

A case study from InterNetX

Mitigating risks for brands with smart domain management tactics and tools

Contents

- 03** Introduction
 - 04** Identifying the risks for your brand and defining clear tasks
 - 08** Building a clear and tactical domain strategy
 - 09** Carry out growth hacking and branding with TLDs
 - 11** Register defensive domains
 - 13** Implement domain and DNS security
 - 17** Monitor your brand and domains
 - 19** When complexity increases, suitable solutions and tools are required
 - 22** Authors
- 

Introduction

InterNetX outlines how a professional approach to domain management is part of how brands manage their online reputation today.

Today we all know that managing reputation online is a complex undertaking for any brand. Not regarding industry-specific challenges, it is crucial to establish and grow brands in the online world, a task that is always associated with additional resources. There are dozens of variables that determine what the best approach for brand building and protection is. Whatever path you take, one element should definitely be included in your specific setup, namely domain names.

Why users rely on domain names on the Internet to find brands, services, professionals and personal websites? Online success starts with and is based on the right portfolio of domain names. Domains are not only the head of a complex technical infrastructure, they are also the banners for effective branding and marketing systems. That makes these brand flagships prone to abuse. There are so many issues and tasks bundled in a domain name that the domain industry is increasingly placing emphasis on the importance of domain management. For many people, a domain name may at first appear to be a rather simple and mundane part of the Internet, but behind each and every domain name, lies a vast and individual world of its own, made up of immaterial and monetary values.

So out of the initial and simple question "Why?", ever more pressing questions arise: What do you have to do to establish your brand domains and keep them running safely? How can you master the task of protecting users and customers through continuous monitoring and analysis of your domains? What do you need to accomplish modern and professional management of your domain portfolio? These are key questions that require close attention in order to lay the foundation for success and to establish a strong and secure online identity. Domains must not only be chosen carefully, they require clever and constant administration to prevent them from becoming doorways for abuse and fraud. For this reason, founders and corporations from all sectors are well-advised to lay out an intelligent domain

strategy. This should include identifying the specific domain brand risks, setting out a clear roadmap for brand growth hacking using appropriate TLDs, defensive domain registration, brand security as well as brand and domain monitoring and protection.

But, let us first take a step back and take a closer look at the challenges modern domain management faces and identify some of the risks that brands are exposed to in the domain name system (DNS).

Identifying the risks for your brand and defining clear tasks

Corporates, brands and domain managers should always keep the following in mind: domains and the DNS can be vulnerable to fraud. From the very first step, there are various types of brand misuse on the web and a great deal of them are associated with domains.

While domain grabbers often target unprotected general terms, cyber or domain squatters target proper names, brands and trademarks to resell domains to the actual rightful holders for exorbitant fees, depending on the type of trademark protection for the occupied terms. Domain squat-

ters prefer profitable targets, such as mainstream search engines and social media, financial, shopping and banking websites. When visiting these sites, users are often prepared to disclose sensitive information. Squatting domains that mimic well-known websites benefit from their credibility in order to attract more users that can be scammed. If website users can be deceived into visiting a squatting domain instead, this willingness and trust exposes them to phishing attempts and scams that aim to either steal valuable user data or money. Or both.

Squatting domains are often used for attacks. The objective of domain squatting is to confuse users, to deceive them into believing that the targeted brands own these misleading domain names. These risks can be mitigated by implementing a defensive domain registration strategy – more on this later.

There are a number of different squatting techniques every domain and brand protection manager should be familiar with:

Typosquatting

Typosquatting is one of the most common types of domain registration abuse. The most frequent typosquatting techniques include registering names just one edit distance away from the original domain, e.g. wikipedda.org or example.com. Also different TLDs are used for typosquatting, e.g. amazon.co or amazon.cm. Typosquatters intentionally register misspelled variants of domains to profit from typing mistakes or to deceive users into believing that they are visiting the correct target.

Combosquatting

Combosquatting is another form of widespread registration abuse that combines popular trademarks with words such as "contact," "payment" or "help", e.g. [contact\[familiar-bank-name\].com](http://contact[familiar-bank-name].com). Combosquatting domains are often used in phishing emails or in the context of social engineering attacks.

