SPUR

Why Residential Proxies Are A Security Risk

Six Steps to Secure Your Environment from Obscured Traffic

Contents

Executive Summary

Residential proxies are technologies that route internet traffic through IP addresses assigned to real households by consumer internet service providers (ISPs). Because these IPs blend in with everyday user activity, they're useful for legitimate regional purposes such as ad verification and localized QA testing.

However, the same anonymizing properties make them a powerful cloak for fraud, credential-stuffing, and scraping, enabling traffic to bypass IP-based defenses. Attackers increasingly pair large residential proxy pools with bot automation to mimic "normal" users, providing an effective route to conduct malicious campaigns and complicate attribution and incident response.

Organizations must gain greater visibility into residential proxy usage in their environments or risk fraud and security incidents and the resulting remediation costs, customer attrition, brand reputation damage, or threats to mission-critical systems.

This paper:

- Defines what residential proxies are (and how they differ from datacenter and mobile proxies and VPNs).
- Identifies the risks posed by residential proxies (including examples of misuse).
- Examines practical detection and response steps to mitigate the risk of residential proxies.

What is a Residential Proxy and How Does it Work?

A proxy is an intermediary that forwards requests to a destination on behalf of a user. A residential proxy specifically routes traffic through an IP address sourced from a consumer ISP, typically from a home network.

Commercial services assemble large “proxy pools” of these IPs – often via software development kits (SDKs) in apps, opt-in “peer-to-peer” clients, or, in some cases, compromised devices – so customers can route traffic through ordinary household connections and appear to be local to a chosen geography. Example residential proxies include BrightData (formerly Luminati), Oxylabs, and SmartProxy.

Since proxied traffic provides a high amount of diversity in IP addresses and blends the proxied traffic in with legitimate user traffic, these qualities make residential proxies difficult to identify and block.

How Residential Proxies Differ from Traditional and Mobile Proxies

Not all proxies are created equal. Traditional datacenter proxies originate from, and route traffic through, hosting providers and cloud networks such as AWS or Google. IPs routed through traditional proxies are usually more easily identified and blocked via known netblocks and intelligence due to their reputations.

In mobile proxies, traffic is routed through an actual smartphone, tablet, or SIM farm using a mobile data connection. IPs sit behind NATs (Network Address Translations), a process that lets multiple devices on a private network share a single public IP address to connect to the internet.

