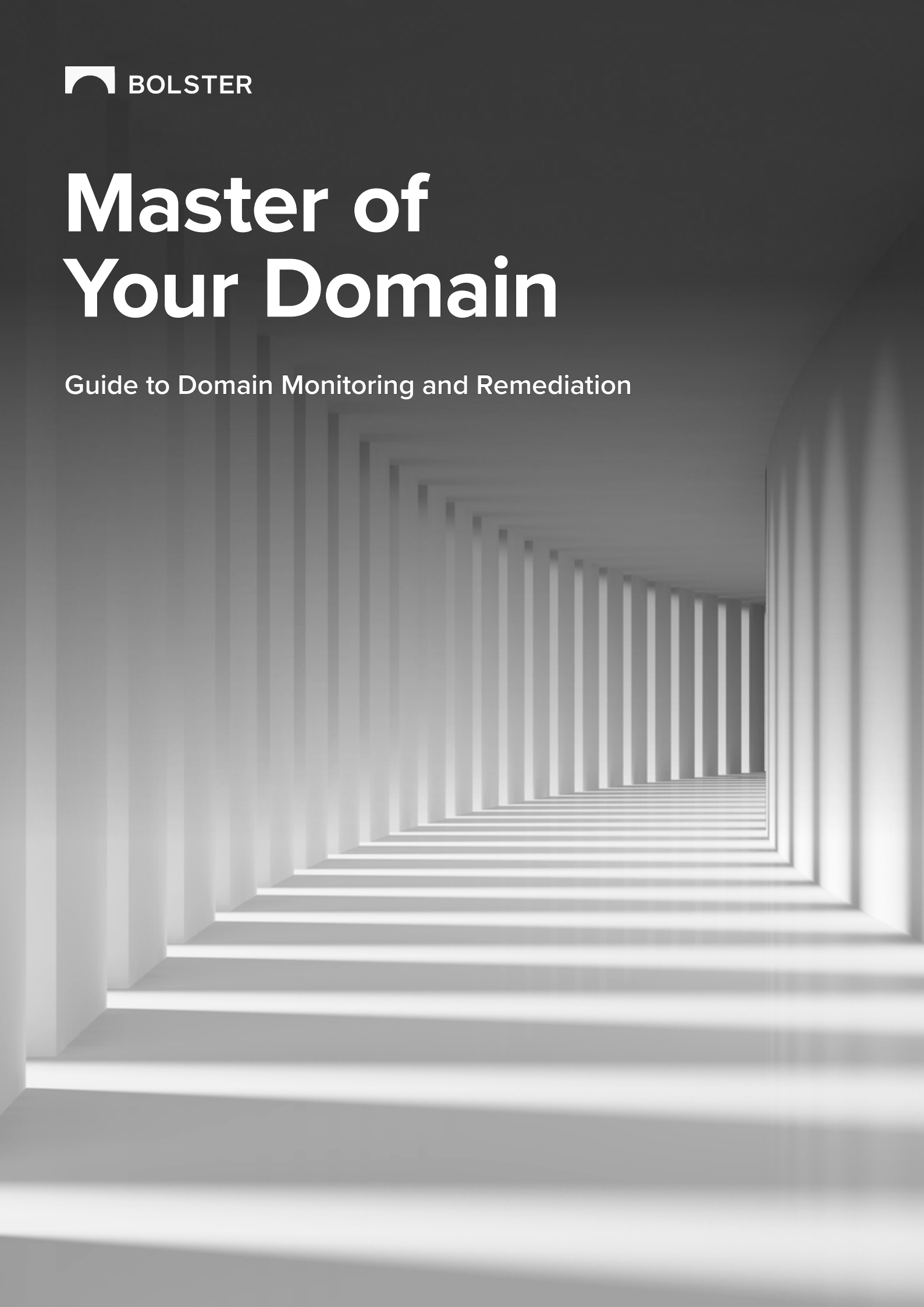
BOLSTER

Master of Your Domain

Guide to Domain Monitoring and Remediation



Contents

Introduction to Domain Variants and Threats

Whether big or small, the first step for any business having an online presence is to secure an Internet domain. This domain typically should match your company's name, brand, or sub-brand. Many organizations believe that creating a compelling internet presence only consists of setting up a website, standing up mail server capabilities, and then being able to conduct business online, however, it is not that simple.

Organizations find that creating an online business comes with complexities. Some common questions raised are:

- What are all the top-level domains (TLDs) besides .com?
- What about all the typosquat variants that fraudsters might stand up to impersonate your brand or an executive at your organization?
- How will you accurately find all the variants of your TLDs on the vast Internet and continuously monitor for new ones?

Take for example the mythical company 'mynewcoolcompany'. The company purchased and registered the mynewcoolcompany.com TLD for business, but there are over 3,000 more variants of 'mynewcoolcompany' top-level-domains (TLDs) between legacy TLDs, new TLDs, and country-specific TLDs.

