Domain Name Protection vs. Domain Name Privacy: What's the Difference?

Posted on August 26, 2025

An organization's domain name is one of its most valuable digital assets, so the desire to secure it is only natural. However, the terms used to describe these security measures—domain name protection and domain name privacy—are often used interchangeably, which can lead to confusion.

While both aim to protect, there are distinct differences, which we discuss in greater detail in this post. Please refer to the table below for the TL;DR version.

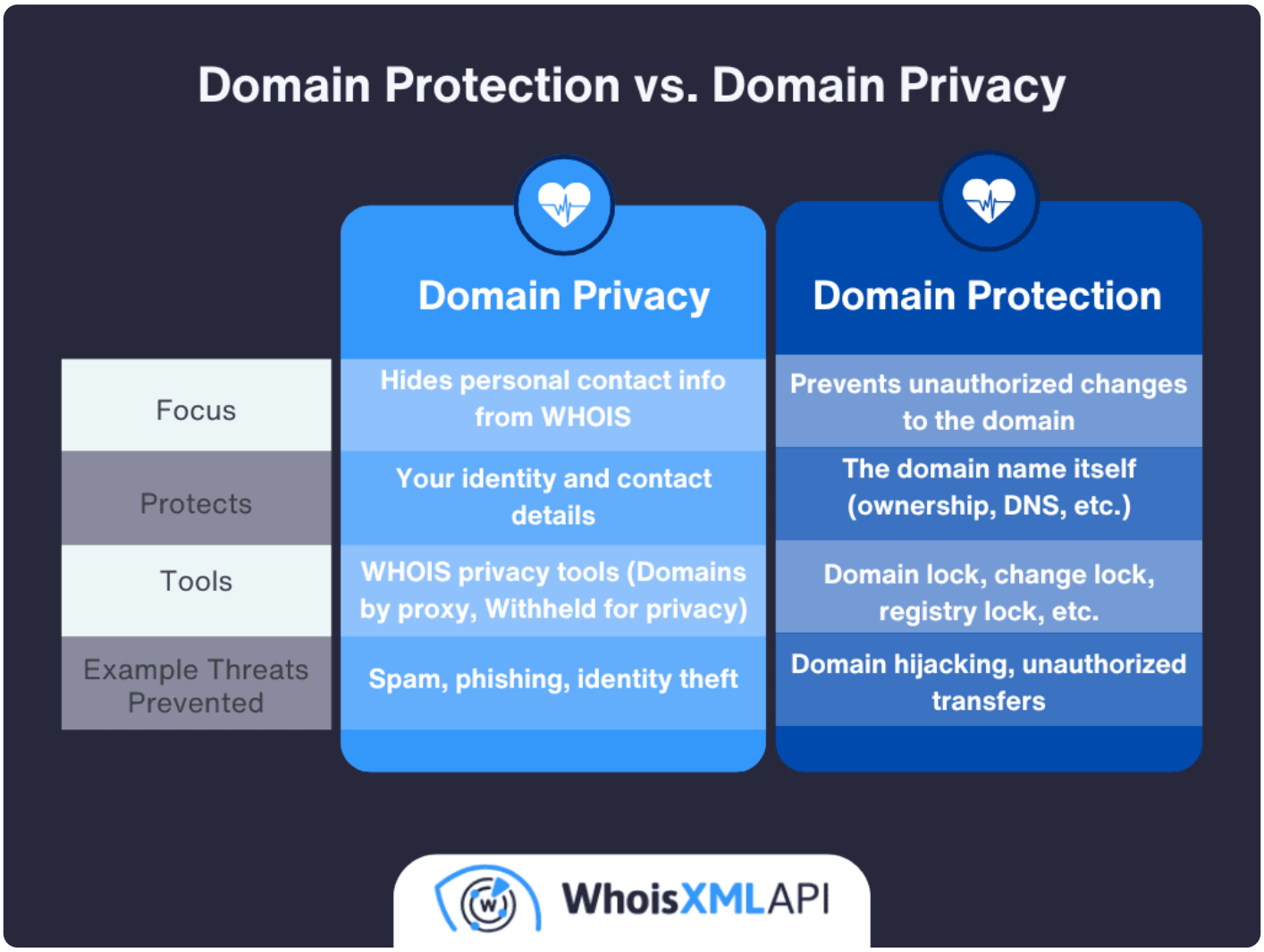


Figure 1: A table comparing domain privacy and domain protection

Domain Name Privacy

Domain name privacy, also known as **WHOIS privacy protection** or **domain privacy protection**, is a service designed to protect the online presence of a domain registrant. When you register a domain name, the Internet Corporation for Assigned Names and Numbers (ICANN) mandates that your personal data — including your name, address, email address, and phone number — be publicly available in the public WHOIS database to ensure accountability and provide a means of contact for legal or administrative purposes.

