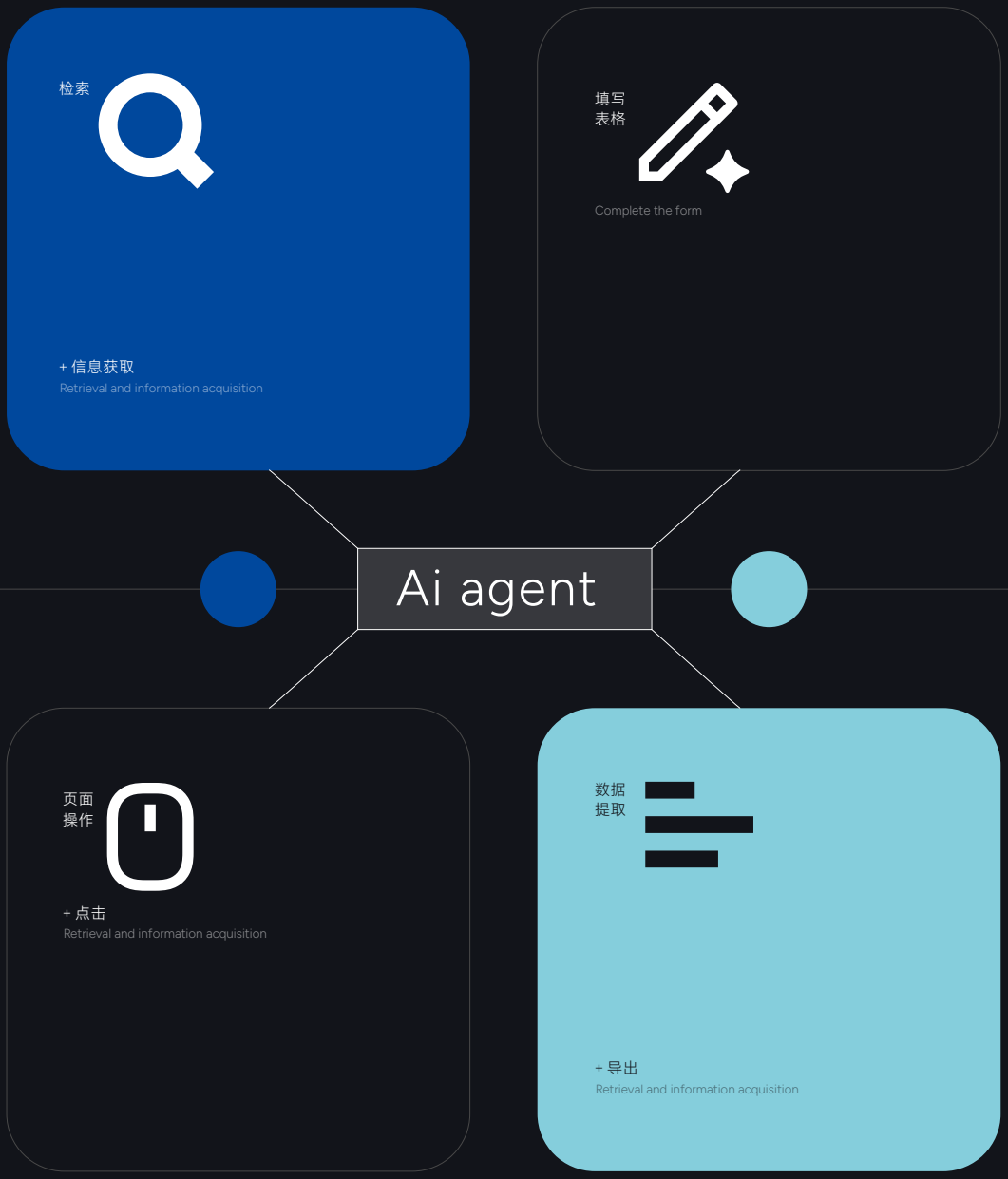
广告投放 / Media buying

社媒运营 / Social media operations

Past / Current **过去 / 当前** - 多账号管理工具

“环境
能力沉淀。”

