



# DNSFilter VS. Webroot Comparison Report



This comparison document shares insights and data from a third-party reviewer - G2. With over 1 million reviews, G2 is the largest online tech marketplace available.

# Why is choosing the right **DNS Protection** important for your business?

## Security threats are on the rise

More instances of cybercrime were reported in 2020 over any other year on record (nearly 2,244 incidents per day), with losses totaling \$4.2 billion. But that doesn't account for the total amount workplaces are spending to deal with computer viruses, which averages \$55 billion per year.

Hackers are more active than ever, and they're targeting businesses instead of home users.

In 2020

**over 155.8 million**

individuals were impacted by data exposures.



There are roughly **18,000** phishing websites created *each day* and



**2,244** cybercrime incidents *occur daily*.

Between 2019 and 2020, ransomware attacks

**increased 62%** worldwide and **rose 158%** in just North America

2019



2020



Part of this is because businesses are becoming easier targets, and the rewards are bigger. Employees are using unauthorized web applications and accessing work networks from their home computers.

As the remote workspace trend gains more momentum, the lines between work and home devices have evaporated. The perimeter is gone. It's difficult for businesses to set up a firewall around their network and feel secure when an employee takes work equipment home.

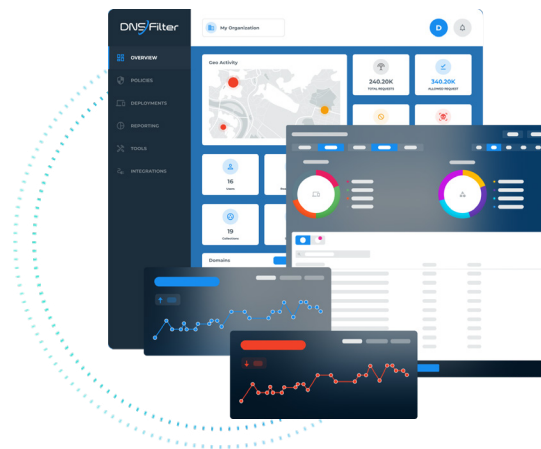
All of this is more alarming when you take into account that over half of all Americans aren't sure of what they should do in the event of a data breach. So if a breach does occur and the wrong person detects it—possibly from a home device—the cost of that breach may be higher than it should be.

For businesses to steer clear of a catastrophic data breach entirely, they need to put the right security measures in place.

## DNS Protection is the key

Cybercriminals' favorite tactics include setting up malicious web content. This comes in many forms, but the main culprits are:

- **Malware**
- **Phishing**
- **Cryptojacking**
- **Ransomware**
- **C2 callbacks**



These types of attacks account for nearly 50% of all data breach root causes.

With over 200,000 new website domains registered daily, it's impossible for a business to keep up with site blocking on its own. That's where DNS threat protection comes in. Implementing DNS security enables businesses to block new, questionable website content as well as known cyber threats.

## Webroot Vs. DNSFilter

Do you want DNS security or antivirus? At DNSFilter, we focus on DNS protection. While Webroot has a DNS filtering option, it's not as robust as solutions that were built exclusively for DNS protection. And if you only need content filtering, you still need to opt into Webroot's entire product suite.

We don't want to box you in—we just want to give you the best DNS protection on the market. With DNSFilter, you'll get a dedicated DNS security solution that features:

- **AI-based threat protection**
- **Whitelabeling for resale**
- **A global anycast network**
- **Lightning-fast response time**
- **A simple (and appealing) UI**
- **0-day threat protection**
- **Mobile Roaming Clients**

For companies with thousands of end users and devices, lacking these modern features just isn't an option. It basically means you have no visibility into your network and can't be flexible as needs change across departments.

# AI-Based Threat Protection




Unlike Webroot, which relies on third-party feeds to categorize threats, DNSFilter's software is driven by in-house AI. DNSFilter doesn't rely solely on domain list uploads, and because of our powerful technology we catch threats up to 6 days before other threat feed providers.

With over 200,000 domains created daily, it is ineffective to rely only on lists—your DNS security would become outdated very quickly if you implemented the wrong solution. DNSFilter can categorize threats in real-time, which means it can mitigate 0-day attacks and brand new cybersecurity threats on previously secure sites. In fact, 76% of the threats we catch, other threat feeds don't.

## Apply Changes Instantly

While Webroot includes similar functionality to DNSFilter, it's not nearly as fast at implementing changes. We understand that the changes you need to make to your policies and block lists should be instant. You can't wait around for a change to happen. And in some cases, Webroot customers have waited as long as 72 hours, with 30 minutes being the average.



"..... it takes a good 72 hours to pick up changes after they are made."

- Webroot user

## Anycast Network

---

DNSFilter operates an anycast network with over sixty worldwide data centers and two distinct networks. This means if a node serving your DNS requests goes down for any reason, DNSFilter will immediately reroute your traffic to the next-nearest location with zero packet loss. It also guarantees 100% uptime. It's part of why we're the fastest DNS resolver in North America (check out our stats at DNSPerf.com). And that means we won't slow down your network, but actually speed up DNS requests.

