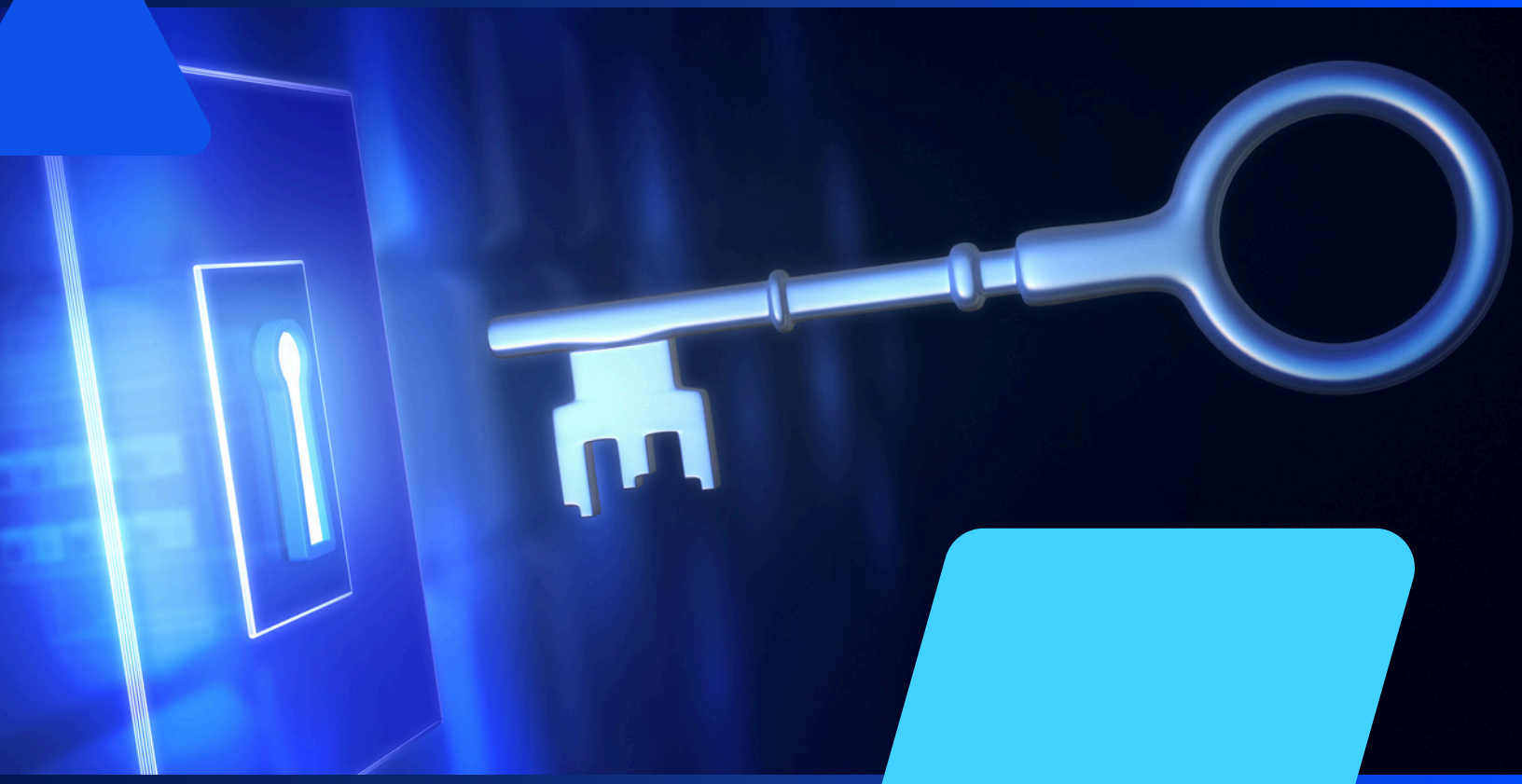
Registry Locking:

Overlooked, Underused, and Essential for Your Domain Safety



Markmonitor™

Meet the Author:
Bonnie Wittenburg, Head of Commercial Strategy

With nearly 30 years of industry experience, Bonnie has guided some of the world's largest brands in crafting solid domain name management strategies. She specializes in navigating the complexities found in international organizations, streamlining portfolios for cost savings, and simplifying processes.

Bonnie's expertise encompasses addressing the intricate needs of diverse, multi-stakeholder organizations by crafting bespoke strategies that balance protection with budgetary constraints. Markmonitor is privileged to have Bonnie as part of its leadership team as Head of Commercial Strategy.

The Overlooked Defense That Deserves Your Attention

I'm often asked about tips and insights that domain managers can use to strengthen the security posture of their portfolio. One recommendation is to look at **registry locking — it's an often underutilized and yet vitally important security measure for safeguarding a business's digital presence.**

With a registry lock, your registrar works directly with the registry to block unauthorized changes — such as nameserver updates, contact detail edits, or domain transfers — unless proper verification and approval are completed. This helps safeguard your mission-critical domains from mistakes, attacks, and unauthorized activity.