Soundsquatting

Soundsquatting domains take advantage of homophones, i.e. words that sound alike. For example: youtube > yewtube.com. Attackers can register homophone variants of popular domains. As text-to-speech software becomes more and more popular, many users are becoming vulnerable to that special form of domain abuse.

Homographsquatting

Homographsquatting domains take advantage of internationalized domain names (IDNs), in which Unicode characters are allowed, e.g. netflix.com (instead of netflix.com). Attackers usually replace one or more characters in the target domain with visually similar characters from another language.

Bitsquatting

Bitsquatting is only viable against very common and popular domains. These domains are almost exclusively owned by big brands and entities with significant resources. Bitsquatting domains have a character that differs in one bit from the same character as the legitimate domain, e.g. micrusoft.com and rely on bit-flip errors that take place in the DNS process.

The more established and successful your brand becomes, the more likely it is to become a target for cyber criminals. They can also become the targets of more complex attacks. Two examples of costly cyber attacks are DNS hijacking and distributed denial-of-service attacks (DDoS).

DNS Hijacking

With DNS hijacking, name resolution (resolving the domain to the correct IP address and therefore correct website/resource) is performed via a name server that is controlled by Internet criminals. Domain Name Server (DNS) hijacking, also named DNS redirection, is a type of DNS attack in which DNS queries are incorrectly resolved in order to unexpectedly redirect users to malicious sites. To perform the attack, perpetrators either install malware on user computers, take over routers, or intercept or hack DNS communication. The communication with the server is a vulnerable part of the DNS, because the exchange of request and answer is often undertaken without encryption and is based on trust in the system. These circumstances give attackers several means of intercepting requests and redirecting users. The hijacking of a domain name's DNS records is one of the worst attacks an organization can suffer, because they lose control over their domain and users are redirected to unwanted websites, where the system they are using can be infected with malicious software.

DDoS

DDoS involves a network being flooded with a deluge of requests from multiple sources so that it becomes overloaded and can no longer process legitimate requests, ultimately resulting in the network and web servers no longer being available.

It goes without saying that if companies fail to protect themselves against these threats, it could lead to disruptions that are critical and damaging to the business. Once again, companies need to consider both the monetary and image value of their online brand and weigh up the damage that could be caused by disruptions compared to the resources and investment needed for additional protection.

A clear domain strategy and management, which take these risks into account, is certainly the right first step and can lead the way to good solutions. Security at the technical level to prevent or mitigate such attacks and threats is a central requirement and its importance on a strategic level should never be underestimated. Nevertheless, a comprehensive domain strategy that works at an international level requires not only technical security, but also other tactical approaches to secure brands at a broader level.

Building a clear and tactical domain strategy

Issues like domain strategy, geographical and socio-political considerations, SEO optimization, traffic boosting and domain value are all tied up in the decision-making process when it comes to domain registration. And if they are not, they should be! Particularly if you are a corporate entity with trademarks and brand names to protect, a clearly-defined domain strategy and efficient domain management are pivotal to successful online branding and positioning.

Brand trustworthiness should be at the forefront of any business strategy and a solid cybersecurity policy helps to achieve this. After more than two decades in the domain business, InterNetX, as a domain registrar and service provider, always advises customers to spread their professional brand and domain protection measures over a number of different supporting pillars, namely:

01

Carry out growth hacking and branding with TLDs

02

Use defensive domain registrations

03

Implement domain and DNS security

04

Monitor domains and brands

Other important determinants for a fully-functioning domain strategy are time, tactics, resources and the use of the right tools. It should be the goal of all companies to operate domain protection and management as effectively as possible, depending on their specific conditions and requirements. In the worst cases, faulty or insufficient domain management can result in potentially disastrous image and

financial damage. Fast-growing businesses should secure the most relevant domain names early on in the process of building the brand. In many cases, companies just do not know which ones to buy. Sometimes, it is a simple matter of companies not thinking about domain registration until after the brand or company name has been chosen. More often than not, it is a question of information and market oversight and not knowing which domain

extensions are available and which may be relevant or useful to the business down the line. These uncertainties keep companies from registering the right domains. No matter the reason, the longer you wait to purchase the name you want or require, the more difficult and expensive it will typically become as time passes. Let us examine the benefits of a multi-tracked domain strategy for your business.

