



## 10 月风险 IP 洞察

过半新增风险 IP 一周内消失 · 静态名单晚一周漏网三分之一

过半新增风险 IP 一周后就不再活跃，IP 名单晚一周更新，三分之一的风险 IP 就会漏网。威胁猎人梳理了 2026 年 9 月 27 日至 10 月 25 日约 4,900 万个涉及风险行为的 IPv4 地址（77% 位于家庭宽带）：风险 IP 分裂成“14% 贡献 63% 风险活动的长周期常驻 IP”与“32% 只出现一天的单日闪现 IP”，且国内风险 IP 中 89% 是劫持共用代理。依赖固定黑名单和一刀切封禁的防守，既追不上闪现风险，又会持续误伤真实用户。

**32% / ~5天**

新增风险 IP 仅出现 1 天  
约 5 天后过半消失

**84.2% → 67.1%**

名单当天更新 vs 晚一周  
当天活跃拦截覆盖率

**14% → 63%**

活跃 15 天以上的少数 IP  
贡献六成以上风险活动

**89%**

国内风险 IP 中  
劫持共用代理占比

## KEY FINDINGS

## 核心发现：把 IP 防线拆成不同生命周期

2026 年 9 月 27 日至 10 月 25 日（29 天观察期），全球约 4,900 万个 IPv4 地址出现过风险行为（占全球可路由 IPv4 的 1.3%，77% 位于家庭宽带）。真正的防守难点不再是“要不要看家庭宽带”，而是风险 IP 极高的周转率与内部结构分化：过半新增 IP 一周内消失，14% 的常驻地址制造了 63% 的风险活动，而国内 89% 的风险 IP 与正常住户共用同一出口。

### 32% / 42.3%

#### 过半新增 5 天左右消失

10 月 4 日至 11 日新增的风险 IP 中，32% 只出现 1 天，约 5 天后只剩一半，第 7 天仍活跃的仅 42.3%；30 天历史名单近一半已失效。

### 84.2% → 67.1%

#### 名单晚一天就多漏近 5%

当天更新可覆盖 84.2% 的当天活跃风险 IP；晚 1 天降至 79.5%，晚一周降至 67.1%，且每天仍有 15.8% 是近 7 天首次出现。

### 14% → 63%

#### 少数常驻制造六成风险

29 天内活跃 15 天以上的风险 IP 仅占 14%，却贡献了 63% 的风险活动（最活跃 10% 贡献 62%），其中 24% 是数据中心 IP。

### 89%

#### 国内近九成是劫持共用代理

国内风险 IP（占总量 25.1%）中 89% 是劫持共用代理，93% 位于家庭宽带；直接封禁会连带封死正常家庭用户。

### +29%

#### 境外风险 IP 十月持续走高

10 月下旬（10/19–10/25）境外周活跃风险 IP 达 2,066 万，较 9 月底上升 29%（约三成），劫持共用不到 0.1%。

### 4,900 万

#### 样本基数与网络底盘

每 75 个公网 IPv4 就有 1 个涉及风险（80% 代理出口、22% 劫持共用代理）；家庭宽带 77%、移动网络 10%、数据中心 6%。

口径说明：全期观察窗口为 2026 年 9 月 27 日至 10 月 25 日（共 29 天）。文中两个“32%”分属不同统计口径：新增留存分析（FIG. 2）追踪 10 月 4 日至 11 日首次出现的风险 IP 随后 14 天的存续情况，其中 32% 仅在首日出现；全期活跃分布（FIG. 4）统计 29 天观察期内仅活跃 1 天的风险 IP 占全部风险 IP 的比例（32%），其贡献的风险活动占 3%。

