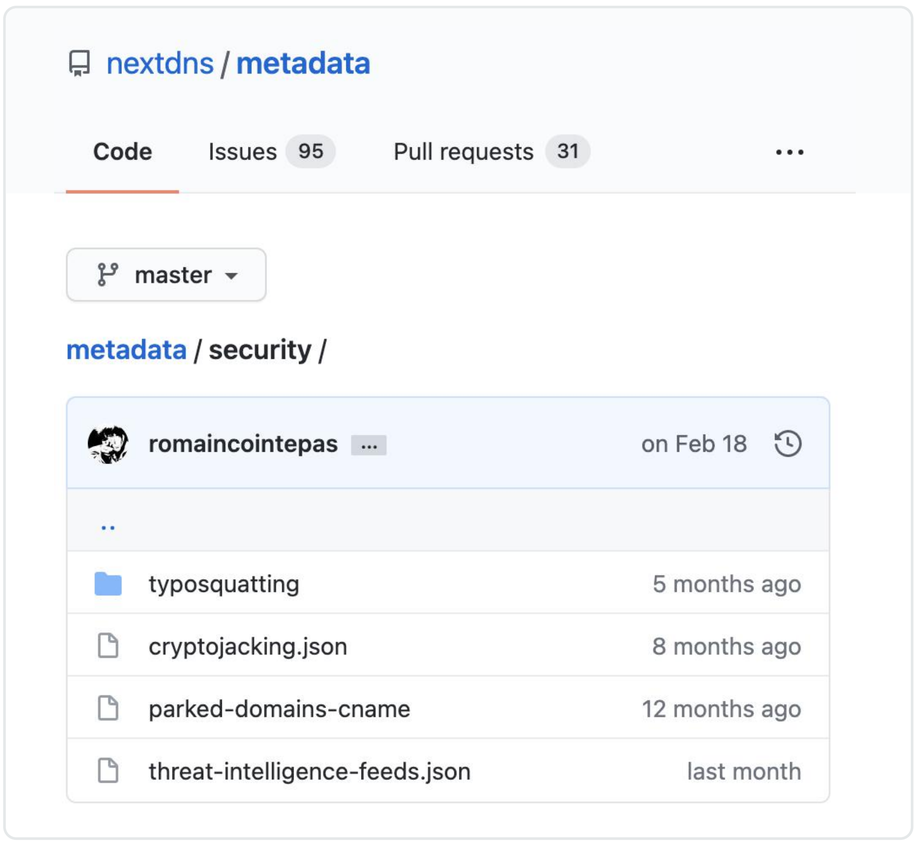
Content Filtering Compared: DNSFilter Vs. NextDNS

NextDNS and DNSFilter are both next-gen DNS security solutions. DNSFilter has spent nearly 6 years building a solution that is both easy to implement and a comprehensive threat protection tool. Still an early-stage startup, NextDNS has focused on usability over other features, while DNSFilter has a blended focus on both customer usability and bulletproof threat protection.

Higher quality security feeds

NextDNS' security options appear to be comprehensive at first glance, but a large portion of their lists (including ad blockers) are either publicly sourced or updated infrequently. Because NextDNS makes their lists public, we can see that a large portion of their security lists go several months without updating.



When you solely rely on public lists to source and block threat domains, there's a large margin of error. First, the people providing these lists might not be cybersecurity experts, thus their data could be inaccurate. But also, deceptive domains don't remain deceptive forever. When you go long periods without updating deceptive domain lists, you inevitably run into false positives—meaning trying to access a domain that is no longer deceptive will result in that domain being blocked.

At DNSFilter, we source both public and private feeds for all of our categories (including our advertising category), but we do not wholly ingest those feeds the way NextDNS appears to. We check these lists ourselves to look for false positives or miscategorized domains. If a list doesn't meet our standards, we don't ingest it. And sometimes we will only ingest a partial list of domains.