01

Carry out growth hacking and branding with TLDs

One of the first steps for startups, brands, corporates or new marketing campaigns is securing the appropriate domain under the preferred domain extension, technically called top-level domain (TLD). Anyone who has started the process of registering a domain name before knows that this is where the headache often starts. The days of simply choosing the domain name of choice under one of the legacy TLDs (.com, .net or .org) are long gone – in total there are 172.2M registered domains (as of June 30, 2020). Not only are the best domains already taken but there are also a multitude of ccTLDs and new gTLDs that could potentially provide better solutions or play an important supportive role.

The legacy TLDs .com, .org and .net remain the clear frontrunners worldwide, but even if you can find a

good, solid domain name under one or all of these, it may not be quite enough to get the most out of your brand. Research shows that Internet users in many regions and countries often demonstrate a strong preference for websites that use the relevant country-code ccTLD, like .de for Germany, .cn for China or .eu for the European Union. The same applies to geoTLDs, like .berlin, .tokyo or .nyc. This preference is often based on emotion and psychology, e.g. the expectation of language use and an instinctive trust in a local presence and support or affiliation to regional lifestyle or trends. In addition to covering relevant geographical and localized market areas, there may be specific new gTLDs which tie in appropriately with the relevant sector and improve visibility, like .app, .auto, .blackfriday or .rent.

Registering your domain names under TLDs like .shop, .blog, .news or .download can add agility to your communication and marketing channels. Other TLDs tie in with positive associations or reach specific target or regional groups due to their meaning. A good example of this is the TLD .xin (which means trust) that has become very popular in China. On the other hand, it could be useful to secure certain domains in order to avoid negative ratings, for example under .sucks. A number of high-profile companies, e.g. Apple, have registered their trademarks under .sucks in order to avoid being torpedoed by irate customers and are instead using it as a channel to get valuable feedback from consumers.

Registering typo-domains (related variations of commonly misspelled words) as well as any relevant internationalized domain names (domains consisting of alphabet characters used within specific regions or languages) may be a clever round-off to your domain portfolio. These can be set up with a redirect to the appropriate website.

Therefore, if you intend to create online branding for your company, trademark, products or campaigns, it is essential to undertake research in the domain market to make sure that it offers enough scope for your preferred choice of domain. Depending on where you do business and which markets and target groups you intend to reach, it is essential to carefully consider which domain extensions to register and implement. Alternatively, if you are not in a position to figure out exactly which domain registrations make sense for your business, it may pay off to work with a domain expert who has a good overview of the various possibilities and benefits of the TLDs and their respective target groups and markets. And it is certainly worth shopping around for a domain registrar that offers all the TLDs you need, domain support and a good domain management system.

02

Register defensive domains

Domain names can be valuable assets and companies should aim to build a broad portfolio through proactive domain registration that firmly establishes the brand in the world of TLDs. And that also provides protection against misuse by others. With cybersquatters scooping up names related to brands, many companies engage in what's known as defensive domain name registration.

Something that often gets brands into hot water is the "first-come, first-served" principle that has become standard in domain registration. Companies are not automatically entitled to register their trademarks. Apart from the Sunrise Phase, in which companies are given the opportunity to secure domain registrations for their trademarks during the launch

of a new TLD, it usually simply boils down to a matter of being quicker than anyone else.

A clever domain strategy includes dealing with questions about which domains are registered under which endings and what these domains are used for in detail. Large corporations may have huge portfolios of defensive registrations that incorporate IDNs and common misspellings of their company name, the names of products and abbreviations as well as the most relevant keyword combinations. Given the recent trend of countries relaxing regulations on their domain name extensions, these defensive registrations may actually include countries where the company does not even have a business presence.

On the flipside of this, companies should carefully weigh up the cost of maintaining these domains with the traffic volume they generate and the potential damage that could be incurred if they were to be registered by third parties. Registration and renewal fees of TLDs all differ and some go hand in hand with substantial financial investments.