Registry locks are a powerful safeguard against domain hijacking, DNS manipulation, and unauthorized transfers. Yet surprisingly, adoption remains relatively low across many portfolios. In fact, less than half of the Top 500 brands have their crown jewel domains registry locked [1].

This caused me to do some digging to discover why, if registry locks are so

highly regarded as a solid protective mechanism, organizations don't consider them.

Here's what I found:

BARRIERS TO ADOPTION

Lack of Awareness
Many organizations simply don't realize how vulnerable their domains are or that registry locks even exist. They often assume that standard registrar locks or two-factor authentication are sufficient.

1. Brand Finance, Global 500 2024

The Overlooked Defense That Deserves Your Attention

Security and IT departments may focus on endpoint protection, firewalls, or cloud security, leaving domain security to fall through the cracks. It is often not part of standard security audits – unless there has already been an incident, a painful way of learning domain security should be prioritized.

Example – a careless employee falls for a phishing email thinking it is from their registrar. They log in, unknowingly giving away their credentials. The hacker now has access and can alter the domain settings, transfer it out, or even redirect traffic to a malicious site. A registry lock would have prevented these unauthorized changes at the registry level. Having a trusted registrar and a registry lock in place is a great way to prevent such disastrous outcomes.

No Industry Standardization

Not every TLD or registrar supports registry locks – or if they do, they may implement them differently. This inconsistency makes it hard to roll out a universal domain protection policy and highlights why a corporate domain registrar is a critical asset in understanding and implementing such protections where available.

Example – A .COM domain involves the registry (e.g. Verisign) in a blend of automated and manual processes, with multi-factor authentication for changes. The domain owner, its registrar and Verisign come together in a triple handshake to make the change. In the case of a .UK domain name, the registry (e.g. Nominet) uses a method called "Registry Lock Service." It's a more manual process than .COM, requiring secure passwords and manual verification for updates. A trusted corporate registrar like Markmonitor helps organizations understand these varied processes and provides guidance and assistance through implementation.

"...inconsistency makes it hard to roll out a universal domain protection policy and highlights why a corporate domain registrar is a critical asset."

The Overlooked Defense That Deserves Your Attention

Complexity and Inconvenience
Registry locks often require a somewhat manual process when changes need to be made to a particular domain. These processes typically involve the registrar and the registry – sometimes requiring phone calls, signed requests, or multi-party authorization.

That's great for security but frustrating for IT teams who need agility. For domains that require frequent updates (e.g. DNS changes or contact info), the added friction of unlocking and relocking can feel like a burden – especially if the domain isn't seen as mission-critical. However, the very fact that these locks require extra manpower and support to implement by your registrar and the registry is the reason they exist and are so effective.

Example - Remember our example of the careless employee who fell for a phishing email and inadvertently shared login credentials with a bad actor? The bad actor will not be able to make any changes to domains that have a registry lock in place. The checks and balances provided by the registry lock process thwarts the bad actor's attempts to take advantage of the phish.

The Overlooked Defense That Deserves Your Attention

Cost and Resource Constraints
Registry locks typically incur a charge, and smaller organizations may not have the budget built in. The added cost may feel unjustifiable – especially if leadership doesn't fully under the risks. But a single incident of downtime may cost the company much more in terms of lost revenue and serious brand damage. An ounce of prevention is worth a pound of cure!

Example - Believing it to be an unnecessary expense, a company does not purchase registry lock for a domain which is critical to its business. Then, disaster strikes – a domain hijack takes down their main site, crippling revenue and reputation. The savings vanish as the real cost of not having the lock in place unfolds.

STILL AN IMPORTANT OFTEN OVERLOOKED TOOL

Despite some hurdles, registry locks are essential for high-value domains—think banks, government portals, healthcare providers, or any brand whose domain is tied to trust and uptime. A single hijack

"A single incident of downtime may cost the company much more in terms of lost revenue and serious brand damage."

could lead to phishing, data breaches, or massive reputational damage.

The Trend Is Shifting
The good news? Adoption is growing, especially among enterprises and security-conscious brands. **As DNS hijacking and registrar-level attacks increase, so does awareness of this simple but effective tool; more organizations are recognizing that registry locks are not just a best practice—they're a necessity.**

If you're managing a domain portfolio, especially for a public-facing or high-risk brand, Markmonitor would be happy to help you explore how to implement registry locks effectively.

Markmonitor provides strategic domain management solutions that help protect the revenue and reputation of the world's leading brands.

Since 1999, Markmonitor has served the domain portfolio needs of businesses around the globe, including many of the most visited websites in the world. An ICANN accredited domain registrar since its establishment, Markmonitor leverages its extensive industry relationships, innovative technology, and broad expertise to manage and protect company domain portfolios, all with data-driven, white-glove consultation designed to maximize domain portfolio value.

Should you need any further information or assistance, please contact your Account Manager or email customer.service@markmonitor.com