While NextDNS relies on these public feeds for their ad blocking capabilities, at DNSFilter we take the use of public feeds a step further. We employ one of the maintainers of those public feeds, giving us an internal expert on ads and trackers who is actively working on our ad block categories.

The value of AI

Another aspect of our threat categorization is our AI. In addition to ingesting some threat feeds, we actively scan (and re-scan) websites to determine if they are malicious. Our AI has over 20 threat indicators that it uses to determine if a site is harmful or benign—including logo-scanning technology to help determine if a page is legitimate or a scam.

This scanning enables us to add to our list of deceptive sites, meaning we're always adding to our list—often daily. We also re-scan previously deceptive sites to determine if they are no longer deceptive and can be removed from our threat categories.

NextDNS only relies on lists. Because of that, their lists need to be manually added to when new malicious domains are found. This inherently adds a delay between a domain being discovered and that domain getting added to NextDNS' service.

DNSFilter's AI discovers malicious domains up to 80 hours before traditional threat feeds, like the ones used by NextDNS. As hackers activate malicious domains in those first 80 hours, DNSFilter customers are protected while services like NextDNS are still allowing resolution of those deceptive domains.

Limited categories

Aside from their threat categories and ad tracking categories, NextDNS only provides 5 categories under the “Parental Control” section. These are:

- Porn
- Gambling
- Dating
- Piracy
- Social Networks

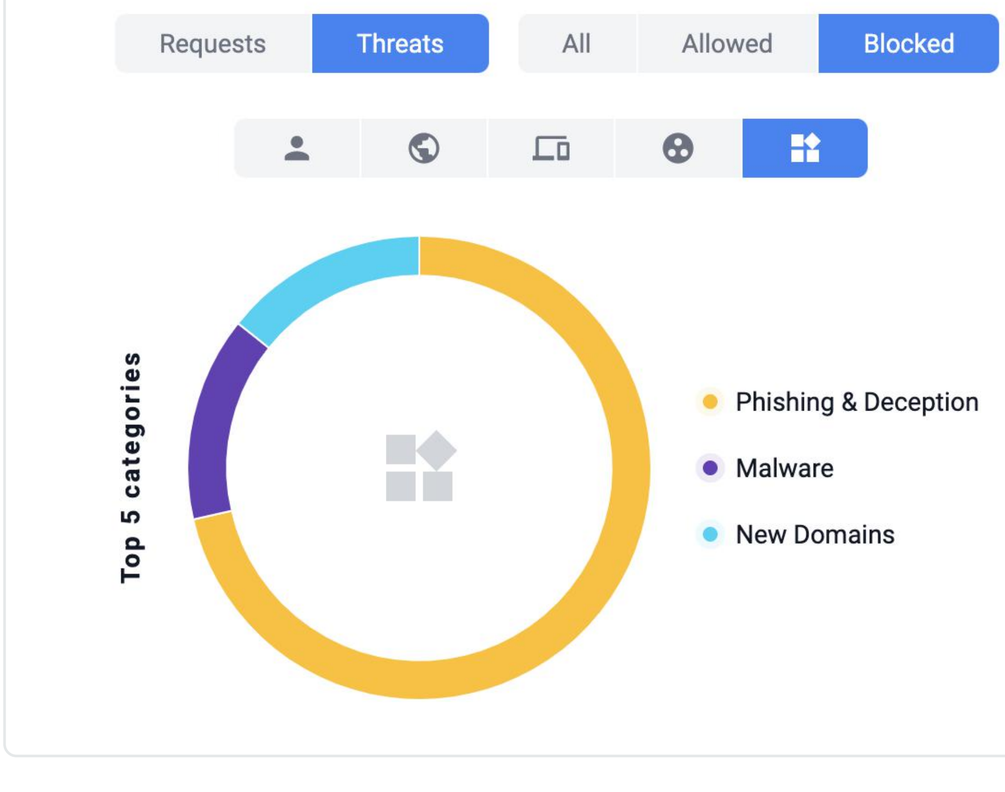
DNSFilter gives users more flexibility with **36 categories**, **7 threat categories**, and multiple **SafeSearch** options. This not only means you have more granular control over what you can allow users access to, but it impacts your reporting.

