



 **GLOBALBLOCK**

Domain Name Blocking Redefined:

Your Guide to Smarter Brand Protection

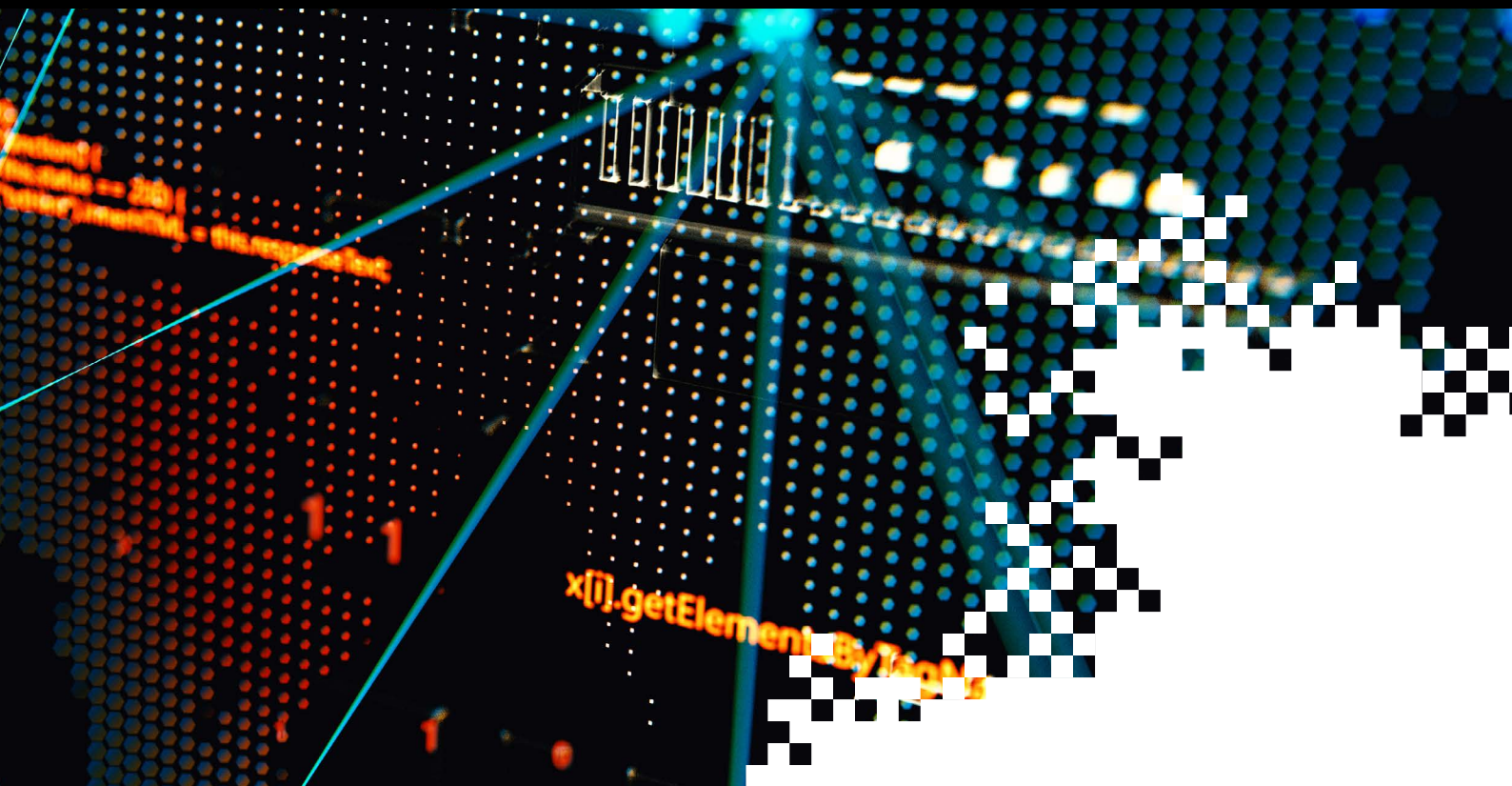
www.globalblock.co

January 2025



TABLE OF CONTENTS

- 01.** Forward
- 03.** A History of Domain Blocking
- 05.** What is Domain Blocking
- 07.** Domain Names and Intellectual Property
- 11.** Why Domain Blocking Should Form Part of a Brand Protection Strategy
- 15.** Improved Domain Management with GlobalBlock's Key Features
- 17.** Four Innovative Ways to Use GlobalBlock



Foreword

Protecting your brand in today's online landscape is more critical than ever.

Brand managers face an array of unprecedented challenges, from rapidly expanding areas of risk to the increasing pressure of shrinking budgets.

With these realities in mind, how can organizations overcome the challenge of “protecting more with less”? Where does innovation fit into the equation, and how can we rethink traditional approaches to explore solutions like domain name blocking through a fresh lens?