However, this public record accessibility has a significant downside. Your personal details are laid bare for anyone to see, making you a target for a host of digital nuisances and threats. Domain privacy services act as a digital shield, preventing this exposure. They protect you from common threats such as contact scraping, identity theft, phishing, and spam.

Domain Name Privacy Service Providers

Some domain privacy providers are independent and work with different registrars, while others are associated with specific registrars. One of the biggest domain registrars, Namecheap, for example, currently relies on Withheld for Privacy that is exclusive to it. Previously, Namecheap used WhoisGuard, which is also available through other registrars, such as PublicDomainRegistry.com and Porkbun. Here's how the WHOIS records of domains protected by Withheld for Privacy and WhoisGuard look like.

Withheld for Privacy **Whoi**

Registrant Contact

Registrant Name: Withheld for Privacy Purposes >
Registrant Organization: Privacy service provided by Withheld for Privacy ehf >
Registrant Street1: Kalkofnsvegur 2 >
Registrant City: Reykjavik >
Registrant State/Province: Capital Region >
Registrant Postal Code: 101 >
Registrant Country: ICELAND >
Registrant Email: d750ceaff0f34d2f83979ade11509e10.protect@withheldforprivacy.com >
Registrant Phone: 3544212434 >

Current WHOIS registrant details of arbitrary[.]ai *Curre*

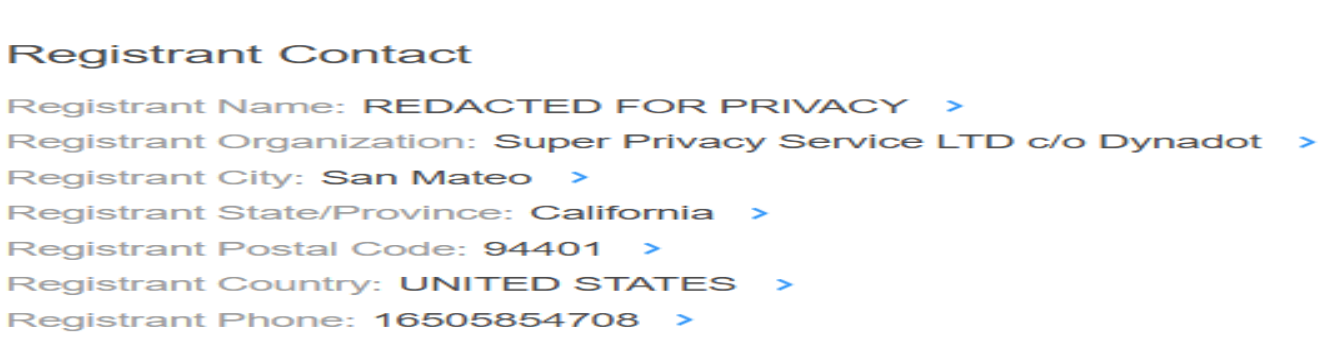
Other popular domain name privacy service providers are Domains By Proxy and Contact Privacy,

which are offered through two other major registrars — GoDaddy and Tucows, respectively. Dynadot also has its domain privacy protection service called Super Privacy Service. Meanwhile, Cloudflare redacts WHOIS registration details completely as a standard feature, so domain registrants don't have to use third-party domain privacy services. Here's a look at what each of these domain privacy protection looks like.

Domains By Proxy

Current WHOIS registrant details of rpbrokers[.]com

Super Privacy Service



Current WHOIS registrant details of brghton[.]com

How Domain Name Privacy Works

When you enable domain privacy, your registrar doesn't actually remove your information from its records. Instead, it replaces your personal contact details in the public WHOIS database with anonymized information or with the details provided by the domain privacy service it partners with. Here’s what typical WHOIS registrant details look like before and after domain privacy is enabled:

Before domain privacy protection	After enabling privacy
Name: John DoeEmail: john.doe@example.comAddress: 123 Main St, Anytown, USA	Name: Domain Privacy ServiceEmail: proxy123@privacyservice.comAddress: 123 Privacy St, Obscurity City

Any communication intended for the real domain owner, such as an abuse complaint or legal notice, is forwarded through this proxy email. This means it's still possible to reach the domain owner, but their identity and personal information are not publicly visible and cannot be abused.