- **独立环境**
- **稳定指纹**
- **参数一致性**
- **自动化协作**



AI agent

自动化网页任务 / Automated web tasks

真实浏览器环境 / Real browser profile

稳定运行基础 / Foundation for stable o peration

Future Outlook

未来延伸 - AI 智能体时代的运行环境基础设施

三、走向合规与专业

随着行业的发展，指纹浏览器也在朝着更合规、更专业的方向演进。

一方面，用户对产品的安全性、稳定性、合规性提出了更高的要求。另一方面，行业自身也需要摆脱早期的模糊印象，向更透明、更规范的方向发展。能否建立起合规、安全、专业的形象，将成为产品长期竞争力的重要组成部分。

四、结语

这份白皮书从一个真实的困境写起，正当经营的用户，在平台从严从快的风控下，承担着并不属于自己的代价。指纹浏览器的价值，正是回应这一困境，帮助正当用户让自己独立的业务在技术上也真正独立，不被粗放的风控无端波及。

它不是万能的，也不该被夸大。它解决的是环境关联导致的误伤，而非为违规操作提供庇护。理解了这一点，也就理解了这个品类真正的价值所在。

平台的风控会持续演进，账号管理的挑战也会长期存在。在这样的背景下，能够提供真实、可控、独立浏览器环境的能力，其价值不会消退，反而会随着场景的扩展而愈发重要。这是指纹浏览器这个品类，面向未来的意义。

数据来源与参考
资料页。

/ *Data Sources and* References.

本白皮书引用的数据与案例，均来自公开可查的来源，主要包括：

跨境电商封号数据与卖家案例 1

来自新京报、21 世纪经济报道、亿恩网、观察者网、 Shopify 官方博客等公开媒体报道「2021年」

浏览器指纹唯一性数据 2

来自电子前哨基金会（EFF）Panopticlick 研究及相关学术研究。

互联网自动化流量与 AI 智能体流量趋势 3

来自 Cloudflare、DataDome、HUMAN Security 等机构的公开报告。

跨境电商行业规模数据 4

来自海关总署、商务部及相关公开行业报道。

The data and cases cited in this white paper are drawn from publicly available sources, mainly including:
Data and seller cases on cross-border e-commerce account bans, from public media reports by The Beijing News, 21st Century Business Herald, Ennews, Guancha, and the official Shopify blog (2021).
Data on browser fingerprint uniqueness, from the Electronic Frontier Foundation (EFF) Panopticlick study and related academic research.
Trends in automated internet traffic and AI agent traffic, from public reports by Cloudflare, DataDome, HUMAN Security, and other organizations.
Data on the scale of the cross-border e-commerce industry, from the General Administration of Customs, the Ministry of Commerce, and related public industry reports.

免责声明。

/ Disclaimer

AdsPower

本白皮书旨在客观介绍指纹浏览器行业的现状、技术与趋势，仅供行业参考与交流之用，不构成任何商业建议或操作指引。

文中所引用的案例与数据均来自公开报道及公开研究，如有出入，以原始来源为准。

文中涉及的具体平台政策可能随时间变化，读者在实际经营中应遵守相关平台的服务条款与所在地法律法规。
指纹浏览器作为一种环境管理工具应被用于正当、合规的用途。

This white paper is intended to provide an objective overview of the current state, technology and trends of the fingerprint browser ndustry, for industry reference and exchange only.It does not constitute any commercial advice or operational guidance.The cases and data cited herein are drawn from publicreports and public research; in case of any discrepancy, the original sources shall prevail. Specific platform policies mentioned may change over time, and readers should comply with the relevant platforms' terms of service and the laws and regulations of their jurisdictions in their actual operations. As an environment management tool, the fingerprint browser should be used only for legitimate and compliant purposes.



2026

公众号

售前

www.adspower.net

AdsPower，浏览器环境管理平台
为多账号管理、隐私保护
Web 自动化与 AI agent 提供
真实、可控、独立的浏览器环境

AdsPower