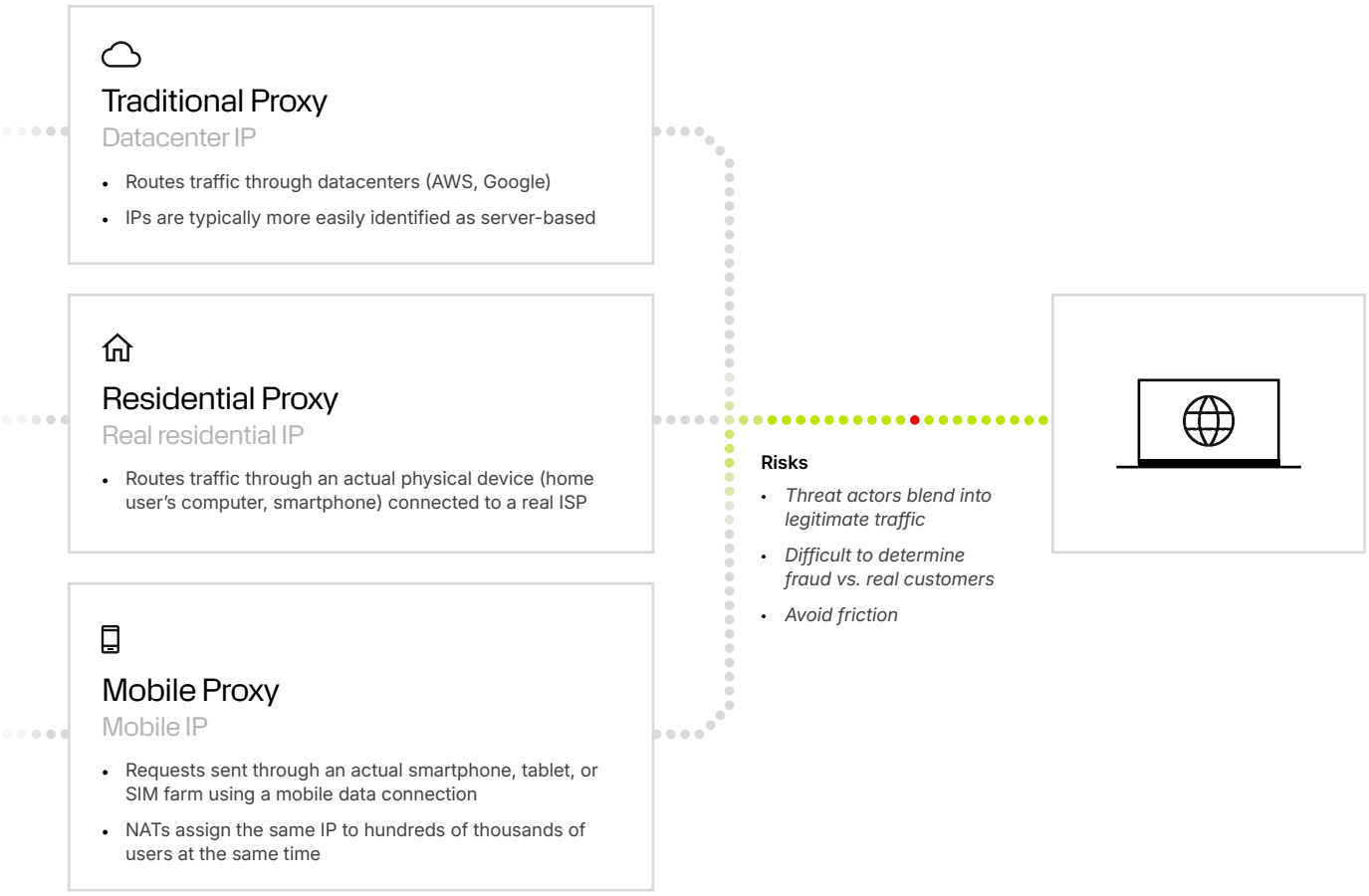


Fig. 1. Proxies rely on different methods to obscure traffic.

How Residential Proxies Differ from VPNs

Residential proxies and VPNs (virtual private networks) are often confused with one another because both conceal a user's real IP address but differ in their methods.

With a residential proxy, IPs are assigned to real households by ISPs. VPNs, on the other hand, use IPs from servers owned or rented by the VPN provider, typically located in data centers. Subscribers to VPN services can connect into any of these IP addresses and use them to hide their "true" IP address, and all traffic is attributed to that service.

Comparing VPNs and Residential, Datacenter, and Mobile Proxies

The table below compares these anonymizing technologies in terms of the sources of IP addresses, detectability, common abuse patterns, attribution risks, and the business risks of over-blocking IPs from these sources.

Attribute	VPN	Residential Proxy	Datacenter Proxy	Mobile Proxy
Source of IPs	Datacenter servers owned/leased by VPN provider	Consumer ISP IPs from real households	Cloud/hosting providers (AWS, Google, etc.)	Carrier networks behind carrier-grade NATs (cellular)
IP Detectability	Easier (known datacenter ASNs; public VPN ranges)	Harder (consumer ASNs; resembles real users)	Easiest (well-known datacenter netblocks)	Hard (carrier ASNs; large NAT pools)
Common Abuses	Geo-evasion; low-sophisticated scraping	Account takeover (ATO); mass account farming; scalping; rate-limit evasion; high-throughput scraping	Basic bots; spam; volumetric scraping (easily blocked)	ATO; evasion via high churn/ attribution noise
Attribution Risks	Medium (server IPs trace to VPN)	High (origin appears as random households)	Low–medium (traceable to hosting)	High (shared carrier egress; hard to tie to an individual)
Business Risks of Over-Blocking	Low–moderate	High (may block real customers)	Low	High (may block many legitimate mobile users)

Residential Proxy Risks

Naturally, because residential proxies relay requests through real household IPs, they have become the tool of choice for cybercriminals to bypass website restrictions and remain anonymous. This section examines risks and actual uses of residential proxies.

Evasion of IP and Geo Controls

Because requests appear to come from consumer ISPs and local geographies, residential proxies commonly bypass region controls, per-IP rate limits, and IP reputation lists tuned for datacenter ranges. The FBI has specifically warned that actors leverage residential proxies to avoid suspicious behavior monitors during credential-stuffing campaigns.

Bot Automation & Account Takeovers (ATO)

Bot operators combine credential stuffing tools and AI with rotating residential IPs to test stolen credential pairs at scale while looking like many independent users. The rotation sidesteps per-IP lockouts, making blocking risker for companies due to the increase in false positives against real customers.

Fraud & Abuse

Residential proxy traffic enables fraudsters with a lower chance of being flagged solely by source IP characteristics.

