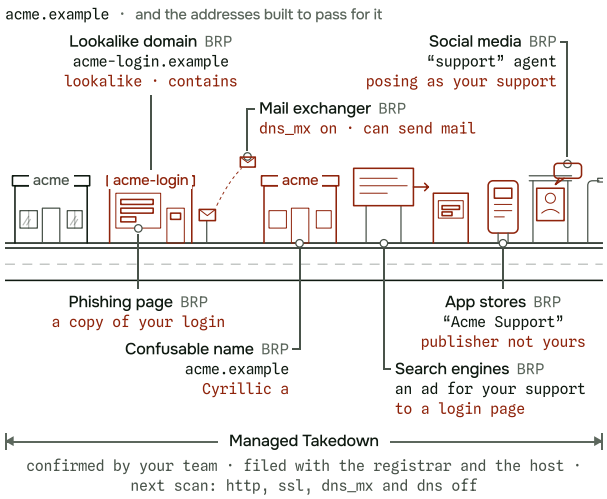
Find the Domains Built to Look Like You.

Brand Risk Protection matches new domains and subdomains against your brand keywords, including names spelled with letters from other alphabets that the eye cannot tell apart. Each lookalike your team confirms is then watched like an asset, so you see when it starts resolving, receiving mail or serving a certificate.

BRAND RISK PROTECTION

Find the Domains Built to Look Like You.

Brand Risk Protection matches new domains and subdomains against your brand keywords, including names spelled with letters from other alphabets that the eye cannot tell apart. Each lookalike your team confirms is then watched like an asset, so you see when it starts resolving, receiving mail or serving a certificate.



A Convincing Phishing Page Needs a Convincing Address.

An impersonation campaign needs a domain before it needs a phishing kit or a mailing list. Registering one is cheap, and the name can look exactly like yours.

REGISTRATION

Any Name, on Almost Any TLD

Your brand plus “login”, your name with one letter doubled, your exact name on a new extension. Each one is a separate registration that anyone can make.

RENDERING

Letters the Eye Can’t Separate

A Cyrillic “a” and a Latin “a” look the same in most fonts. In an email or a chat message, an internationalized name can read as yours while DNS resolves an `xn--` name underneath.

PREPARATION

Setup Leaves Traces

To host a login page a lookalike needs DNS records and usually a certificate. To send or receive mail it needs a mail exchanger, and each of those shows up in data the platform already collects.

One Watch From Lookalike to Takedown.

Fraudulent Domain Monitoring does the matching and the watching on domains. Social media, app store and search engine monitoring cover where customers meet your brand away from your domains, and Managed Takedown handles removal.

Fraudulent Domain Monitoring	Rules match new domains and subdomains against your brand keywords, from exact names to typos and confusable letters. Confirmed lookalikes are monitored for DNS, MX, SSL and HTTP activity, with a risk score kept as a timeline.	`Domains →`
Social Media Monitoring	Accounts on social platforms that present themselves as your brand or as one of its official channels.	`Social →`
App Store Monitoring	Apps listed in app stores under your brand name that your organization did not publish.	`Apps →`
Search Engine Monitoring	Results on search engines that use your brand to send people somewhere you don't control.	`Search →`
Managed Takedown	When your team confirms a lookalike is abusive, Deepinfo's takedown team files the removal requests and follows each one to a close.	`Takedown →`

Match Types That Catch What a Typo Filter Misses.

Each rule pairs a brand keyword with one match type. Below, one name and what four of the types would catch: the confusable types add the substitutions a typo filter never checks.

acme.example	YOUR KEYWORD Each rule pairs it with one match type
acme.test	SAME NAME `exact` The name itself, on another TLD
acrne.example	TYPO `fuzzy` One edit away: a dropped, doubled, swapped or mistyped letter
acme.example resolves as xn--cme-5cd.example	LOOKALIKE LETTERS `confusable_exact` Letters swapped for ones that look identical
acem.example resolves as xn--aem-4ed.example	LOOKALIKE AND TYPO `confusable_fuzzy` A typo and a lookalike letter together

From a Keyword to a Monitored Lookalike.

01 → 02 → 03 → 04 → 05

Rule

Pick a brand keyword and a match type, then narrow the rule: domains or subdomains, extensions to include or exclude, words that discard a match.

Match

The rule runs against new domains and subdomains as they enter Deepinfo's index. With `include_past` on, it also checks names registered before the rule existed.

Review

Matches arrive as suspicious domains, each with the rule that found it. Your team approves or ignores them one by one or in bulk, and can revert either decision. A rule you trust can approve its own matches.

Monitor

An approved match becomes a fraudulent domain. The platform tracks whether it resolves, receives mail, serves a certificate or answers HTTP, and keeps its DNS, SSL, WHOIS, web data and port history.

Act

File with the collected evidence yourself, or hand the case to Managed Takedown. A notification rule on `new_fraudulent_domain_detected` emails your team instantly or in an hourly to monthly digest.

What Each Lookalike Carries With It.

A match is not a verdict. Each record keeps what your team needs to decide, and the history to support a takedown request or a dispute later. These records also come back from the BRP API, under the platform's `apikey` header.

NAME	`fraudulent` and `fraudulent_unicode`: the name as registered, in `xn--` form for internationalized names, and the name as a browser displays it
TYPE	`fraudulent_type`: domain or subdomain
DETECTIONS	`detection_history`: the rules that matched the name, and when
STATE	`state`: `in_review`, `approved` or `ignored`, with the date of each decision
INDICATORS	`monitoring_indicator`: the flags `dns`, `dns_mx`, `ssl` and `http`, for whether the name resolves, receives mail, serves a certificate and answers on the web
LOGIN PAGE	`is_login_page` and `screenshot`: whether the lookalike serves a login page, and a capture of the page itself
RISK SCORE	`risk_score`: the current score, plus a timeline of how it has moved
HISTORY	DNS, SSL, WHOIS, web data and port scan history for each monitored lookalike

Query This Data Through the API

Lookalike matching runs over the domains the index sees each day. Data teams can take these domains as a feed and run their own matching. The index holds 400M+ domains, 2B+ subdomains, 200B+ DNS records and 30B+ SSL certificates.

Newly Registered Domains Stream FEED →	Domain Search API API →
Daily Registered Domains Feed FEED →	Same-Time Registered Domain Finder API API →

See Your Own Exposure, From the Outside.

REQUEST A DEMO

www.deepinfo.com/request-demo

PRICING

www.deepinfo.com/pricing

API DOCUMENTATION

docs.deepinfo.com

OFFICES

Istanbul (HQ)
Paris
Kuwait City

CONTACT

www.deepinfo.com/contact

SECURITY

security@deepinfo.com

© 2026 DEEPINFO