This report is designed to provide brand owners with key insights on how domain blocking can help improve your domain portfolio's efficiency whilst generating significant cost savings and operational benefits.

The journey to creating the Brand Safety Alliance and the GlobalBlock service began several years ago. It started with extensive exploratory interviews with large corporations to better understand their challenges regarding domain names and their impact on holistic reputation management and brand protection practices.

A common theme emerged from this research: the desire for a simplified and more effective approach to domain names and brand protection. We learned that brands are dealing with new threats in an evolving industry. They are also struggling to manage as the budgets to deal with these threats continue to shrink—including navigating countless providers, services, rules and conditions, pricing, and technology offerings.

Historically, a relatively simple domain portfolio would have included <corebrand>.com/.net/.org/.info/.biz, and a handful of relevant ccTLD registrations. Today's portfolio can now include thousands of variations to the left-hand side of the dot, multiplied by thousands of extensions on the right. For just about every brand on the planet, this strategy is not affordable nor capable of ensuring the required level of protection.

Primarily, throughout this research phase, we saw an opportunity – and a desperate need – to be more customer-led in how the domain name industry protects intellectual property online.

The early assessment concluded that the best approach was to develop a global domain blocking service. Domain blocking provides a broader scale of protection and enabled real cost benefits to brand owners that are experiencing unprecedented budget pressure.

Beyond this, we knew that the expansion of the internet had created a truly global problem for brand owners in protecting their identities, and it required an equally global solution.



GlobalBlock officially launched in early March 2024 and at the time of publishing this paper, includes more than 600 web extensions across new and legacy gTLDs, ccTLDs, and Web 3.0 namespaces. We are strategically broadening our namespace offerings, with an ambitious pipeline of additional extensions. With the next round of new TLDs on the horizon, we are also focused on creating a better outcome for rights protection and IP owners during this time.

The ability to block domains at this scale and do so for proactive brand protection purposes is revolutionary. It prompts a re-thinking of how brand protection specialists can incorporate blocking into their IP protection strategies.

This white paper is designed specifically to create context for brand owners around the world. It provides an overview of blocking, how it works and its role in brand protection, as well as how GlobalBlock has expanded the possibilities of domain blocking to provide ease, simplicity and peace of mind in the complex space of domain name portfolio management.

We hope you find this paper to be a helpful tool in your toolkit, and that it demonstrates how domain name blocking can revolutionize your brand protection strategy.

Sincerely,



Ben Anderson - Product Director



Tony Kirsch - Commercial Director



A History of Domain Blocking

For many years, the primary defense against brand imitation and fraud using domain names was to register any domain matching your brand before the bad actors could.

However, as businesses grew to include more brand and product names, the internet expanded to include thousands of domain extensions (including those from the 2012 new TLD program). This approach has become increasingly complex and resource-intensive for many brand owners to maintain at scale.

In 2011, ICM Registry introduced the .xxx domain extension for use by the adult entertainment industry. While the extension had a niche target market, many global brands faced a challenging situation. On one hand, they didn't want to be seen as registering .xxx domains and aligning their brand with this industry. On the other hand, a brand could not afford to have domains matching their brands purchased by squatters or anyone intending to damage their brand with adult content.

To solve this issue, ICM Registry introduced a blocking service through which brands could prevent their trademarks from being registered as a .xxx domain. This 'Sunrise B' program removed domains from the market for 10 years, without the need to register, manage or renew them.

This service was later expanded into the popular AdultBlock service in 2019, adding the other adult-themed extensions: .porn, .adult, and .sex. This particularly appealed to companies who did not want to register an adult domain and create an association between their brand and the adult entertainment industry.

Since then, other blocking products have followed suit, protecting trademarks in various extensions covering around a third of the market.

One of the more widely recognized is the Domain Name Protected Marks List (DPML) service, which blocks domains across approximately 300 extensions including .fail, .fyi, .info, and .group. Other blocking services have also since launched; however, they are typically selective or carry only a small number of extensions.

While appealing to brand owners, these blocking services only solved a piece of the puzzle as there remained no simple, unified approach to blocking on a widespread scale that covered all types of web extensions where brand owners needed protection.

Through this, the Brand Safety Alliance (BSA) evolved with a vision to service the needs of brand owners and create a safer internet. The BSA is dedicated to developing products and services that allow brand owners to protect their online identity.

In 2024, the BSA introduced GlobalBlock, the largest domain blocking service to enter the market. GlobalBlock launched with more than 500 domain extensions included in its coverage, and a unique approach that aims to continue to grow this coverage over time. Today, GlobalBlock supports over 600 domain extensions, with

plans for continued growth and innovation.

It's current coverage includes gTLDs, ccTLDs and Web3.0/Blockchain extensions.

By adding features that solve issues with domain portfolio management and brand protection, GlobalBlock represents a new era of domain blocking.



2011

ICM Registry introduced the .xxx domain extension for use by the adult entertainment industry.