Account farming: If an attacker uses thousands of residential IPs, each IP creates a few accounts staying under per-IP thresholds while enabling massive total volume.

CASE STUDY

Social Media Platform Stops Account Farming and Spam

A social media platform needed help fighting a surge in successful fake account registrations. Actors would use a series of VPNs and residential proxies to register counterfeit profiles in different regions. These registrations would pass bot protections such as captchas, SMS, and phone verification steps. Actors would then use these accounts to perform activities like phishing, spam, view farming, trend manipulation, denial-of-service attacks, or other platform-degrading activities.

To address this challenge, the social media company used IP enrichment to tag the account creation activity with important context, such as whether the IP was a datacenter IP, if an anonymity service was being used, behavioral characteristics, and high-level signals such as user-count estimates. With these insights, the social media company dramatically reduced account harvesting operations, protecting users, and resulting in a shut-down of the dark web offender.

Read more here

Inventory scalping: Retail sites limit purchases per IP or use IP-based bot-detection rules. Distributed residential IPs let scalpers make many purchase attempts appearing as distinct buyers across regions, reducing the chance of triggering simple per-IP purchase limits.

CASE STUDY

Online Retailer Prevents Scalping on Major Releases

An online retailer knew they had issues with scalping bots and that these bots affected the company's bottom-line on high profile sales. The company had rudimentary tools and tracking in place to help detect and score various carts in their digital storefronts. By themselves, however, they were only able to see a small part of the picture.

To address this challenge, the online retailer used real-time IP intelligence within their sales flows revealing that more than 100 different anonymity networks were involved in scalping inventory. This bot detection analysis has since moved beyond individual product releases and has become an integral part of the entire customer session tracking process, improving customer experience, and maintaining company growth goals.

Read more here

Site scraping: Sites throttle by IP or implement soft rate limits. Distributing scraping requests across a large residential pool lets an adversary stay under per-IP thresholds, avoiding automatic throttles or bans.

CASE STUDY

Delivery and Logistics Platform Reduces Unwanted Web Traffic

A delivery and logistics platform was experiencing increasingly aggressive site crawling that closely mimicked legitimate customer behavior. The abusive behavior was both large enough in volume to cause operational challenges and sophisticated enough to bypass legacy defensive measures.

By integrating real-time session intelligence, the logistics firm added a precise, low-latency layer to its defensive stack, decisively distinguishing genuine users from automated scraping tools that had slipped past their web application firewall (WAF). The result was improved visibility, cleaner analytics, and reduced infrastructure spend — all without negative impact to the customer experience.

Read more here

Coupon abuse: Coupon systems often restrict redemptions per IP or per device. Rotating residential IPs, paired with simple browser automation, enables creating many accounts and redeeming offers repeatedly without exceeding IP-based thresholds.

Ad fraud: Residential IPs generate impressions and clicks that resemble organic users, making it harder for fraud-detection systems to separate real clicks from fraudulent ones based on IP.

Compliance and Legal Exposure

The inability to discern legitimate from illegitimate traffic can create privacy and regulatory challenges. For example, without proper attribution, government agencies may be unable to detect anonymized access attempts against government networks, flag masked users in digital citizen services, and support law enforcement investigations of cybercrime.

How to Spot a Residential Proxy in Use

Identifying residential proxies requires in-depth IP intelligence that traditional signals can't deliver. Combine internal detections with external observations from proxy/VPN intelligence providers to raise confidence and reduce false positives.

Note: For a complete examination of IP intelligence attributes, please see Anatomy of an IP Address*.*


```
{
  "as": {
    "number": 49981,
    "organization": "WorldStream"
  },
  "client": {
    "behaviors": [
      "FILE_SHARING"
    ],
    "concentration": {
     "city": "Polāia Kalān",
      "country": "IN",
      "density": 0.2675,
      "geohash": "tsn",
      "skew": 6762,
      "state": "Madhya Pradesh"
    },
```