Important Considerations on Domain Name Privacy

There are a few things to keep in mind when it comes to domain name privacy protection.

- **Not all TLDs allow it**: Not every country's domain registry allows for WHOIS privacy. Extensions like .us (United States), .ca (Canada), and .in (India), for example, have stricter rules and require public disclosure of domain name registrant information.
- **Pricing varies**: Some registrars, like GoDaddy, might charge extra for domain privacy as an add-on or bundle it with a higher-tier service package. Others, like Namecheap, offer it for free with every domain registration.
- **Post-GDPR WHOIS redaction**: After the implementation of GDPR, WHOIS has significantly changed. Many registrars now automatically redact personal data by default for domain registrants in the EU, reducing the need for traditional domain privacy add-ons.

How to Check If a Domain Uses Domain Name Privacy

You can easily check a domain name's privacy status by performing a WHOIS lookup using any of the free tools available online. Enter the domain name on the tool, and the results will show you the registrant's details.

If you see phrases like "Redacted for Privacy," "Withheld for Privacy," or "Proxy Service," it means that the domain is using a privacy service.

How to Find Contact Details For a Privacy-Protected Domain

Even with domain privacy enabled, there are still ways to get in touch with the domain owner:

- **Use the proxy email**: You can still write an email to the anonymized proxy address listed in the WHOIS record. The registrar is then responsible for forwarding that message to the real owner.
- **Use WHOIS history**: The WHOIS History API can show you what the records looked like before privacy was enabled or before GDPR redactions took effect. This can sometimes give you access to older, unredacted contact information.

Domain Name Protection

Domain name protection refers to a set of security features that help prevent unauthorized changes, domain hijacking, loss of your domain name, or domain transfers without authorization. While domain privacy protects your personal data, domain protection focuses on safeguarding the domain itself so it doesn't fall into the wrong hands or be accidentally deleted.

It’s worth noting that domain protection does not involve only one service but rather a suite of tools that registrars and third-party companies offer to protect your domain.

How Domain Name Protection Works

Here are six tools that make up a strong domain name protection strategy:

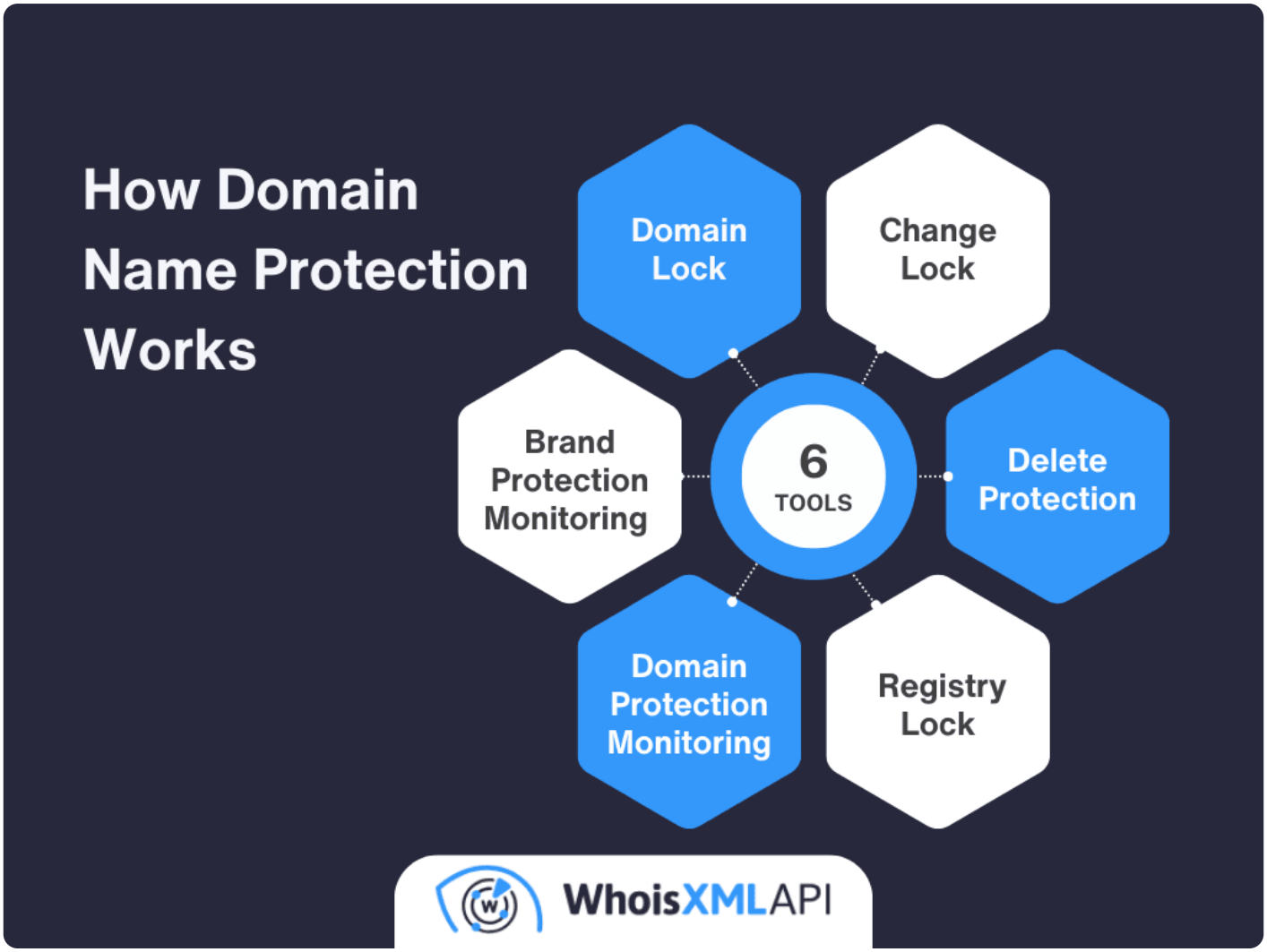


Figure 2: Domain name protection tools and techniques

1. Domain Lock

Domain lock (also known as **Registrar Lock**, **Transfer Lock**, or clientTransferProhibited status)

prevents your domain from being transferred to another registrar. When a domain is locked, any transfer request is automatically declined, keeping your domain safe against domain hijacking, which can occur through unauthorized registrar transfers and accidental or malicious transfer-out requests.

To transfer your domain, you must first manually unlock it in your registrar account. You can check if a domain has this lock enabled by performing a WHOIS lookup and looking for the status clientTransferProhibited. You can watch this webinar to learn more about domain statuses.

2. Change Lock

A **change lock**, sometimes called an **update lock** or **change protection**, is another registrar lock that prevents any unauthorized modifications to your domain's DNS records and WHOIS information. This helps prevent DNS hijacking, where an attacker changes your DNS settings to redirect your visitors to a different server.

A change lock also stops anyone from altering your contact information without your permission, which can ward off social engineering attempts and accidental misconfigurations. A WHOIS record for a protected domain will often display the status clientUpdateProhibited.

3. Delete Protection

You can also protect your domain from being mistakenly or maliciously removed from your account by ensuring that the WHOIS status is clientDeleteProhibited, which is another registrar lock.

4. Registry Lock

For high-value or mission-critical domains, a **registry lock** provides the highest level of security. This is a server-side lock that must be enabled directly at the domain registry, not just at the registrar level.

A domain registry lock means that even if the registrar account is compromised, your domain will remain safe, since it makes any unauthorized changes—including deletion, transfer, or modification of nameservers—virtually impossible without an extensive, multi-step authentication