2013

Domain Name Protected Marks List (DPML) service, which blocks domains across approximately 300 extensions.



2019

AdultBlock added the other adult-themed extensions .porn, .adult and .sex.



2024

The BSA introduced GlobalBlock, the largest domain blocking service to enter the market. Its coverage includes gTLDs, ccTLDs and Web3.0/Blockchain extensions.

What is Domain Blocking?

Unlike defensive domain name registrations, a blocked domain name cannot be used for websites, email, or other purposes. The domain itself is placed in the company's blocking account, removing it from public access and availability altogether, meaning no other party can register or use it.

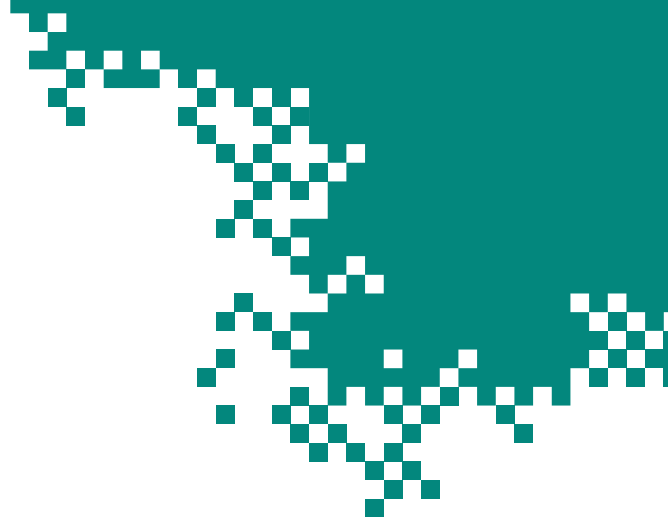
This is achieved by implementing the block at the Registry level, providing greater security, scalability and protection to the brand owner in web extensions where the brand has no intention of using the domain, as they are not required to maintain the registration and continue paying associated individual domain name renewal fees.

Additionally, certain domain blocking services have additional benefits for brand owners and often include features that block variations of brand names, such as using visually similar characters and/or lookalike characters from different languages to imitate a domain – tactics often engaged by bad actors to trick consumers into clicking fraudulent links or trusting false emails. Identifying and defensively registering these across hundreds of domain extensions would be resource-intensive and challenging to maintain.

As a result, blocking can serve as an efficient tool in helping to manage domain-related risks, reduce administrative complexity and contribute to operational efficiencies.

While domain blocking is not a silver bullet for all online brand abuse, it is a crucial new tool in the online protection toolkit, offering a way to proactively reduce the burdens of large portfolios while helping provide peace of mind against brand challenges.





REGISTRY:
operates the
domain extension
and allocates
domains



GLOBALBLOCK:
blocks names
before they're
released

REGISTRAR:
sells domains to
the public



**REGISTRANT/
BUSINESS/BRAND:**
registers the domain
to use or protect



Domain Names and Intellectual Property

Why Domain Names Should Be Treated as IP Assets

Domain names occupy a unique position in intellectual property law. While not automatically protected as intellectual property, domain names can receive various forms of IP protection, particularly when they function as trademarks or source identifiers.

Despite this, they play a critical role in establishing digital identity and brand recognition.

Digital assets like domain names have emerged as valuable business assets that typically require protection through a combination of traditional IP rights and specialized safeguarding measures.

They are often the first interaction point with customers, significantly impacting trust and brand reputation.

In this context, brands need to consider protecting domains with the same rigor as other IP assets; to preserve brand reputation, protect customers and avoid costly brand infringement.

Domain names are unique identifiers

By definition, two companies or individuals cannot have the exact same domain name. A domain uniquely distinguishes a business from its competitors and forms part of the customer experience.

This places it squarely alongside logos, taglines and other assets as a piece of your brand. Suppose a domain name is lost, misused, or copied by a competitor or malicious actor. In that case, it can lead to confusion among consumers, dilute the brand's identity, and erode the competitive advantage that the business has worked to establish.

Domain names are vulnerable to cybercrime

Protecting branded domain names is critical to maintaining a business's reputation, as they are particularly susceptible to various forms of brand abuse. Abuse by bad actors can lead to severe consequences including financial losses, reputational damage and loss of consumer trust.

Domain names require a financial investment

The cost to acquire, maintain and manage a domain can make it a significant financial investment for businesses. Domain costs can include registration or purchase from a third party (potentially at a premium), ongoing renewal fees, and any costs of domain management.



On the other hand, the costs of recovering or disputing a domain that has been used maliciously can also be substantial, especially for domains that underpin key online activities like websites or email or are tied to flow-on costs for hosting, design, marketing, and more.

Safeguarding these domains ensures that the time, money and effort invested does not go to waste.

Brand Risks of Domain Abuse

In dollar terms, the consequences of a brand's domain name falling into the wrong hands can be significant. Domain squatters – bad actors who register domain names they believe to be high-value, such as those relating to brands and companies – can attempt to hold a domain to ransom.