Some examples of variants of 'mynewcoolcompany' could include:

- mynewcoolcompanys.com
- mynewcoolcompany.net
- mynewcoolcompany.fr
- mynewcoolcompany.info
- mynewcoolcompany.info.uk

What does this mean for organizations looking to conduct healthy and legitimate online business? Fraudsters can very easily and quickly go out and purchase any one of those unregistered domains that resemble your TLD and set up a fake site to start staging attacks against your customers, employees, contractors, and/or supply chain.

The risks don't just stop with securing the plethora of TLD variants. There's also the real and sizable threat of look-alike or typosquat domains. Look-alike and typosquat domains are domains that sneakily look like yours but aren't like for example: thenewcoolcompany.com, mynewcoo1company.com, mynewcoolcmpany.com. These are just a few examples of what could be full-blown fake sites, logos and all, designed with the intent to trick end-users, and all achieved through a malicious variant of the legitimate domain.

The problem of look-alike or typosquat domains can quickly become difficult to manage as it is a function of the number of characters in the domain name. As the number of characters increases, so too do the number of look-alike or typosquat combinations (see Figure 1 below). We can extrapolate that for our 16-character mynewcoolcompany example, the problem is difficult to resolve on your own and requires a significant amount of resources.

The internet is expanding at a rapid rate. New digital experiences are being created every day, whether it be a new social media platform or marketplace or something more revolutionary like the Metaverse. Humans just can't keep up with the scale at which the internet (and attack surface) is growing and fraudsters know this. This is where AI comes into play.

Domain Monitoring: Is it Enough?

In order to combat the threats to an organization's online presence, there are too many ways of defending against the fraudsters. Organizations can proactively purchase and register all the domain variations (TLD variants, look-alikes, typosquats, etc), but this is not the most ideal solution as it will often oustrip allotted security budgets.

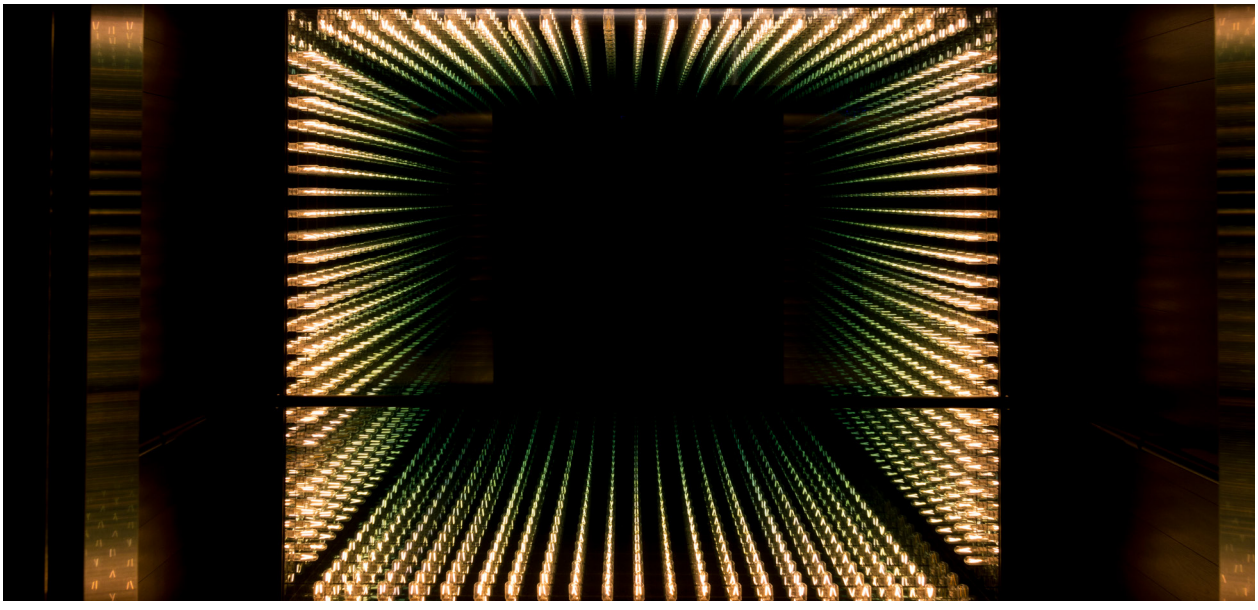
The only way for this kind of proactive purchase to be viable and economical is with the use of Artificial Intelligence (AI) to build purchasing priority-ranked recommendations with algorithms that factor in cost and relative risk. By doing so, organizations can optimize their spending on the most malicious sites first, then with any leftover budget be allocated to suspicious sites - essentially getting the maximum amount of risk reduction for the most optimal amount of spend.

Organizations can continually monitor the Internet for look-alike and typosquat domains with legacy domain monitoring tools that assess risk and remediate continuously. However, these legacy tools lack the intelligence to understand the context, landscape, and risks of the malicious or suspicious URLs.

Without AI to accurately detect all variants and typosquats and then prioritize which risks to mitigate based on severity, the process of domain monitoring will be a never-ending and overwhelming challenge. Many organizations simply cannot keep up with the massive volume of data resulting from the frequency at which changes occur at the domain registration level combined with an ever-changing threat landscape.