A registered domain is an asset, and like many other assets, it can gain value over time. The longer a domain is kept (and used), the more valuable it becomes and the more likely it is to be acquired and subsequently misused if the company drops it or misses renewal. How far-reaching would the image and financial damage to your business be if a specific domain name was registered and implemented abusively under a specific TLD? Compare that to the cost of purchasing and maintaining that domain and you will start to gain an understanding of exactly which defensive domain registrations make sense.

Most domains that do not resolve were registered defensively or acquired on domain marketplaces — without much thought given to where the domains should actually point. And going back to point traffic to relevant content after a domain has been acquired can be a daunting task — especially for domain professionals who only spend part of their time managing domain name portfolios. Depending on the volume of traffic the domain is expected to generate, it might be worth the investment of time and effort to set up redirects toward the main brand content. In this way, companies are not only protecting their brand, but also controlling and maximizing the flow of traffic towards their main websites.

A tip: your defensively registered TLDs should also be redirected to live content or redirected back to the main site. This means that the traffic going to these TLDs is not wasted, while visiting traffic can lead to increased website conversion rates.

03

Implement domain and DNS security

Domain management also means dealing with technical protection mechanisms and domain security mechanisms that work on different levels. Some of them are bound to the respective TLD, others can be selected and controlled by the user. As a consequence, it is not only the chosen TLD that is decisive with regard to the possibilities for protection, but also the registrar with its security service offerings. The registrar used to obtain domains is therefore another influencing factor that is often overlooked, but may be critical in providing you with effective and solid tools to improve domain security. There are several points that should always be considered

when managing larger domain portfolios, particularly if you must meet high trademark protection requirements. But exactly how can companies implement effective preventive measures? What offers and services does the market provide for this? Fortunately, there are a number of protective services that are generally available when registering domain names or can be offered by your service provider.

Here some are suggestions for domain-side protection options:

Multi Factor Authentication

Multi factor authentication: With multiple security layers and individual blocking procedures using PIN/mTAN, domains are securely stored in a virtual safe. InterNetX has developed a solution called DomainSafe, which protects domains from unauthorized access.

Whois Protection / Domain Privacy

Whois protection / domain privacy: The Whois allows you to view the data of domain owners. To avoid this visibility, domain owners can use Whois privacy functions to prevent their data from being viewed by third parties. Domain privacy services are often offered by a number of domain name registrars. Users like brands can buy a privacy service for chosen domains and providers replace the user's information in the Whois with the information of a forwarding service. The Whois contains data on the individual domain owners. Although the introduction of the DSGVO means that no personal data may be publicly accessible within the EU, the regulation does not apply beyond the borders of Europe.

SSL/TLS Certificates

SSL/TLS certificates: SSL and TLS encryption have become standard online. Over 90 percent of websites have implemented SSL/TLS certificates and they are an essential part of brand creation, not only to protect sensitive information, but also to build customer and user trust in the brand and its services. Depending on your business and specific online requirements, there are a number of different encryption technologies and security levels available. For high-value brands or domains implementing the transfer of payments or sensitive user information, investing in an extended validation certificate is highly recommended.

Professional domain management also includes the server-side protection of domains: the DNS configuration of domains is stored on DNS servers (also known as name servers). This configuration is used to connect your domain to the server(s) hosting websites or email addresses. And there are also different protection methods for this. Basic server-side security measures include:

DNSSEC

To protect data integrity, use Domain Name System Security Extensions that digitally sign DNS data so that name servers can ensure their integrity when responding to queries. This security standard is an asymmetric encryption method that uses a key pair consisting of a public key and a private key. Registrants should always check whether individual TLDs support DNSSEC in advance. Nevertheless, it is highly advisable to implement it in order to secure a good level of protection

Anycast

With Anycast, a group of computers is assigned a common address. The special feature of this type of addressing is that access is always routed via the computer that is closest to the requestor. InterNetX uses the Anycast service NodeSecure, whose name servers are distributed worldwide and thus ensures the highest availability and shortest access times.

DDoS Protection

To avoid business-critical failures, you should minimize the risk of attacks with DDoS Mitigation Services. Especially important with regard to domains: DNS name server protection against DNS flood and other DDoS techniques aimed at crashing or disrupting DNS name servers. Hereby the primary server is hidden and the resolver is protected with a secondary DNS to reduce the possibility of domains going offline due to DDoS attacks. This allows protection of both hidden servers and domain names served by a fast anycast DNS. This service is also available for Cloud Servers or individual solutions at InterNetX.