The processes for purchasing it back or disputing ownership to have it returned can be time-consuming and costly, not to mention the ongoing reputational damage of such a dispute or of the domain being misused in the meantime.

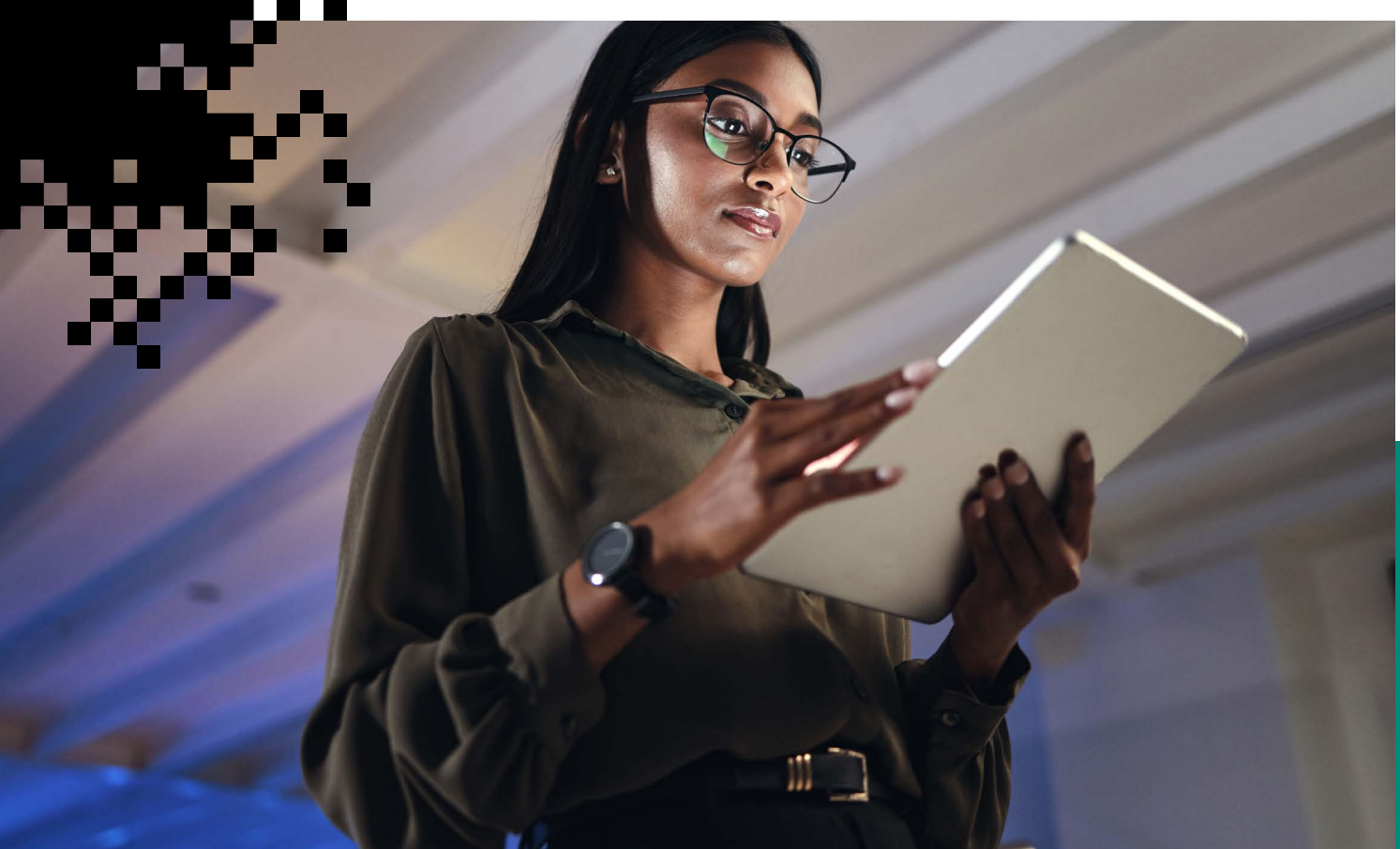
For example, a request under the Uniform Domain Name Dispute Resolution Policy (UDRP), one of the most common ways to contest a domain name, can cost around USD\$1,500 just to file for up to five domains, in addition to legal support costs.

However, a UDRP dispute typically takes around two months to complete, which could be enough time for the domain to be used for nefarious purposes. These disputes also rely on demonstrating that the domain is being used in bad faith – such as to hijack traffic or imitate a brand.

Despite this, total UDRP filings over the past three years have continued to grow compared to the previous historical three-year period (totaling 16,743 filings from 2021-2023 compared to total of 11,344 filings from 2018-2020) according to WIPO statistics, as brands are left with few other options to combat bad actors. On the other hand, in some cases, domains held by third parties have been listed for resale at significant prices, with documented examples ranging from thousands to tens of thousands of dollars.