ASN & ISP Context

Traffic sourced from consumer ISPs (vs. cloud ASNs) is a clue, but residential proxies are supposed to look like that, and some actors now announce proxy ranges through residential ASNs. Use curated datasets that specifically flag proxy IPs.

```
    "count": 4,
    "countries": 2,
    "proxies": [
      "LUMINATI_PROXY",
      "KOOKEEY_PROXY",
      "PROXYAM_PROXY",
      "NIMBLEWAY_PROXY",
      "ABCPROXY_PROXY",
      "9PROXY_PROXY",
      "BIGMAMA_PROXY",
      "NETNUT_PROXY",
      "GOPROXY_PROXY"
    ],
    "spread": 4724209,
    "types": [
      "MOBILE",
      "DESKTOP"
  ]
  },
  "infrastructure": "DATACENTER",
  "ip": "89.39.106.191",
  "location": {
    "city": "Amsterdam",
    "country": "NL",
    "state": "North Holland"
  },
  "organization": "WorldStream B.V.",
  "risks": [
    "CALLBACK_PROXY",
    "TUNNEL",
    "GEO_MISMATCH"
  ],
  "services": [
    "OPENVPN"
  ],
  "tunnels": [
    {
      "anonymous": true,
      "entries": [
        "89.39.106.82"
      ],
      "operator": "PROTON_VPN",
      "type": "VPN"
    }
  ]
}
```


Known Proxy Ranges & Fingerprints

Subscribe to specialized residential proxy datasets and APIs to identify IPs associated with proxy providers, including dynamic pools and ISP/static (a.k.a. “ISP” or “static residential”) allocations.

Rotation Patterns

Repeated short-session connections where user agents, device fingerprints, or cookie jars are inconsistent, yet IPs hop across many consumer ISPs or cities, suggests proxy-backed automation.

Mismatched Telemetry

Device and locale claims that are inconsistent with geolocation and language settings are a clear sign that a residential proxy is in use.

Behavior + IP Correlation

Look for indicators such as high login failure rates, automated navigation patterns, direct API calls without page renders, and abnormal signup or checkout flows.

Six Steps to Secure Your Environment from the Risk of Residential Proxies

Combatting the risks from residential proxy traffic includes a multi-step process.

01

Establish Policy and Risk Tiers

Classify features or endpoints by abuse sensitivity (for example prioritize authentication flows, signup, checkout, inventory, APIs, etc.). Decide where residential proxy traffic is acceptable with friction (e.g., enforcing challenges) versus blocked outright. Document business exceptions (e.g., your own QA teams using approved proxies).

02

Layer Controls

Start by establishing strong credential protections such as enforcing multi-factor authentication (MFA), breached password checks, and credential stuffing mitigations. Implement adaptive challenges such as triggering CAPTCHAs, step-up authentication, or proof-of-work when risk signals cross acceptable thresholds.

03

Use High-Fidelity IP Intelligence and Session Enrichment

Ingest commercial datasets or leverage real-time APIs that specialize in residential proxy detection. Favor vendors that differentiate residential, mobile, ISP/static, and datacenter proxies; provide reasons/metadata; and update continuously to track fast-changing proxy pools.

04

Correlate Across Telemetry

Blend IP intelligence with device, session, and behavioral analytics. Look for velocity patterns and impossible travel. Download IP intelligence data into analysis engines and data lakes to enable broad correlation among diverse datasets. Look for solutions that offer pre-build integrations to commonly used SIEM and SOAR tools to enable that.