There are also a number of additional options that are useful for extra protection:

Registry Lock

A registry lock provides increased protection for domains and can be used to make domains even more secure. It reduces the risk of domains being inadvertently changed, deleted or transferred. With a registry lock, registrants can benefit from the highest level of security for the most valuable and visible domains. However, these services are not offered by all registries.

Registrar Lock

The registrar lock also protects your domains from unintentional changes, but as opposed to the registry lock, a domain protected by the registrar lock can still be transferred. This service is not offered by all registrars.

For the administration of domains, using software is indispensable and with a constantly growing portfolio, there should ideally also be possibilities for the administration of user accounts. In the context of professional domain management, domain security at the software level could include:

Access Control Management

Not every user requires full access to all applications in your domain management system. Using access control (ACL) management, user rights can be assigned separately and limited to individually defined users in your company, depending on the required scope of the tasks they carry out.

Two-Factor Authentication / IP Restriction Users

Logging on to the domain management software should be using at least two-factor authentication to ensure multiple protection. The software you are using should offer IP restriction features to avoid unwanted logins. Both features ensure that only pros who know what they are doing are taking care of the company's domain assets.

There is no 100 % failsafe protection. In order to make your domains and online appearance as safe as possible, you should always take advantage of the entire security process of a proven provider that you can rely on to avoid losing control.

04

Monitor your brand and domains

A trademark and domain name are not identical. Although most domain registries offer so-called Sunrise Phases during TLD launch phases, in which companies can secure their registered trademarks, simply owning a trademark does not immediately entitle you to the allocation of the corresponding domain name. Over and above this, new TLD launches are not always marketed globally and relevant information about introductions and registration requirements is not always immediately available or visible to those not actively involved in the domain market. However, there are a number of processes and tools available to help trademark owners to protect their brands.

Firstly, many domain management platforms offer domain monitoring or trademark scan tools which allow trademark owners to keep an eye on potentially abusive registrations by other parties and check whether their trademark has been registered under other TLDs. Some tools also send proactive notifications if a new domain is registered using trademarks or related terms. A number of registries also provide the option to enable domain blocking, which prevents certain trademark domains from being registered.

Secondly, ICANN has implemented the Trademark Clearinghouse (TMCH) as a central mechanism towards protecting rights in its new gTLD program, recently also for gTLDs like com, .net, .cat, .coop, .jobs, .mobi, .museum, .pro, .tel, .travel, .xxx. TMCH provides a number of important functions for trademark holders. It allows registered trademarks to be submitted to a central database which is tied into all launches of new gTLDs. Trademark holders can then participate in the Sunrise Phase of all subsequent new gTLD launches and therefore have the first option to register their trade names under these TLDs if they wish to do so. If a domain name matching a trademark in the TMCH is registered by a third party, the registrant automatically receives a notification that such registration could potentially pose a trademark infringement. If the registration is nevertheless carried out, the trademark owner receives a notification of the registration and can, if necessary, initiate legal action.

And last, but certainly no less important, the importance of using an efficient domain monitoring and management tool again comes to light with the seemingly simple question of domain renewal. While many registrars offer long validity periods or auto-renewal options, which require domain owners to actively delete domains they no longer want, a number of registrar systems work on an auto-delete basis, which means that domain owners have to actively renew the domains they want to keep when they reach expiration. If this does not sound like a big deal, try keeping tabs on all the renewal dates of domain portfolios with hundreds or even thousands of registrations, including domains that are worth stately amounts. Some famous examples of unintended domain expirations include high-profile companies like Microsoft, Google and Foursquare. Even if a missed domain renewal does not always result in permanent loss of the domain, it can result in an embarrassing and painful loss of reputation and earnings and, in the worst case, lead to high recovery costs for acquiring the domain again if it is grabbed by another registrant.