More comprehensive reporting

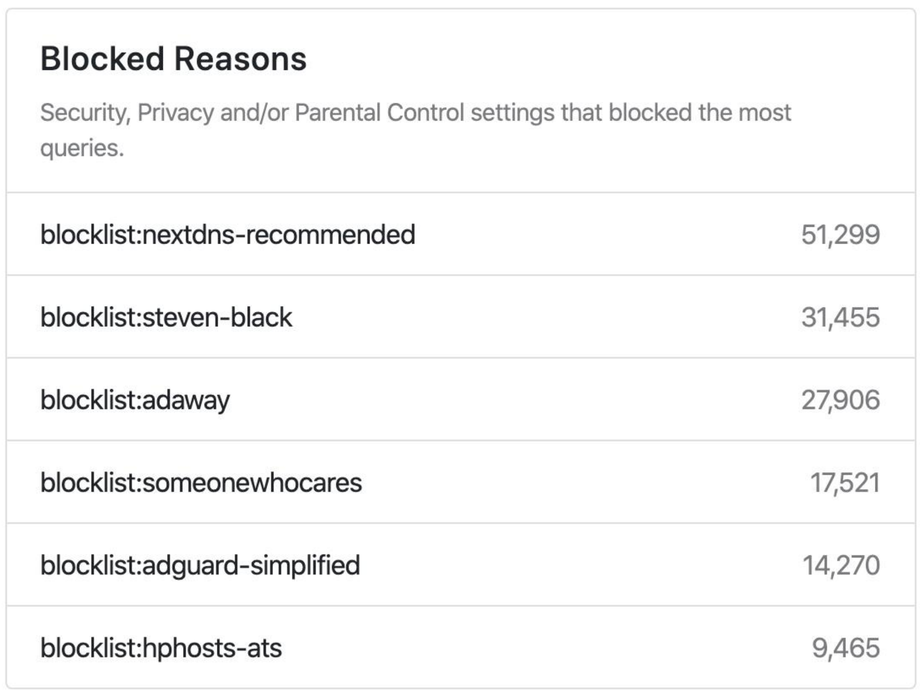
With DNSFilter, you’re able to dive into what domain categories are accessed most often on your network. Whereas with NextDNS, you only have the ability to see “Blocked Reasons,” which may only provide the name of a list such as “blocklist:steven-black.” This doesn’t give you true insight into why a particular site was blocked.

Another problem with these limited categories is you’re not able to see possibly malicious sites that were allowed by your filtering in NextDNS. As a DNSFilter user, you are able to toggle to “Allowed” threats. So even if you’ve decided to not include certain threat categories in your filtering policies, you still have the ability to monitor those threats.