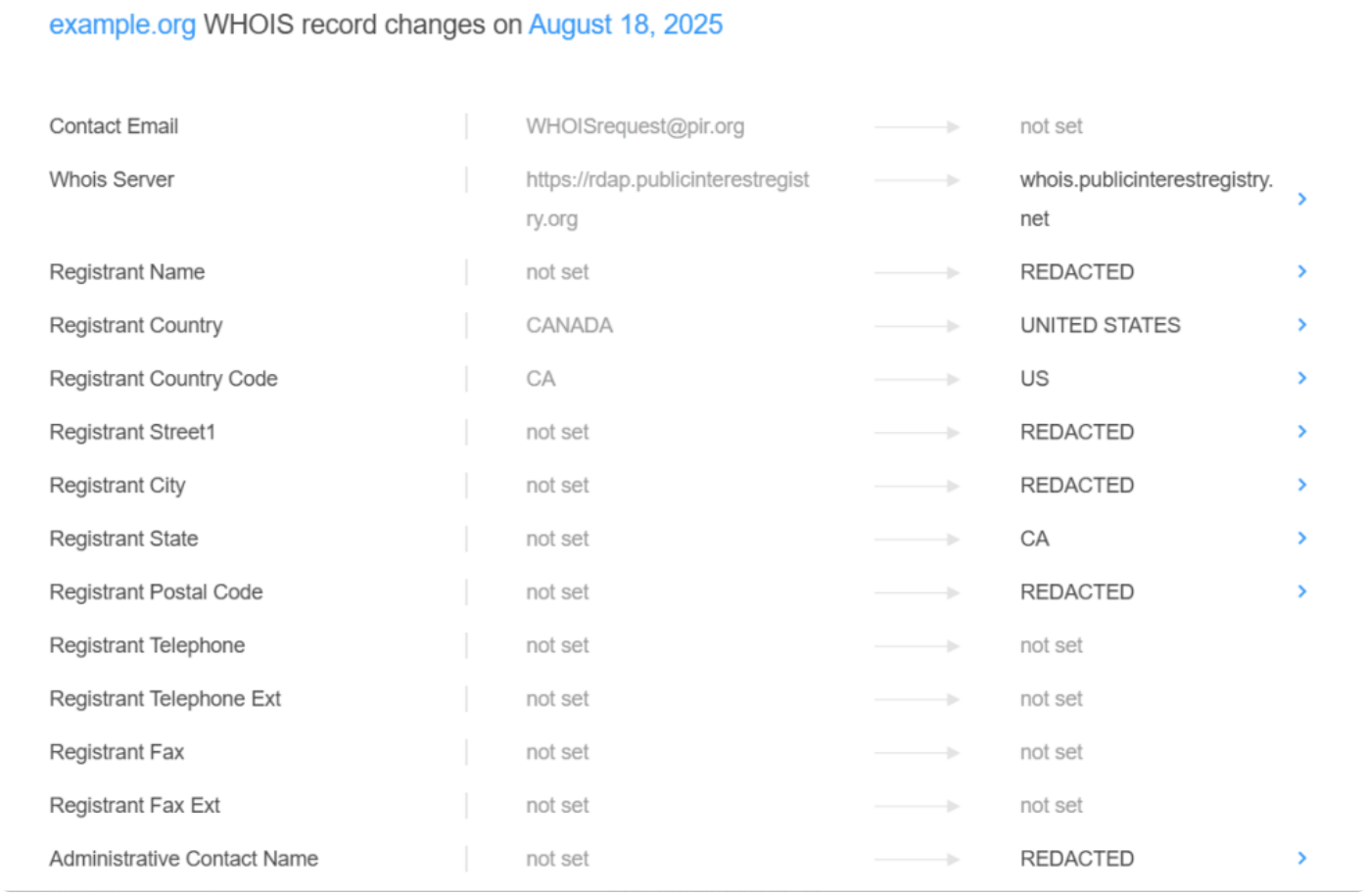
process between the registrar and the registry itself.

This process may involve phone verification, SMS notification, passphrase confirmation, or even manual paperwork. You can check for a registry lock in a WHOIS record by looking for domain statuses like serverTransferProhibited, serverUpdateProhibited, or serverDeleteProhibited.

5. Domain Protection Monitoring and Alerts

Another way to stay on top of domain protection is to set up alerts for when your domain name's WHOIS configuration changes. This is a proactive way to help detect suspicious activity right away.

You can use WhoisXML API's Domain Monitor tool for this. The tool can be configured to send emails when WHOIS record changes are made, and you can see exactly what data points were modified.