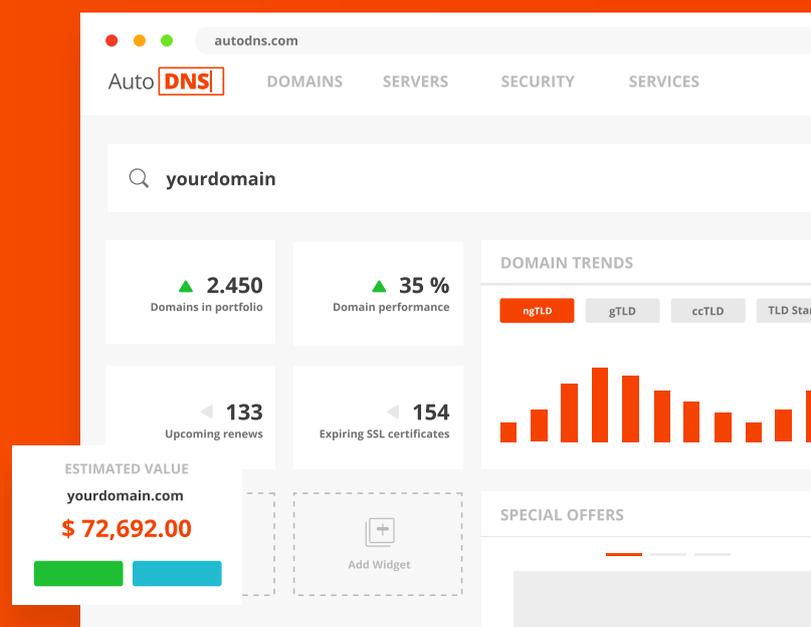
When complexity increases, suitable solutions and tools are required

Domains have become essential cornerstones to the online world and require adequate protection and professional management. They are no longer simply part of the company contact data, directing potential customers to the relevant website, but have become marketing tools in their own right, capable of conveying powerful messages, transporting emotion and attitude and creating confidence amongst target groups.

All said and done, it is well worth the time and resources needed to set out a solid domain roadmap. Corporates and brands need a clear strategy, protection and tools to establish and protect their brands and deal with ever-changing tasks and threats – the job is far from done with simple domain registration and renewal. Not only companies that manage large domain portfolios or high-value brands need strong tools and partners they can rely on. Prosumers (individuals or companies that are consumers as well as providers of a specific product or service) also need to be able to rely on systems from their providers.

With corporations often requiring a multitude of domain names for their trademarks, brands and campaigns, actually finding a provider that is accredited by all the relevant registries and can supply the desired and specific range of different TLDs for growth branding and hacking is no easy task.

As one of the leading domain registrars in B2B on the European market, InterNetX have been developing custom-fit solutions in the domain business for over 20 years to meet all these market requirements. And this is no small challenge. Building on two decades of experience, we have developed a domain platform that meets all requirements and bundles everything you need into one solution: AutoDNS – the domain platform.



Screen: AutoDNS the domain platform Dashboard

Our incentive is to offer our customers the necessary tools and resources to manage and protect their domains. Using applications and software as well as domain services is all but mandatory and certainly market relevant for professional domain management.

A good domain management platform will include extended functions in domain searches that facilitate defensive domain registration. Apart from listing all available TLDs, they also generate automatic suggestions of other related domains, including alternative and popular keyword combinations, the most common misspellings and relevant IDNs, allowing registrants to simply select the combinations they want and carry out a bulk registration with just a few clicks.

Tools like our Domain Studio allow businesses to search for domains under more than 1,000 TLDs and list these according to relevance and availability. Available domains can be registered immediately in bulk, while others that are up for sale can be acquired over the tied-in domain aftermarket. Whois services allow companies to view information about domain owners and make offers or submit requests for domain transfers if the relevant domain names are already taken.

The screenshot displays a search interface for 'yourdomain'. At the top, a search bar contains the text 'yourdomain' with a magnifying glass icon on the left and a close 'X' icon on the right. Below the search bar, the results are organized into four main sections: 'LOCATION BASED', 'MARKETPLACE', 'SUGGESTIONS', and 'SIMILAR'. Each section lists domain names with associated actions and prices. A 'FILTERS' panel is also visible on the right side of the results area.