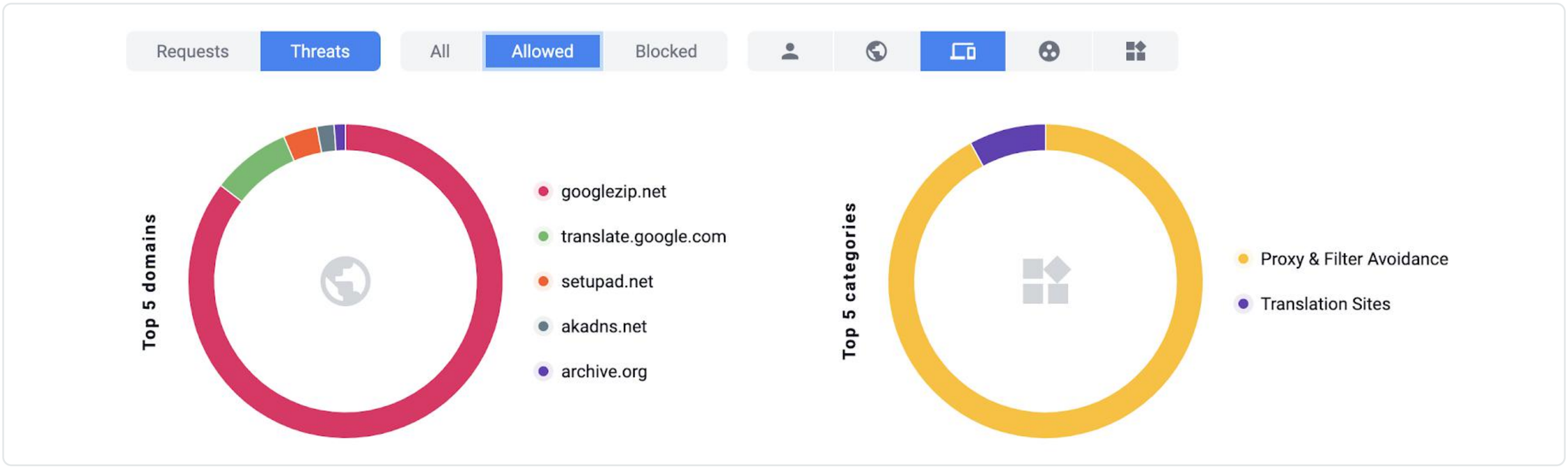
DNSFilter



NextDNS



NextDNS also gives users the ability to block certain applications. Platforms like Facebook can’t be blocked by simply adding facebook.com to a block list since Facebook is made up of dozens (or hundreds) of domains. NextDNS allows users to block 35 applications. But DNSFilter has nearly 700 applications that users can choose from. This gives users greater control, particularly if they’re interested in enforcing parental controls.

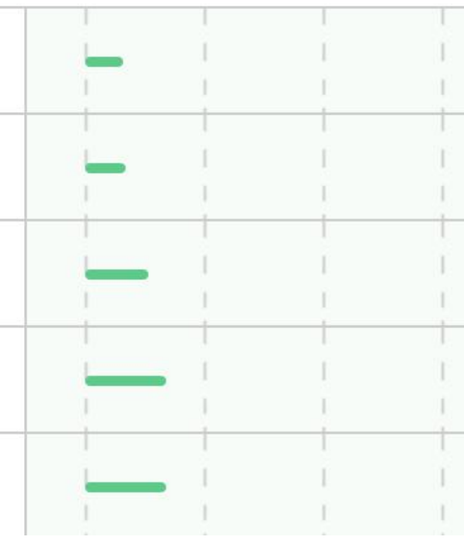


A faster network

DNSFilter and NextDNS both run BGP Anycast networks, but DNSFilter is faster worldwide and in North America according to DNSPerf.com.

Location: North America | Type: Raw Performance | Uptime | Quality | Period: Last 30 days

	DNS name	Query Speed
1	DNSFilter	6.6 ms
2	1.1.1.1	6.86 ms
3	Cisco Umbrella	10.77 ms
4	Google	13.8 ms
5	NextDNS	13.93 ms



Part of the success of DNSFilter's Anycast network is that we focus on working with three major hosting providers. Out of the top 10 hosting providers worldwide in terms of peer-to-peer connections, our preferred providers are in the top six. This means we are able to work with fewer providers while optimizing the strength and extent of our network.

NextDNS connects directly with 10 hosting providers, meaning they need to manage 10 individual relationships. And only one of their providers is in the top 10 peer-to-peer connections worldwide. If NextDNS wants to improve latency on their Anycast network, it's going to be more difficult to enforce changes than at DNSFilter since they work with so many providers.

Part of NextDNS' network strategy is to work with local hosting providers to achieve good latency in certain markets. Their network is fast in South America and Oceania because they work with localized hosting providers in those areas. But even in areas where they're fast, it still doesn't match DNSFilter's fastest speeds. And out of a list of 62 countries that both NextDNS and DNSFilter operate in, DNSFilter is faster than NextDNS 65% of the time.

If you're concerned with blocking more threats and having more granular control over your network, DNSFilter is the *only* solution that will help you achieve your goals.