Some bad actors, however, have a more sophisticated plan. Scammers can attempt to imitate brands and organizations using domains that appear to be legitimate for the purposes of phishing, fraud, humiliation or other forms of deception. This can result in financial, reputational and operational damage and costs far beyond the price of registering a domain.





With the expansion of the domain name system to include ‘internationalized domain names’, characters other than those in the ASCII alphabet (a through z) can now be registered in domains. This created possibilities for impersonating a brand using confusingly similar characters from other alphabets such as Cyrillic or Greek to imitate brand names.

Recognizing the growing challenges with confusingly similar domains, including those using non-Latin characters, the Brand Safety Alliance developed GlobalBlock+ to offer additional protective features for brand owners.

The problems caused by online brand imitation are growing.

In Q2 2023, the Anti-Phishing Working Group (APWG) observed more than 1.28 million phishing attacks worldwide: the third-highest quarter on record. This doesn’t account for attacks that may have gone unnoticed or unreported. The World Economic Forum also reported that in 2020, malware and ransomware attacks increased by 358% and 435% respectively.

With a domain name that appears legitimate, this risk increases. A survey conducted by Proofpoint found that 63% of participants think that an email address always belongs to the corresponding website of the brand, and 44% believe an email is safe when it features familiar branding.

The APWG reported that business email compromise, one of the most common forms of online fraud, has resulted in \$50.8 billion dollars in losses between October 2013 and December 2022.

While the growth of the domain name industry has created more opportunities for creativity and more availability of domains, this, in turn, has increased the challenges for brand owners – and the need for additional tools to complement existing brand protection strategies.



Why Domain Blocking Should Form Part of a Brand Protection Strategy

Businesses invest a lot of time and money in domain names.

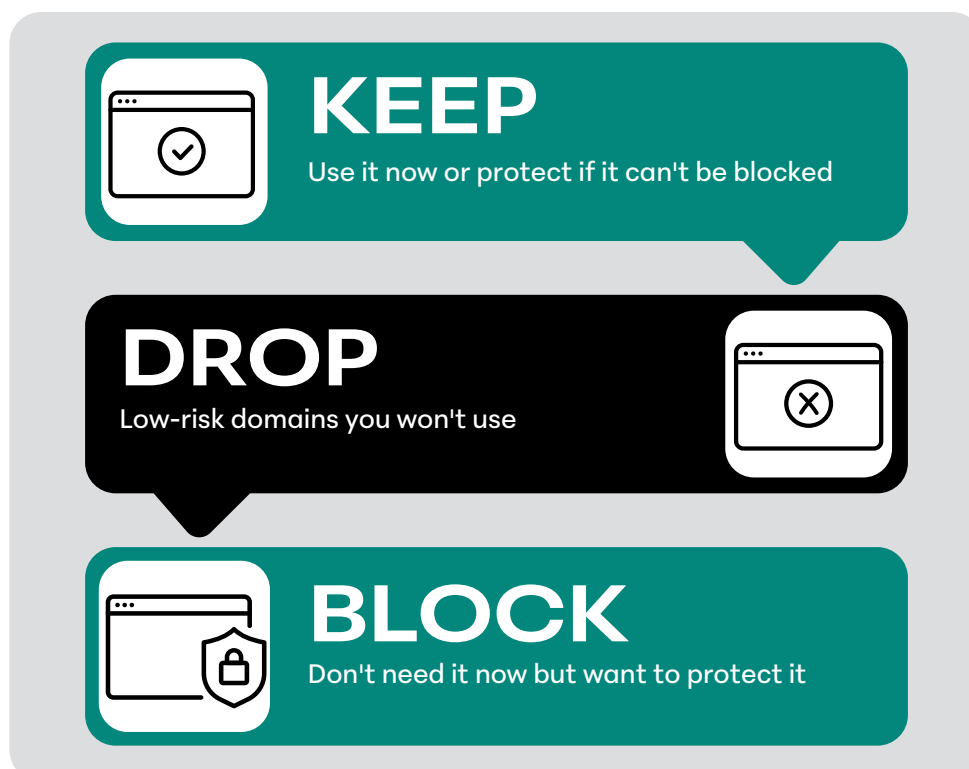
In fact, GoDaddy Corporate Domains' analysis of the [Global 2000 companies in 2022](#) found that the top 50 had an average domain portfolio of around 8,300 domains and spent an average of \$373,000 on domains per year.

Furthermore, companies with [10,000 domains](#) dedicate at least 4-5 days a week to managing them all, so it's no wonder corporations are constantly looking for ways to be more efficient and this is not limited to internal staff.

[External corporate domain management providers](#) now prioritize helping customers “rightsize” portfolios, acknowledging that the historical approach of just registering every domain isn't sustainable.

Domain blocking is now emerging as an additional tool in the online brand protection kit, providing a viable and reliable alternative to large defensive domain name portfolios.