LOCATION BASED	MARKETPLACE
yourdomain.nyc ADD TO CART \$ 13.40	domain.com BUY \$ 23,490.00
yourdomain.us TRANSFER	domain.de
yourdomain.miami	domain.net
yourdomain.vegas	domain.jobs

SUGGESTIONS	SIMILAR
yurname.com ADD TO CART \$ 8.00	yourdoma.in TRANSFER
yoururl.today	mydoma.in
yoursmtp.net	
yername.com	

FILTERS

Number of results 60

- Similar domains
- Premium / Marketplace
- Location based matches
- Price estimation

Screen: Domain Studio

Businesses requiring extensive domain portfolios will find it invaluable to use a domain management platform provided by a registrar that offers the widest possible selection of global TLDs and also connects to domain portfolios that are held with other registrars, allowing external domains to be monitored and managed. An efficient overview of domain portfolios and central management – all in one place.

JSON, EPP and XML API solutions also allow external systems to be integrated seamlessly and white-label features make this kind of domain platform particularly attractive to domain resellers.

The domain portfolio overview in AutoDNS, for example, can be used to select defensive domain registrations and platform functions allow redirects to be set up for multiple domains in order to maximize the volume of traffic directed towards the main brand website.

And it offers the necessary domain security features to safeguard domains individually with multiple blocks using a PIN / mTAN procedure and protect them in a virtual vault against unintentional access. The Whois privacy feature allows the contact data of domain owners to be concealed from third parties. The domain monitoring feature in AutoDNS allows

domain owners to draw up a list of domains to be monitored and sends regular reports about their status and any critical developments.

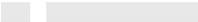
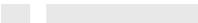
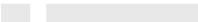
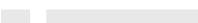
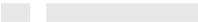
A news feed is also integrated so that domain managers can stay informed about current market developments, releases, changelogs and trends.

Detecting domain fraud requires a great deal of research and is cost-intensive. That's why the Trademark Research feature is definitely another unique selling point of AutoDNS. It is a powerful toolbox for anyone faced with the task of protecting brand names and brand keywords in the international domain universe. This intelligent tool collects data when searching for trademark infringements resulting from unauthorized third-party domain registrations in order to support trademark owners, trademark attorneys and brand managers in their everyday business of trademark protection. Using the Trademark Zone Scan, a search for any keyword or brand name can be undertaken in over 1,700 root zones. The scan is performed twice, just to be on the safe side. Thanks to the Trademark Research Services in AutoDNS, the domain platform, it is now possible to automatically detect potential infringements of trademark law involving domains and to take prompt legal action. It is an extremely practical tool for the active enforcement of brand protection in the DNS.

Keyword Monitoring

Trademark Zone Scan

KEYWORD SCAN

Search term	Scan Intervall	Result	Last scan
yourbrand	monthly	NO WARNINGS	
yourtrademark	daily	NO WARNINGS	
yourproduct	weekly	NO WARNINGS	
yourkeyword	weekly	NO WARNINGS	
yourbusiness	weekly	NO WARNINGS	

This is all rounded off by a range of domain and security measures that have already been mentioned, like DomainSafe, DNSSEC and NodeSecure, the Any-cast service for secure and fastest possible access times. InterNetX offers a free basic SSL certificate with each registered domain and has designed the SSL Certificate Wizard, a useful tool that helps users find the most suitable SSL solution for their project.

The platform interface can be adjusted individually, allowing news feeds about TLDs and the market trends to be displayed alongside information on the latest features, user domain statistics and most-used domain services.

Let us get back to the point: It is more essential than ever to build a suitable domain portfolio that strengthens the brand and grows its visibility on the net while mitigating the risks at the same time. There are several mechanisms and tools that can be used to protect domain brands, gain and improve customer confidence and trust and to minimize the risks of both image and financial damage. Domain and brand managers have to monitor several dimensions to weigh up the risks, security issues and potential gains involved. And they require appropriate instruments to do so. This is what professional domain management really needs.

Authors

Birgit Berger and Natalie Berisford of InterNetX outline how a professional approach to domain management is part of how brands manage their online reputation today.



Birgit Berger
Lead Performance Marketing
@ InterNetX



Natalie Berisford
Partner Communication Manager
@ InterNetX