05

Create an Analyst Playbook

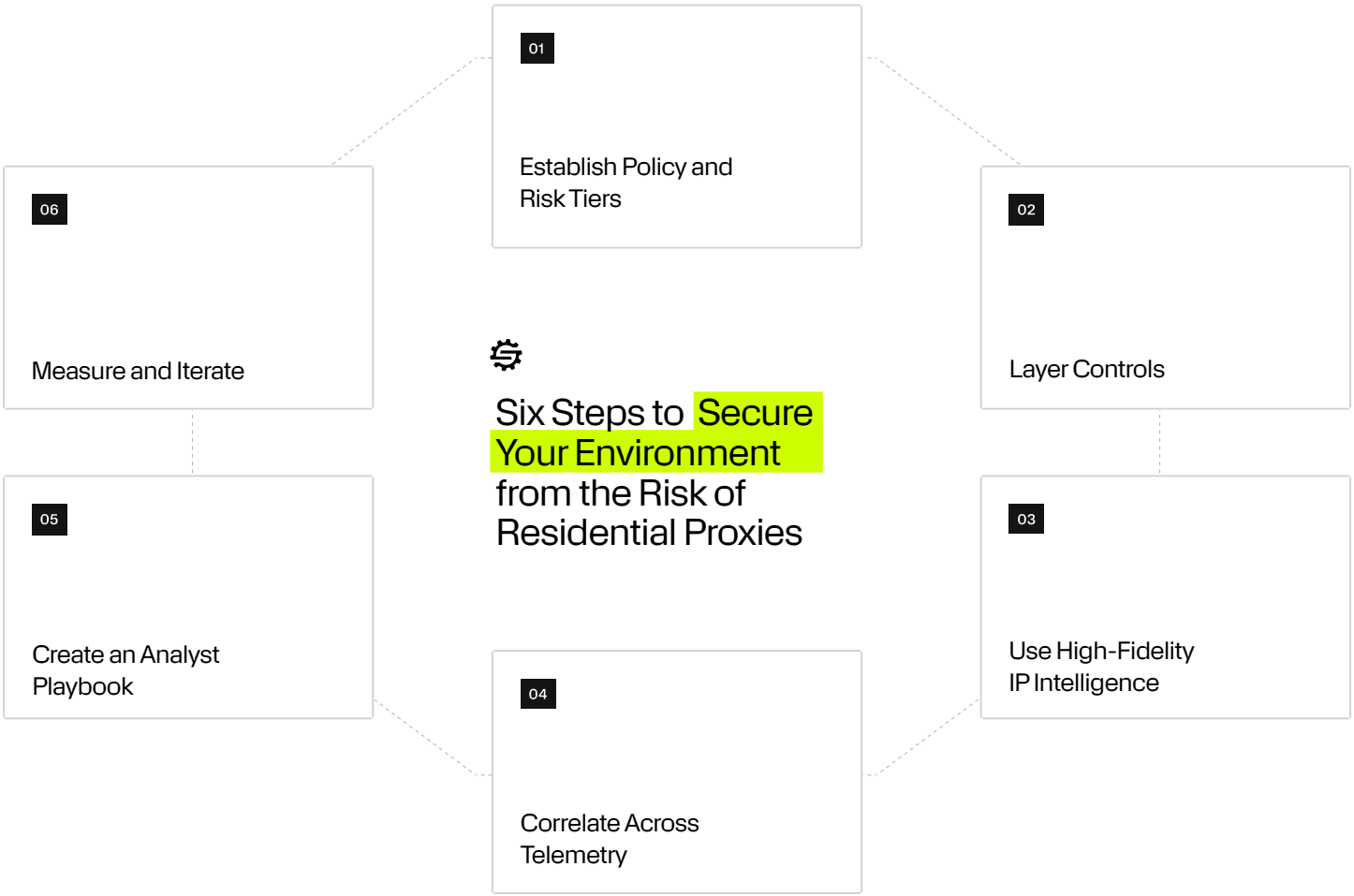
When residential proxy use is detected:

- **Confirm intent** enriching logs with IP intelligence. For example, is it credential stuffing or QA?
- **Contain** by tightening per-entity limits and issuing challenges.
- **Block or rate-limit** ranges/IPs tied to known proxy pools.
- **Document indicators** (IPs, ASNs, user agents, automation artifacts) and share.

06

Measure and Iterate

Track false-positive rates and user friction; tune step-ups and allow-lists (e.g., your own test traffic). Regularly reassess provider coverage, update lists, and calibrate controls as new proxy types emerge (mobile/ISP/ static residential).



How Spur Helps Bring Clarity to Obscured Internet Traffic

Residential proxies are a dual-use technology. For legitimate testers and advertisers, they provide ground-truth views of what users see in specific locales. For attackers, they are a scalable disguise that blends automated abuse into the crowd of normal consumer traffic. Effective defense means enriching the IP with residential proxy intelligence and responding adaptively based on risk. Organizations that combine network intelligence, device and behavioral analytics, and targeted friction can reduce fraud and abuse while protecting real customers.

Spur helps by delivering the highest-fidelity IP intelligence available to detect anonymized, proxied, or otherwise obscured internet traffic, empowering you to stop fraud, fake users, and threats. Designed by expert security researchers and engineers, Spur elevated VPN attribution, bot detection, and residential proxy tracking to defend the most mission-critical government and commercial systems in the world.

What differentiates Spur from other providers of IP intelligence?

Breadth of Coverage

Spur delivers more comprehensive detection than anyone else in the market, covering 220 million+ anonymous IPs per month, and 1,000+ active VPN and proxy services.

Depth of Attributes

Spur provides more than 20 attributes, including geo location, ASN, proxy/VPN status and attribution, device type, connection type, tunnel entry/exit context—not opaque scoring.

Focus on Residential Proxy

Spur is the only source that delivers insights into residential proxies, mobile IPs, and botnets — where traditional providers fall short.

High-Fidelity Data

Spur delivers real-time data that is accurate, fresh, and actionable, focusing on transparency and trust with low false-positive.

Historical Data Access

Delivers access to historical records dating back to 2020.

Results in Minutes

Spur delivers fast onboarding, clear documentation, and responsive support for engineers and analysts.

To start a free trial and experience our high-fidelity IP intelligence in action, visit spur.us.