



DATENBLATT · DATEN-APIS · VPN-ERKENNUNG

Echte Adresse oder Tarnung? Ein Aufruf zeigt, was hinter der IP steckt.

Die VPN-Erkennung prüft eine IP-Adresse gegen Listen von VPN-Diensten, Proxys, Tor-Knoten, Rechenzentren und Sperrlisten und nennt zu jedem Treffer die Quelle. Für Shops, Plattformen und Formulare, die Bestellungen und Anmeldungen absichern: per REST-API und MCP.

AUF EINEN BLICK

37 Listenquellen in einem Aufruf: Die Antwort trennt VPN, Proxy, Tor und Rechenzentrum und nennt im Feld type die Liste, die angeschlagen hat.

01 · Worum es geht

Jede Bestellung sieht echt aus. Die IP verrät mehr.

Bei einer Bestellung oder Anmeldung sehen Sie Name und E-Mail. Ob jemand dabei über ein VPN, einen Proxy, das Tor-Netz oder einen Server im Rechenzentrum kommt, bleibt verborgen. Die VPN-Erkennung zeigt es Ihnen, bevor Sie die Anfrage annehmen.

EINGABE

IP-Adresse oder Hostname; ohne Angabe die Adresse der Verbindung

ERGEBNIS

is_vpn, is_proxy, is_tor, is_datacenter, is_blocklisted, is_malware, score, score_basis

QUELLEN

37 Listen: VPN-Anbieter, Tor, Proxys, Cloud-Netze, Sperr- und Missbrauchslisten

ZUGANG

REST-API mit API-Schlüssel, MCP-Werkzeug
po_ip_geolocation_vpn_detection

**Getrennte Kennzeichen**

VPN, Proxy, Tor, Rechenzentrum und Relay-Dienste stehen als eigene Felder in der Antwort. Ihre Anwendung reagiert auf jedes einzeln.

Quelle je Treffer

type nennt die Liste, die angeschlagen hat, score_basis den Grund, score einen festen Wert je Grund. Bei mehreren Treffern zählt details.match_count mit.

Sperr- und Missbrauchslisten

Adressen aus Spam- und Angreiferlisten schlagen ebenfalls an: unter is_vpn und als is_blocklisted. is_malware liefert false, seine Quelle ist eingestellt.

Abgleich über den Provider

Ohne Listentreffer prüft die API die Namen von ISP und Organisation auf VPN-, Tor- und Hosting-Begriffe. type beginnt dann mit isp_.

Listenstand in jeder Antwort

last_paperofficeai_overseer_crawl zeigt, von wann die geprüften Listen stammen. So bleibt jede Entscheidung nachvollziehbar.

Mit Standort kombiniert

/ip2location/full liefert VPN-Kennzeichen und Standort in einem Aufruf, etwa für den Abgleich von IP-Land und Rechnungsland.

02 · SO FUNKTIONIERT ES

IP senden, Kennzeichen lesen. Die Regel legen Sie fest.

Die Prüfung ist ein einzelner Aufruf mit direkter Antwort. Was bei einem Treffer passiert, bestimmen Sie in Ihrer Anwendung: zusätzliche Bestätigung, Freigabe von Hand oder Sperre.

1

API-Schlüssel anlegen

Unter **API & Entwickler** > **API-Keys** legen Sie mit **Neuen Key erstellen** einen **API-Key** an. Kopieren können Sie den Schlüssel dort jederzeit.

2

IP prüfen

GET /ip2location/vpn?ip=... mit dem Schlüssel als Bearer-Token, etwa aus Ihrem Checkout oder Ihrer Registrierung.

3

Kennzeichen lesen

Im Block vpn stehen is_vpn, is_proxy, is_tor und is_datacenter, bei einem Treffer dazu type und details.

4

Regel anwenden

Ihr System entscheidet je Kennzeichen, etwa Rechenzentrums-IPs bei der Anmeldung prüfen lassen oder Tor im Checkout sperren.

TECHNISCHE DATEN

MERKMAL	DETAILS
Endpunkt	GET /ip2location/vpn; zusammen mit dem Standort: GET /ip2location/full
Basis-URL	https://api.paperoffice.ai/latest/
Parameter	ip (IP-Adresse oder Hostname, optional)
Antwortfelder	is_vpn, is_proxy, is_tor, is_relay, is_datacenter, is_blocklisted, is_malware, score, score_basis, type
Quellen	37 Listen in den Kategorien VPN, Tor, Proxy, Relay, Rechenzentrum, Cloud, Sperrliste und Malware
Zugang	API-Schlüssel als Bearer-Token; MCP po_ip_geolocation_vpn_detection im Katalog /mcp-full
Abrechnung	Nach Verbrauch

03 · IM EINSATZ

Wo die Prüfung hilft. Drei typische Abläufe.

Checkout absichern

Kommt eine Bestellung über Tor oder einen Proxy, fordert Ihr Shop eine zusätzliche Bestätigung an, bevor die Ware versendet wird.

Registrierung prüfen

Anmeldungen aus Rechenzentrumsnetzen landen in einer Prüfliste. Automatisierte Konten fallen so früh auf, echte Nutzer melden sich wie gewohnt an.

Länderangebote schützen

Länderpreise und regionale Inhalte richten sich nach dem Land der IP. Mit `/ip2location/full` sehen Sie Land und VPN-Kennzeichen in derselben Antwort.

HÄUFIGE FRAGEN

Was wird erkannt?

VPN-Dienste, Proxys, Tor-Knoten, Relay-Dienste, Rechenzentrums- und Cloud-Netze sowie Adressen aus Sperr- und Missbrauchslisten, jeweils mit der Quelle im Feld `type`.

Wie aktuell sind die Listen?

Jede Antwort nennt im Feld `last_paperofficeai_overseer_crawl` den Stand der geprüften Listen. Sie sehen also bei jeder Entscheidung, auf welcher Grundlage sie gefallen ist.

Woran sehe ich, warum eine IP angeschlagen hat?

`type` nennt die Liste, `score_basis` den Grund und `score` einen festen Wert dazu: 95.00% für VPN-Listen, 0.00% ohne Treffer. Kam der Treffer über den Providernamen, steht `detection_method` `isp_name` in `details`.

Kann ich Standort und VPN zusammen prüfen?

Ja. `/ip2location/full` liefert Standort, Provider und VPN-Kennzeichen in einer Antwort, mit demselben API-Schlüssel.

JETZT STARTEN

VPN-Prüfung in Ihren Checkout holen

Konto anlegen, unter **API & Entwickler > API-Keys** einen API-Schlüssel erstellen und den ersten GET auf `/ip2location/vpn` senden.

paperoffice.ai/de/ki-anonymity-detector-anonymitaets-erkennung-vpn-proxy-detection



MEHR ZUM MODUL

paperoffice.ai/de/ki-anonymity-detector-anonymitaets-erkennung-vpn-proxy-detection

PREISE

paperoffice.ai/de/preise

KONTAKT

paperoffice.ai/de/kontakt