DNSFilter

DNSFilter VS. Cloudflare Comparison Report

Why is choosing the right **DNS Protection** important?

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:

- **Phishing**
- **Ransomware**
- **Malware**
- **Cryptojacking**
- **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.

Narrowing down your options

When it comes to selecting the right DNS threat protection software for your organization, most of the companies we talk to narrow it down to two options: DNSFilter® and Cloudflare®.

Cloudflare Vs. DNSFilter

At DNSFilter, our mission has always been to do one thing and do it well. While other competitors have a host of offerings, it usually means that their DNS filtering service doesn't get the full attention it deserves. Cloudflare's DNS filtering capabilities are very young, having been announced in March 2020.

Their DNS filtering product (Cloudflare Gateway) is meant to integrate with their Cloudflare Access subscription. Because of this, Cloudflare Gateway is bare bones and lacks several features:

- **No detailed reporting by location or user**
- **No bulk management of allow & block lists**
- **No business-grade rollup reports**
- **No whitelabeling for Managed Service Providers**

For companies with upwards of thousands of end users and devices, lacking these 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.

Fighting for the fastest spot

Everyone knows that Cloudflare is fast. But DNSFilter? It's just as fast, and sometimes faster. Cloudflare and DNSFilter have been neck-and-neck for a while, consistently fighting for the top spot on DNS ranking site DNSPerf.com.

We're always in the fastest spot in North America for DNS resolvers. We're also No. 1 in Africa and at the top of the pack for South America and Europe.

Ease of use

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

- Ease of use
- Ease of admin
- Quality of support
- Ease of setup
- Ease of doing business with
- Product direction

Whether it's onboarding or troubleshooting, DNSFilter customers get the support they need quickly. Common complaints about Cloudflare, however, primarily revolve around support.

Some examples of what some **Cloudfare users** from G2 said -

> "The support staff didn't read the notes on the ticket, didn't understand what was going on, gave solutions that didn't work at all, were just completely incompetent. They took 3-4 days between some responses."
> **- Cloudflare user**

> "On-boarding support is non-existent. If you have an issue setting things up expect a period of extended downtime"
> **- Cloudflare user**

DNSFilter Support

Best Relationship
SUMMER
2021

Best Support
SUMMER
2021

Easiest To Do Business With
SUMMER
2021

While support seems to be a major sore spot for Cloudflare customers, **DNSFilter customers rank DNSFilter as "Best Support"** in the DNS Security category on G2. A customer on G2 stated that DNSFilter is "simple to setup and deploy across the network . . . The support people I've worked with have been amazing to work with and respond quickly."

While another said, "the tool works as it should and sales as well as support are top notch when something doesn't work!"

"The support from DNSFilter at all levels is also excellent."
- Customer Max D.

"Very responsive support and dev departments to implement new ideas."
- Customer Rick S.

"The support people I've worked with have been amazing to work with."
- Network Admin

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 Cloudflare, everything has Cloudflare's logo on it. For MSPs that want to completely white label DNS security, Cloudflare is not the right choice.

RATINGS	DNSFilter	CLOUDFLARE®
Meets Requirements	93%	93%
Ease of Use	96%	92%
Ease of Admin	94%	90%
Quality of Support	94%	84%
Ease of Doing Business With	97%	88%
Positive Product Direction	94%	87%

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 >

DNSFilter