Webroot, on the other hand, does not operate an anycast network. This means a single point of failure could result in major regional internet outages.



When it comes to Webroot's DNS query speed, it's not clear how fast they are because they don't make their speeds public. However, we have seen some user reviews complaining about speed, including, "Sometimes the internet is very slow because it's going through the proxy. There are also some issues with it failing to connect frequently." Webroot even responded to this review saying, "experiencing changes in your connection speed when using a DNS solution is to be expected," which you can see from the results on DNSPerf is not true of DNSFilter.

Also, because Webroot doesn't operate an anycast network, there is nothing to stop your DNS query in Sydney, Australia from going all the way to New York, New York—wasting time sending your information across continents and delaying your resolution speeds.

We can't guarantee Webroot's speeds, but we can absolutely guarantee ours.



# Head-to-Head Key Features

Features		
Anycast Network	✓	✗
DNS Response Time	8ms	>100ms
Real-time Domain Categorization	✓	✗
Imagery-based Anti-phishing	✓	✗
Time it Takes to Reflect Policy Changes	Instant	Avg. time 30 min
Captive Portal Support	✓	✗
Desktop Roaming Clients	Windows & MacOS	Windows
Mobile Roaming Clients	✓	✗
LAN Proxy / Virtual Appliance	✓	✗
Whitelabeled for Resale	✓	✗

## Ease of use

---

When it comes to ease of use, DNSFilter outranks Webroot in the following categories on G2:

- **Ease of use**
- **Ease of admin**
- **Quality of support**
- **Off-Network Protection**
- **BYOD Protection**
- **DNS Lookups**
- **Advanced Traffic Filtering**
- **Policy Enforcement**
- **Ease of setup**
- **Ease of doing business with**
- **Product direction**
- **Guest Network Protection**
- **Native DNS over HTTPs (DoH)**
- **Threat Protection**
- **Whitelisting**
- **Incident Reports**
- **Multi-Network Management**

When it comes to features and product offering, DNSFilter customers tend to find their requirements consistently met. Common complaints about Webroot, however, primarily revolve around functionality and missing features.

One Webroot user on G2 said, “I dislike the fact there aren’t more options to do. As of now, all I can do is block a domain and change policies. I feel there should be more customization or more features..” While other users note, “it would either block everything or nothing at all,” and, “It’s also a bit disappointing that there’s no DNSP agent available for Mobile devices.”

While features seem to be a major sore spot for Webroot customers, DNSFilter customers rank DNSFilter as “Best Meets Requirements” and “Best Results” in the DNS Security category on G2. A customer on G2 stated, “I also like the speed of returning DNS results, and the speed with which the filters are updated with new threats.” While another said, “the product meets all our requirements.”















# DNSFilter is built for MSPs

DNSFilter has a fully multi-tenant MSP dashboard that allows for complete whitelabeling, including block page customization and forwarding. Our dashboard, roaming applications, and transactional emails will appear to come from you, not us.

We also share whitelabeled marketing materials for our MSP partners to help them succeed in closing more sales and hitting their ROI goals.

MSP customers will be interested to know that only DNSFilter allows whitelabeling. When MSPs use Webroot, everything has Webroot’s logo on it. For MSPs that want to completely white label DNS security, Webroot is not the right choice.

RATINGS	DNSFilter	WEBROOT®
Meets Requirements	 93%	 93%
Ease of Use	 95%	 92%
Ease of Admin	 94%	 89%
Quality of Support	 94%	 91%
Ease of Doing Business With	 97%	 91%
Positive Product Direction	 94%	 90%



PROTECTION	DNSFilter	WEBROOT®
Quarantine	91%	92%
Continuous Monitoring	89%	92%
Off-Network Protection	90%	89%
Guest Network Protection	91%	90%
BYOD Protection	94%	90%
Native DNS over HTTPs (DoH)	90%	89%
<b>FUNCTIONALITY</b>		
Meets Requirements	93%	87%
Ease of Use	89%	88%
Ease of Admin	91%	86%
<b>ADMINISTRATION</b>		
Quarantine	91%	92%
Continuous Monitoring	89%	92%
Off-Network Protection	90%	89%
Guest Network Protection	91%	90%
BYOD	94%	90%

# How Do Leading DNS Security Products **Stack Up?**

---

DNSFilter is the fastest, easiest-to-use, and most resilient DNS protection on the market. While the competition lags behind in use of AI, speed, implementation, and support, DNSFilter is expanding the definition of “DNS protection” with new functionality that will complete your security stack.

No matter where your employees are in the world, DNSFilter can be your first line of defense from security threats and block your users from malicious websites.

Our threat detection and categorization is more accurate in head-to-head comparisons and we catch threats days before the competition. That's because we don't rely on people to encounter a threat and add it to a list. Our AI blocks threats in real-time, when it matters most.

**Take your DNS protection into the future with DNSFilter.**

See firsthand how DNSFilter is challenging the way the industry thinks about DNS security.

[Request a Demo >](#)

