CYBEREINFORCE

BRAND PROTECTION

Look-alikes of your brand, found and blocked first.

A domain one letter away from yours is all it takes to send your customers a fake invoice. Cybereinforce watches every new website certificate, every new registration and the names most likely to be registered against you. Every look-alike is checked, blocked in protected browsers and reported to your SOC, usually before the first phishing email.

30 million+	**300,000**	**1,000+**	**250+**
new website certificates checked every day	newly registered domains checked every day, on average	domain extensions watched, from .com to country domains	most impersonated brands watched for every customer

FOUR PLACES EVERY LOOK-ALIKE SHOWS UP

MINUTES

Website certificates

A phishing page needs the padlock. Every trusted certificate is published in Certificate Transparency logs, and we read all of them.

DAY ONE

New registrations

New domains across more than 1,000 extensions are checked daily, so a look-alike is caught the day it is registered.

EVERY HOUR

Your likeliest look-alikes

Misspellings, look-alike letters and your name next to invoice, login or support, .de and .eu included.

LOOK BACK

Domains that already exist

Switch it on and we look back over existing registrations too, so you start with the full picture.

Every spelling that matters

Your domain and company name, watched in the spellings attackers use. Using Microsoft as the example:

`microsoft-login.com` `securemicrosoft.net` `rnicrosoft.com` `micros0ft.com` `microsoft.com (Cyrillic i)` `microsft.com`

- **Your name as a word or inside a word**, next to phishing vocabulary in eight languages
- **Misspellings**: letters added, dropped, swapped or replaced
- **Look-alike letters**: rn for m, digits for letters, Cyrillic and Greek characters

Checked, not just matched

- ✓ **Age.** The registration date comes straight from the registry. A look-alike registered in the last 30 days is blocked right away.
- ✓ **Owner.** Domains held by a brand's own specialist registrar are recognised as the brand's and left alone.
- ✓ **Evidence.** Every new sighting adds evidence, and a stronger signal turns a warning into a block.
- ✓ **People.** Anything that needs a human eye goes to our analysts, and a reviewed domain stays decided.
- ✓ **Your domains stay yours.** Your own domains are never flagged; mark a partner's as yours with one click.

FOLLOWED THROUGH EVERY STEP AN ATTACKER TAKES

STEP 1

Registered

Found and checked. A Microsoft Sentinel incident opens with the domain as its entity.

STEP 2

Given a certificate

It gets the padlock a phishing page needs. A second, higher severity incident opens.

STEP 3

Set up for email

Mail servers appear. Your administrators get an email, usually before the first fake invoice.

STEP 4

Taken down

One click: we report it with evidence to its registrar, host and browser blocklists until it is gone.

PLAN	PRICE	WHAT IS INCLUDED
Enterprise+	**Included**	From 100 licences: one watched domain per 500 licences.
Every other plan	**$29 / month**	Add-on billed annually ($348 a year). Two domains included, extra domains $10 a month each.
Takedowns	**$199 each**	Charged only once the domain is actually down. Nothing is due if it stays up.
Extended Check	**Per domain**	Deep search of existing look-alikes, parked and email-only ones included, one-off or monthly, with a PDF report.

See which look-alikes of your brand already exist.

Switch it on in your admin portal and the look-back starts straight away. Prices in USD, plus VAT where it applies.

Start free trial →