## 01 · 规模与底盘

## 约 4,900 万个 IPv4 涉及风险，77% 在家庭宽带

观察期内，约 4,900 万个 IPv4 地址出现过风险行为，占全球可路由 IPv4 的 1.3%，相当于每 75 个公网地址中就有 1 个。八成（80%）是代理 IP，即被黑灰产用作代理出口的地址；22% 是劫持共用代理：正常用户的设备被植入代理程序后，其网络被代理平台转卖，正常用户与黑灰产共用同一个 IP；秒拨等其他类型合计不足 1%。少数 IP 同时属于两类，因此各类占比相加略超 100%。

| 网络类型 | 占风险 IP 比例 | 策略含义                                        |
|------|-----------|---------------------------------------------|
| 家庭宽带 | 77%       | 运营商动态重分配频繁，封禁必须设 7-14 天 TTL，否则易误伤重分配后的正常住户。 |
| 移动网络 | 10%       | 基站切网与共享出口普遍，需结合设备与会话信号实时评估。                 |
| 数据中心 | 6%        | 在 15 天以上常驻风险 IP 中占比达 24%，适合直接纳入静态黑名单硬拦。     |
| 企业专线 | 5%        | 多为固定出口代理或被利用的企业网络。                          |
| 校园网  | 0.3%      | 占比极低，多为共享出口。                                |

从地域看，境外占 75%，国内占 25.1%。境外风险 IP 分散在 116 个国家和地区，以巴西（7.9%）、印度（7.3%）、美国（6.7%）最多；按区域看，拉美、欧洲和南亚居前。

国内占四分之一，境外风险 IP 以巴西、印度、美国最多

各国家和地区占全部风险 IP 的比例；境外合计 75%

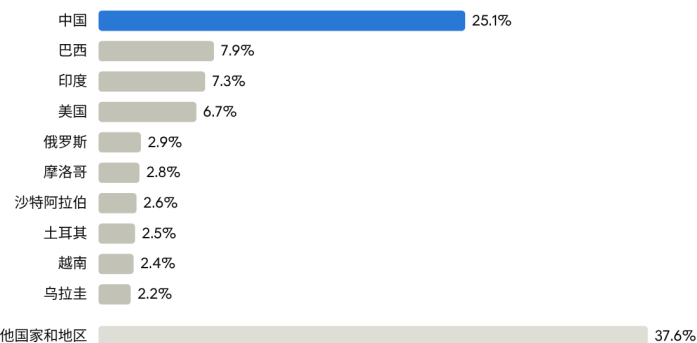


FIG. 1 各国家和地区占全部风险 IP 的比例（2026.09.27 – 10.25；境外合计 75%）。

## 02 · 存续与名单时效

## 快进快出：过半新增风险 IP 一周后不再活跃

新增风险 IP 存续时间很短。对 10 月 4 日至 11 日新增的风险 IP 逐个追踪 14 天：32% 只出现一天（第 1 天留存 68.1%），第 3 天降至 55.2%，约 5 天后只剩一半，第 7 天仍活跃的仅 42.3%，第 14 天降至 24.8%。从全局看，观察期内出现过风险行为的 IP，近一半在最近一周已不再活跃。

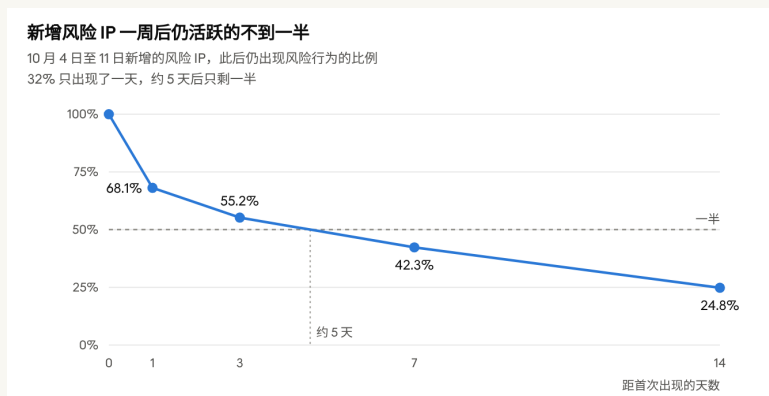


FIG. 2 10 月 4 日至 11 日新增的风险 IP 在随后 14 天内仍出现风险行为的比例。

**风险研判** 封禁一个新增风险 IP，有效期大约一周。家庭宽带地址会被运营商重新分配给正常用户，长期封禁容易误伤后来的使用者；直接拿近一个月的历史名单做拦截，名单里近一半的 IP 最近一周已不再活跃。

## 03 名单晚一天更新，就多漏一截

以「过去 7 天出现过的风险 IP」为名单，拦截覆盖率随更新延迟快速下降：当天更新能覆盖 84.2% 的当天活跃风险 IP，晚 1 天降至 79.5%（下降近 5 个百分点），晚 3 天降至 73.4%，晚一周降至 67.1%（三分之一漏网），晚两周只剩 61.3%。即便当天更新，每天仍有 15.8%（约 16%）的风险 IP 是近 7 天首次出现。