Keep, Drop or Block



When to Register and Keep

Registering a domain and keeping it in the portfolio means committing to its ongoing management and, in some cases, treating it as a corporate asset and managing it as one accordingly, even if it is for one-time use. This includes meeting eligibility requirements, tracking renewal terms, and paying ongoing registration fees.

Registration may be particularly appropriate when:

- ✓ **The brand uses the domain in its business (for a website or email, for example)**
- ✓ **The domain benefits from traffic that is funneled to other company properties**
- ✓ **The brand plans to use it in future**
- ✓ **The domain uses non-trademarked terms where the brand can't claim ownership**
- ✓ **It could reasonably be used to imitate the brand**
- ✓ **It can't be protected through a blocking service**

This approach recognizes that domain names are an essential element of a digital brand and should be protected from misuse. It also focuses on the future by securing domains needed down the track, before they hit the spotlight.

The downside of this strategy is that every domain adds to the size of the portfolio, increasing its complexity and cost of management.

When to Delete or Expire

Portfolio optimization may include evaluating domains for potential deletion or non-renewal. This process can help manage costs and administrative overhead, as each domain typically requires ongoing fees and management resources.

Brands often consider removing domains from their portfolio when:

- ✓ **The domain's characteristics make it unlikely to be used for brand imitation**
- ✓ **A brand has no current or planned use for the domain (following risk assessment)**
- ✓ **The maintenance costs exceed the domain's strategic value**



Naturally, there are risks in releasing domains back to the open market. Expiring domains can pose significant risks to your brand if not managed carefully. Opportunistic third parties relentlessly monitor domain expirations and quickly seize those domains tied to well-known brands. These domains are often resold at inflated prices or leveraged to extract payment directly from the brand. To safeguard your reputation and mitigate potential financial and legal risks, consider implementing a gradual deactivation strategy to reduce the domain's resale or misuse value over time.

When to Block

Now, domain blocking services offer a viable option to add to a domain management strategy. Domain blocking services scan for available domains matching a brand and block them at the Registry level. This means the available domain matching the brand cannot be registered and the brand benefits from automated domain management and renewal processes.

Blocking a domain may be particularly appropriate when:

- ✓ **A brand doesn't want to use a domain, but also doesn't want to take the risk of someone else owning it**
- ✓ **A brand wants to protect domains at scale**
- ✓ **Traditional registration isn't feasible due to eligibility requirements**
- ✓ **The blocking service covers the domain extension in question**

It is important to understand that not all domains can be blocked and blocking can't impact domains already registered by someone else. While blocking services provide additional valuable tools for domain management, they should be evaluated as part of a broader brand protection strategy.

Finding the Right Approach

Incorporating domain blocking into the domain management and brand protection strategy means that to keep or to drop is no longer an either/or decision.

To determine whether to register, delete or block a domain, some of the factors that should be considered include:

- ✓ **Cost of registering/retaining a domain or blocking a domain, in conjunction with the available budget**
- ✓ **How closely the domain resembles the brand**
- ✓ **If the domain is currently in use, used in the past or likely to be used in future**
- ✓ **If blocking is available based on the domain extension**
- ✓ **Likelihood of reclaiming the domain if registered by a third party (for example, through trademark claims or domain dispute processes)**

The three-pronged approach of keep, drop or block provides flexibility in managing domains and helping protect brands from imitation and abuse online.