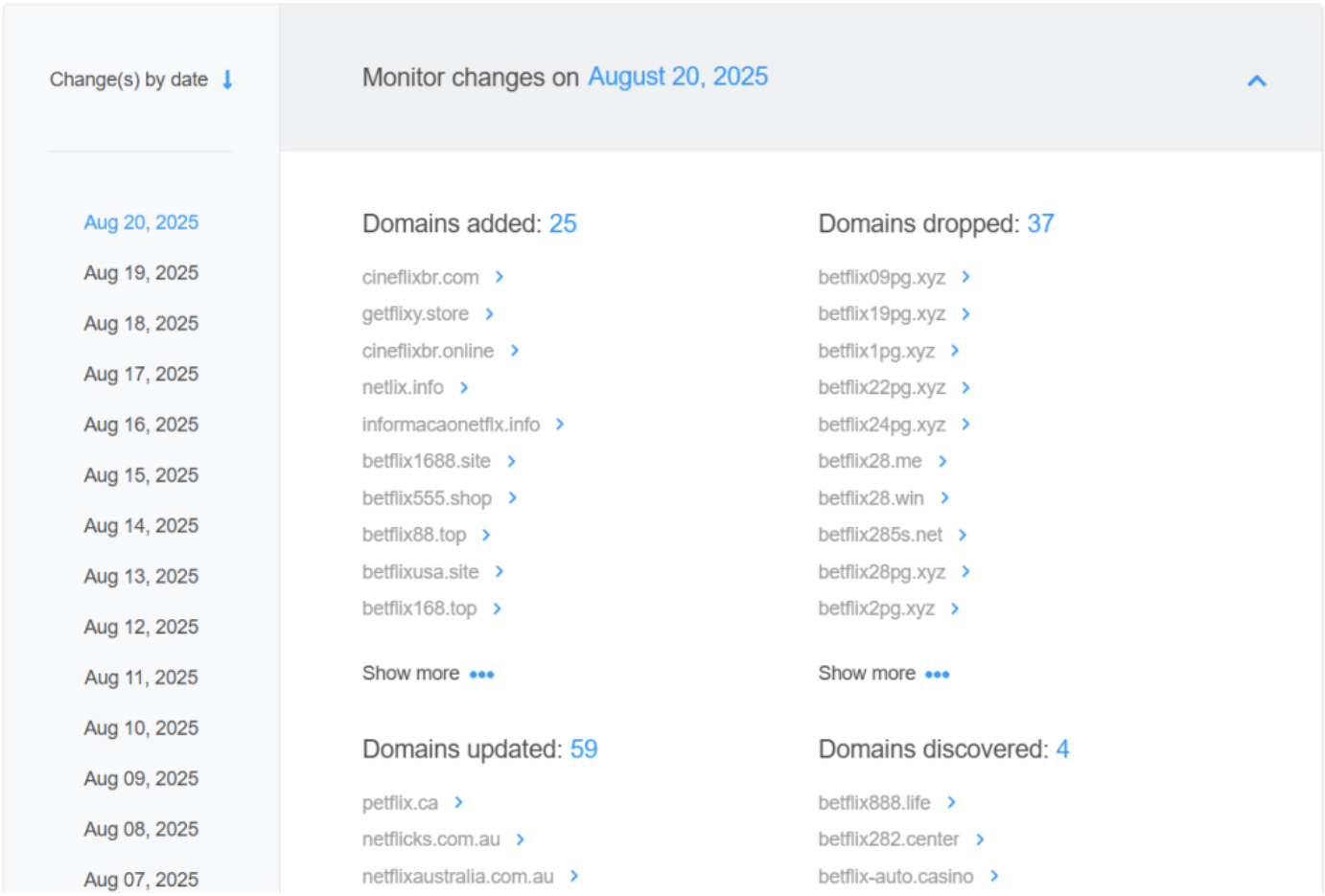


6. Brand Protection Monitoring and Alerts

You can also go a step further and get notifications not just about your domains but your entire brand. This helps you react quickly to brand-related threats such as cybersquatting, impersonation, and more. Threat actors often register cybersquatting domains or domains similar to a legitimate company's domain to impersonate that organization.

Brand monitoring services like WhoisXML API's Brand Monitor can alert you when someone registers a domain that closely resembles your domain name. Here's an example of a brand monitor we set up for Netflix, which showed that 25 look-alike domains were added in one day

alone.



What Else Should You Do to Protect Your Domain

Aside from the techniques and tools above, there are other security measures you can take for your domain name protection, including the following.

- **Choose a trusted registrar:** A reputable registrar will have advanced security features and easy-to-access customer support to help if something goes wrong. Also, something is just less likely to go wrong with a provider that cares about its reputation.

- **Set up 2-step verification (2FA)**: This is non-negotiable. Enabling 2FA on your registrar account makes it much harder for a hijacker to access your domain, even if they have your password.

- **Turn on domain auto-renewal**: About 60% of data breaches involve human error, according to Verizon's 2025 Data Breach Investigations Report (DBIR). For this reason, it's better to automatically renew domain registrations and not rely on remembering to do it on time. This helps avoid the risk of missed renewals, which can lead to legal actions, where the new owners may still legally keep the domain.

Conclusion

Domain privacy refers to a specific service that shields your online presence and personal information from the public, while domain protection is a security strategy that involves the use of various tools to prevent unauthorized changes and domain removal. Both are important for domain owners as they help secure their most important digital asset.