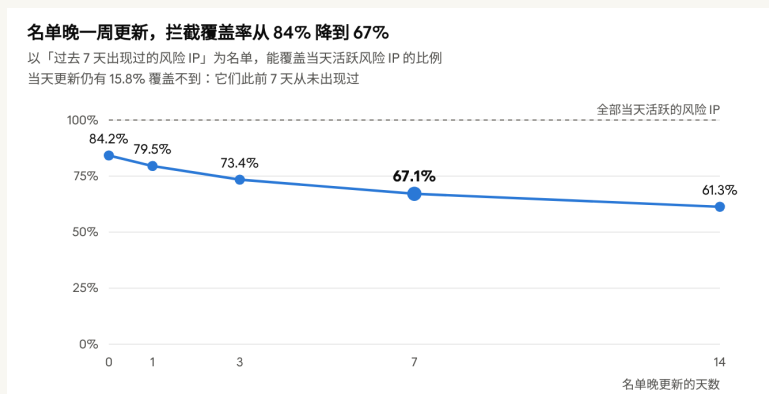


FIG. 3 名单更新延迟天数与当天活跃风险 IP 拦截覆盖率（10 月 4 日至 25 日合并统计）。

**风险研判** 名单最好实时更新，至少按天更新，越慢漏得越多。当天新增的那 15.8% 风险 IP 此前 7 天从未出现，任何历史名单都无法提前收录，只能依靠实时风险评估识别。

## 04 · 头部集中与境内外结构

## 14% 的长期活跃 IP，贡献了 63% 的风险活动

风险 IP 分成两类完全不同的对手：长期活跃的少数，和短暂出现的多数。29 天观察期中活跃 15 天以上的风险 IP 只占 14%，却贡献了 63% 的风险活动（最活跃的 10% 贡献了 62%）；而仅出现 1 天的风险 IP 占数量的 32%，只贡献 3% 的风险活动。

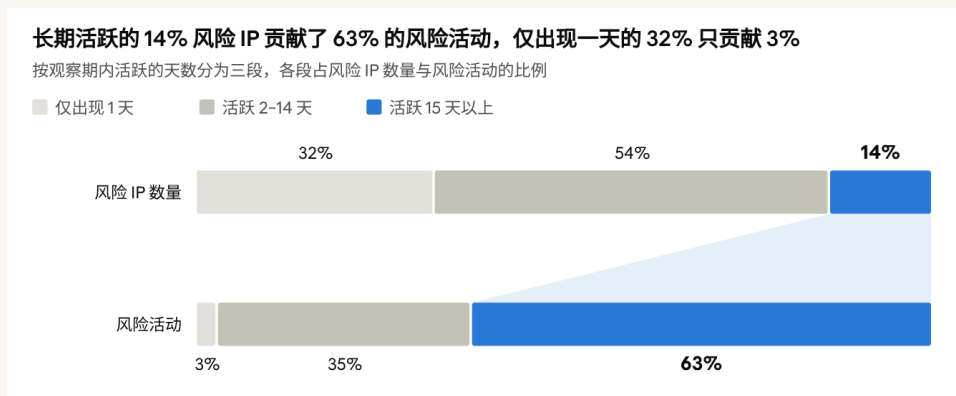


FIG. 4 按 29 天观察期内活跃天数分段，各段占风险 IP 数量与风险活动的比例。

| 观察期内活跃天数  | 占风险 IP 数量 | 占风险活动量 | 数据中心 IP 占比 | 最近一周仍活跃占比 |
|-----------|-----------|--------|------------|-----------|
| 仅出现 1 天   | 32%       | 3%     | 2%         | 33%       |
| 活跃 2-14 天 | 54%       | 35%    | 4%         | 56%       |
| 活跃 15 天以上 | 14%       | 63%    | 24%        | 95%       |