Organizations must leverage modern domain protection solutions that help them optimize costs and reduce risks in a way that is effective and secure. The best way for organizations to achieve this is with a strong AI engine that is able to accurately assess the online threat landscape, make recommendations, and then help automate the domain takedown process.

Without AI to accurately detect all variants and typosquats and then prioritize which risks to mitigate based on severity, the process of domain monitoring will be a never-ending and overwhelming challenge.



Simple Steps to Assessing Online Threats

Protecting your brand online shouldn't have to be an insurmountable process. Here are some steps to get started on your domain protection.

Step 1

Create a comprehensive catalog of domains owned and managed by your organization.

Step 2

Identify possible typosquatting variants of each domain that represent a risk to your organization. The domain variations that need to be considered extend beyond the simple character replacements. For example "app11e" is a variant using numerics instead of the text-based "apple." The variants also need to include word combinations such as "apple-support" or "applepasswrd" that may create confusion. A popular tool used by many teams for discovery is the open source project "dnstwist" (https://dnstwister.report/). To use this project, go to the URL and enter your domain names in the <name.TLD> format (example: notion.com).

Step 3

Repeat the same process for every other TLD that poses a potential threat. Some examples could include a sub-companies or brands, mergers and acquisitions, or an executive name.

Step 4

Repeat steps 1 through 3 usually need to be repeated daily. This is a critical step since phishing, fraud, or malicious sites can be set up at any time, by anyone. Continuous monitoring, though demanding, ensures rapid detection and remediation of online threats.

This process should be tracked in a simple, coherent way to ease ongoing management and enforcement.

Enforcement can create more risks as any online activity that you take (i.e. visiting a site) must be performed in a secure, safe manner to avoid a potential cybersecurity incident such as accidentally downloading drive-by malware.

The four steps described, while simple, are by no means easy. In real practice, monitoring and remediating online threats is tedious and time consuming.

For example, the domain 'notion.com' generates 217 variations for just the .com TLD. When you consider all of the nearly 3,000 TLDs that exist on the Internet, that number grows to 651,000 domain variations that need to be assessed and monitored continuously! Acquiring all of these domains is not a practical option as it would cost roughly $19.5 million per year, assuming an average cost of $30 per domain.

Ultimately, to effectively assess and remediate online threats, it comes down to adopting a scalable and cost-effective solution. While in theory domain monitoring seems simple, the challenge arises in prioritizing the most malicious of the e 651,000 domains on a daily basis to make sure that organizations are addressing real threats first. Many organizations have more than one domain and this example is only a small fraction of the headache that comes with domain monitoring and remediation.

Trusting the Experts for Domain Monitoring and Remediation

Monitoring and remediating online threats can quickly become a problem of seismic proportions. Large enterprises will struggle with the volume of TLDs they need to manage and the amount of threat actors targeting them. Smaller organizations will struggle with in-house resources they can dedicate to this growing problem. Whether large or small, companies that choose to address this problem solely in-house will run into a myriad of challenges. Even the takedown process requires niche legal expertise and established technology partnerships.

Simply put: trust experts to help with your domain protection strategy. Domain monitoring and remediation should be powered by an intelligent engine that can accurately scan the threat landscape for all online threats, assess the risk of the threat, and then give recommendations to how organizations of all sizes can mitigate risk. In addition, resource constraints and volume management can be alleviated with an easy-to-use automated solution that can scale to any size. In-house solutions to domain monitoring are more expensive and less accurate, exposing your organization to undue data breaches.

Try Bolster Domain Protection for Free

Start with a free, no obligation, Domain Acquisition Analysis from Bolster, the most advanced and automated domain protection solution on the market.

Bolster scans 3,000+ global top-level domains daily to determine typosquatting variants that are available for purchase and the associated costs to acquire them. Bolster helps organizations of all sizes adopt an acquisition strategy to reduce their overall online threat exposure. Bolster helps optimize security budgets by allowing organizations to instantly see all their purchasing options, ranking by overall risk level - across all top-level domains and all geo-locations.

For domains already registered by potential bad actors and for domains left unpurchased, Bolster can set up an online real-time monitoring dashboard with full visualization and remediation strategies. Bolster allows for organizations to easily identify active TLDs, look-alike and typosquat variants, prioritize them based on threat level, and monitor them for changes.

What's more, Bolster detects new registrations and monitors each for changes in risky activity over time. The Bolster platform provides an intelligent and automated way for organizations to get ahead of threats and take the best remediation before online attacks can occur.

Visit www.bolster.ai to start protecting your domains.

About BOLSTER

At Bolster, our mission is to make the internet safe for everyone. That's why we created the first and only fully automated platform purpose-built from the ground up to detect, monitor, and take down fraudsters on the Internet. We call it Automated Digital Risk Protection. Our comprehensive platform offers the most efficient protection across web, social media, app stores, and the dark web to combat fraudulent sites and content.

Contact us today:

4940 El Camino Real, Suite #200, Los Altos, CA, USA 94022
bolster.ai