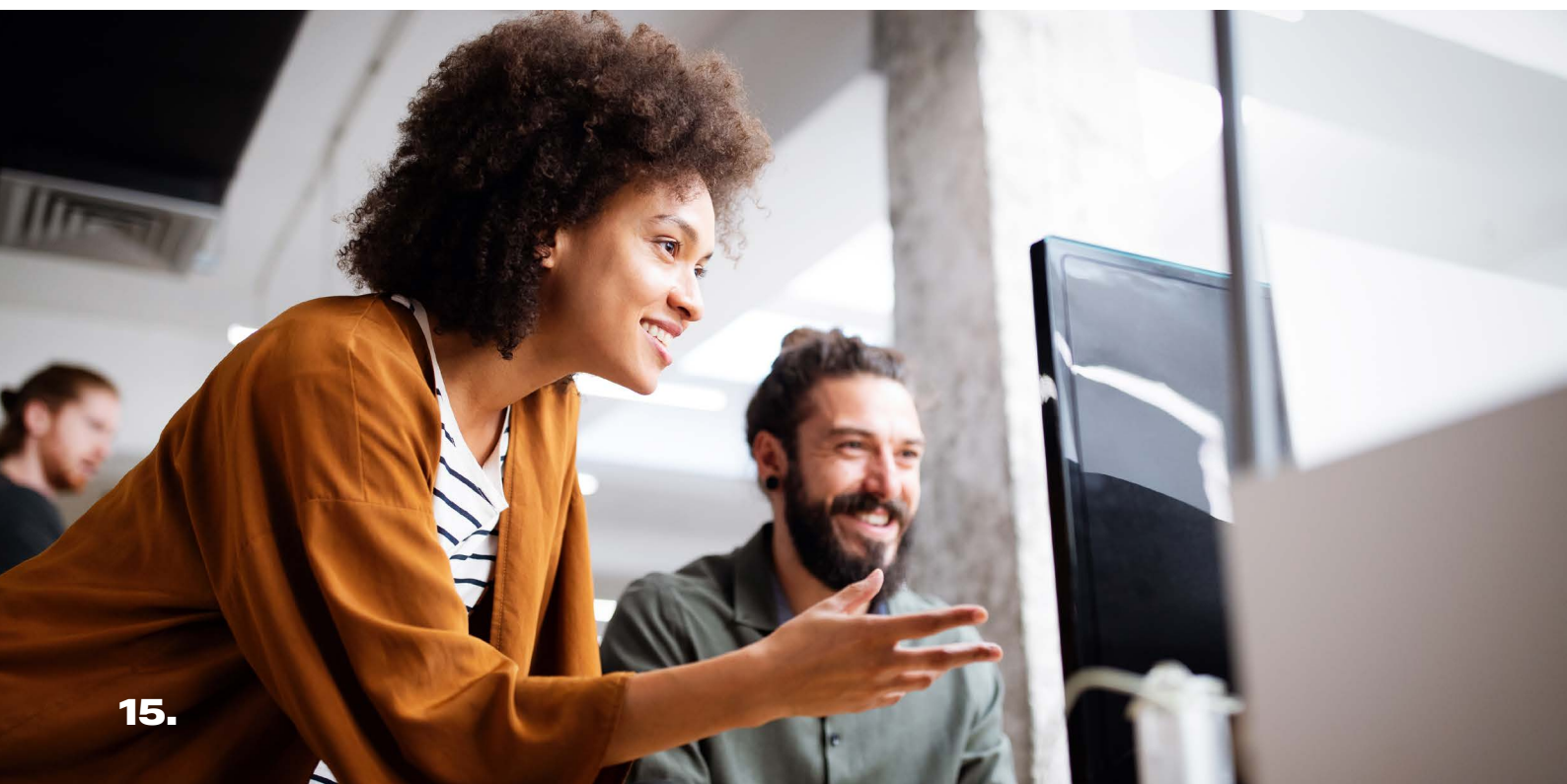
Improved Domain Management with GlobalBlock's Key Features

In addition to the largest coverage of any domain blocking service* as detailed below, GlobalBlock includes several unique features designed to simplify brand protection and address the challenges of managing domain portfolios.

Together, these features are intended to:

- ✓ Help reduce opportunities for unauthorized domain use and stay ahead of bad actors
- ✓ Save time on endless defensive domain registrations
- ✓ Assist in managing certain domain-related costs, such as domain acquisition and brand monitoring
- ✓ Provide additional safeguards against human error and lost domains
- ✓ Helps brands manage risks associated with online fraud and its potential reputational, commercial, and technical impacts
- ✓ Complement existing brand protection and domain management strategies

*Based on October 2024 publicly available data for number of TLDs/Extensions in a single blocking service compared to blocking services from leading competitors.



Key GlobalBlock Features



UNPRECEDENTED PROTECTION

GlobalBlock is the largest domain blocking service in the world. With GlobalBlock's real-time blocking solution, your brand can stay protected across 600+ domain extensions in a wide range of namespaces, including extensions your brand isn't eligible to register.

A list of included extensions can be found on the [GlobalBlock](#) website.



EXPANDING COVERAGE

GlobalBlock, backed by the Brand Safety Alliance team of industry experts, is dedicated to keeping your brand protected as the digital landscape evolves. Our mission is to continuously expand our coverage to add as many TLDs as possible, including legacy, new gTLDs, and TLDs to come in the next ICANN round.



PRIORITY AUTOCATCH

Stay ahead of bad actors with our groundbreaking Priority Autocatch feature. If a previously unavailable domain matching your brand becomes available, our proprietary technology allocates it to your account before it can be caught by other drop catching services or savvy squatters.



DOMAIN ASSURANCE

Automatic Domain Assurance is your domain management safety net. It automatically secures any domain within your portfolio that matches your brand, safeguarding you from the risk of missed renewals or deletions. Your brand's digital assets stay protected, effortlessly.



DOMAIN UNBLOCKING

GlobalBlock gives you ultimate control of your domain portfolio. Found a use for a blocked domain? With Domain Unblock, easily activate or retire domains as needed, without complicated buy-backs or disputes.

Four Innovative Ways to Use GlobalBlock

A key benefit of a blocking service like GlobalBlock is the ability to remove numerous branded domains from market availability, helping to protect against third-party registrations.

However, additional GlobalBlock features are designed to improve or streamline the domain management process, saving time and resources and offering a solution to some of the most common challenges.