仅出现一天的风险 IP 中，81% 位于境外，以家庭宽带和移动网络为主。长期活跃的 14% 适合纳入名单直接拦截；单日闪现的 32% 名单来不及收录，只能依靠实时风险评估。

## 05 国内风险 IP 近九成是劫持共用代理

国内风险 IP 约占全部的 25.1%，其中 89% 是劫持共用代理（93% 位于家庭宽带；中国电信 38%、中国移动 28%、中国联通 27%；最近一周仍活跃占 45%，低于其他风险 IP 的 57%）。其余约 11% 以云厂商机房和企业专线上的代理 IP 为主。境外风险 IP 则以代理 IP 为主，劫持共用代理不到 0.1%。

**风险研判** 国内业务遇到风险 IP，多数情况下对面是一个被利用的真实用户网络。直接封禁会误伤真实用户，更稳妥的做法是以二次验证代替拦截，并结合设备、账号等信号综合判断。

## 境外风险 IP 十月持续走高，防护需分层

10 月下旬（10/19–10/25），境外风险 IP 的周活跃规模达 2,066 万，比 9 月底（9/28–10/4）高出 29%（约 30%），且逐周上升；国内先升后落，末周为 598 万，比首周高约 10%，涨幅明显小于境外。这一变化是否延续，需结合 11 月数据继续观察。

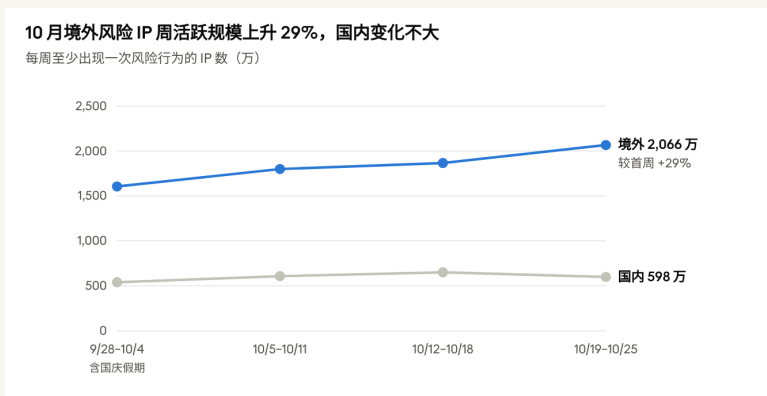


FIG. 5 每周至少出现一次风险行为的 IP 数（万，每周自周一至周日）。

## 07 防护建议：让 IP 判定跟上风险的变化

| 防线动作               | 配置建议与数据依据                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------|
| 1. 为封禁设置 7-14 天有效期 | 新增风险 IP 过半在一周内消失（第 7 天仅 42.3% 活跃），30 天历史名单近半已失效；到期应复核解封，防误伤重分配住户。                          |
| 2. 名单至少按天更新 + 实时评估 | 晚 1 天更新覆盖率即从 84.2% 降近 5 个百分点，晚一周降至 67.1%；每天另有 15.8% 为近 7 天首次出现，需实时评估兜底。                    |
| 3. 长短周期两类对手分层处置    | 活跃 15 天以上的常驻 IP（占 14%、贡献 63% 活动，24% 在机房、95% 近一周仍活跃）纳入黑名单硬拦；单日闪现 IP（81% 在境外）交实时评估。          |
| 4. 国内场景以二次验证代替硬封   | 国内 89% 为劫持共用代理（93% 在家庭宽带），建议用二次验证结合设备、账号信号综合判断；境外重点地区（巴西、印度、美国等，10 月涨 29%）加强住宅与移动 IP 实时评估。 |

威胁猎人持续监测全球风险 IP 的出现与消失，提供实时 IP 风险评估（[threathunter.cn/products/ip-risk-intelligence](https://threathunter.cn/products/ip-risk-intelligence)），帮助业务按 IP 当下的风险状态做判断，而不是依赖过期的名单。

数据来源：威胁猎人 Threat Hunter IP 风险情报（2026.09.27 – 10.25） · [threathunter.cn](https://threathunter.cn) · 联系邮箱：[marketing@threathunter.cn](mailto:marketing@threathunter.cn)