1. Delete Domains with Confidence

Defensive domain registrations have been a core strategy for online brand protection for years. It stands to reason – register branded domains so they can't be claimed by a third party who wants to imitate a brand or hold it for ransom OR hold domains won through a dispute process to help prevent repeated abuse.

The issue becomes that every domain a brand holds defensively must be managed, renewed and paid for each year, adding cost, risk and complexity to the portfolio.

However, in most cases brands would hold these names indefinitely as the dangers of releasing them back onto the market are often too high to accept.

GlobalBlock's Priority AutoCatch feature is designed to acquire deleted or expiring domains matching the brand before they're purged and placed back on the market, providing all GlobalBlock customers with the ability to delete and secure unwanted domains.



2. Manage Excessive Domain Transfer Demands

For decades, domain squatters have recognized the inherent value in a brand's name and used this to capitalize on domain names as a commodity.

Some bad actors register domains that use a brand's name or trademarks and then seek substantial payments for their transfer. This can then lead businesses to pursue lengthy and expensive legal action to retrieve the domains.

GlobalBlock's Priority AutoCatch service provides brand owners with additional options when facing domain acquisition requests. Brands may choose to:

- Wait for policy violations that could support dispute resolution proceedings, or
- Monitor for domain expiration, at which point Priority AutoCatch is designed to capture the name and add it to the customer's existing GlobalBlock service under standard service terms.

This unique service offers value to brand owners seeking to manage domain recovery costs and streamline their response strategies.



3. Register Domains When They're Needed (and Block the Rest)

A lot of defensive domain registrations are based on a 'just in case' mentality; claiming domains that might be of use or might pose a threat to a brand in the future.

Even with clear plans in place, it can still mean holding on to domains for years until a brand is ready to use them. Not surprisingly, this creates the issues of ongoing renewal fees and maintenance/monitoring, whilst creating a very challenging business case for measuring Return on Investment (ROI).

At the same time, taking a risk and leaving a domain on the market until it's needed can be just as costly, especially if someone else claims it first and demands a high price to purchase it back.

GlobalBlock helps address these challenges by offering enhanced flexibility for brand owners.

From a protection standpoint, when a GlobalBlock order is placed, available domains matching the brand are instantly blocked and removed from the market so no one else can register them. They can stay this way indefinitely, providing reassurance that they won't be misused.

When a brand identifies a use for one of its blocked domain, **Domain Unblock** provides a streamlined process to request the release of a domain for registration. After paying any applicable registration fees through a Registrar of choice, the brand can then use the domain and manage it as it would any others in its portfolio.



4. Manage Human Error Risks

Considering the number of terms brands want to protect and the hundreds of domain extensions available, it's easy to see how portfolios can quickly grow to thousands of individual domains.

What's more, each domain has its own registration fee, renewal schedule, terms and conditions to keep across. With all this complexity to manage, the risk of human error also grows.

Even the most detail-oriented people make mistakes at times. When it comes to domain name management, there are many ways things can go wrong:

- Missing a renewal date and losing a domain
- Failing to update payment methods and defaulting on a payment
- Incorrectly deleting domains that should remain registered
- Domain management provider making an error
- Making typos or spelling mistakes so the wrong domains are registered
- Causing delays so domain squatters to beat brands to the punch
- Poor record keeping resulting in a lack of knowledge about how domains are managed
- Staff departures or changes leading to a loss of experience or knowledge
- Malicious or retaliatory actions by an individual staff member

One tactic used by brands to mitigate these risks is to partner with corporate domain service providers who manage the process - but the costs remain of individually holding thousands of domains and engaging an additional service to manage them.

GlobalBlock's **Automatic Domain Assurance** feature is designed to help address potential oversights in complex domain portfolio management by seizing qualifying brand-match domains when they become available, including through accidental deletion or expiry.* After paying any applicable registration fees through a Registrar of choice, the brand can then use the domain and manage it as it would any others in its portfolio.

*Subject to technical limitations, timing, and service terms. Not all domains may be eligible for recovery.



Preliminary Report for globalblock

 GLOBALBLOCK

GlobalBlock Standard can block

608 Domains

using **one** of the main labels below. You can choose to block all of the main labels using GlobalBlock+.

 GLOBALBLOCK+

GlobalBlock+ can block up to

115,418 Domains

using **all** the main labels below and the variations of your brand we automatically generate for further protection*.

* A sample of variants labels is provided at the end of this report and in the accompanying data file.

Main Labels

globalblock

global-block

**600+ TLDs.
One solution.**

 GLOBALBLOCK

Want an inside peek to see how GlobalBlock can help your business?

Request your custom Domain Vulnerability Report at

www.globalblock.co





For more information, contact
a Brand Safety Alliance
representative at
hello@brandsafetyalliance.co

 **GLOBALBLOCK**

© 2025 Brand Safety Alliance LLC.