# DNSFilter Security Practices

## Introduction

DNSFilter believes in giving you a secure and performant DNS solution. In order to fulfill that mission, we've designed our systems from the ground up to protect your data and mitigate DNS attacks. This document outlines the security standards and procedures that we have in place.

## Organizational Security

All DNSFilter staff undergo an onboarding procedure which includes a full background investigation and signing a non-disclosure agreement to protect sensitive information, including DNSFilter technology and customer data.

The "principle of least privilege" is employed so that staff are only given access to systems and applications which are necessary for them to access to fulfill their job functions. If their job no longer requires them to access a given system, their credentials are downgraded or revoked. Only executives (CXO level) are granted administrative access to SaaS applications in use by DNSFilter, all other staff have manage, edit, or read-only access which is appropriate to their engagement with that application.

Computing resources which are issued to staff (laptops, mobile devices) have full disk encryption and location sharing enforced so that in the event of theft or compromise, sensitive information is not at risk. Multi-factor authentication (2FA) is enforced organization-wide for every 3rd party application which offers this capability.

Our Security Operations team consists of individuals with a background in information security and penetration testing.

Upon separation from DNSFilter, all access to DNSFilter systems and 3rd party applications is immediately terminated.

# Infrastructure Security

## Infrastructure Security Operations (SecOps)

DNSFilter infrastructure is monitored in real-time at several levels:

- System health monitors ensure that our infrastructure performs at an optimal level and that impending hardware/software failures can be diagnosed and remedied.
- Traffic monitoring ensures that DNS traffic flows smoothly from customer sites to our several datacenters around the world. BGP Anycast also ensures that problems are routed around.
- DNSFilter servers are hardened by employing bastion hosts and multiple layers of process privilege separation. Alerting is in place to notify the operations team if/when requirements are breached.
- DNSFilter incorporates services which monitor third-party libraries for vulnerabilities. Libraries, programming interpreters, and operating systems are regularly updated on all server nodes.
- SSH access to servers is heavily restricted to only necessary staff.
- Rogue process monitoring ensures that the security team is notified of any breaches or vulnerabilities in infrastructure.

## DNS Security

As a DNS provider, we are keenly aware that we are a target of DNS-based attacks such as Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM), DNS Amplification, and DNS cache poisoning. In order to mitigate this, DNSFilter separates our infrastructure at various points:

- Server nodes operate independently so that MITM and cache poisoning attacks would be restricted in effect.
- Our root CA certificate for blocked pages is manage by only a couple personnel. In the case of compromise, we have the ability to notify customers along several channels.
- Resolver networks DNS1 & DNS2 operate within two separate BGP Anycast networks.
- The DNSFilter resolver system is a closed system which does not answer to queries from unknown sources. This greatly reduces the potential for DNS amplification attacks.
- Our infrastructure monitoring allows us to pinpoint customers which have compromised devices and are participating in DDoS attacks. We work with customers for resolution and can cut offending traffic if necessary.

## Product Security

DNSFilter regularly updates our software through the use of Continuous Integration/Continuous Delivery (CI/CD) mechanisms. This includes our frontend application, API, roaming clients, and Query Processor.

Code is committed to secure, version-controlled repositories where it is peer-reviewed. Once this is complete, it is deployed to a development environment where a thorough Quality Assurance process is employed. The QA process consists of testing by full-time staff as well as repeated and automatic software tests. Software also checks code dependencies for software vulnerabilities.

Privilege separation is employed so that software developers are unable to push code changes to the production environment. Only key personnel have the capability to bring software changes from the development to the live environment.

Binaries for all roaming applications (Windows, MacOS, Android, iOS) undergo a strict code signing process. Limited personnel have access to the signing keys.

## Customer Data Security

DNSFilter takes seriously the responsibility that we have to safeguard your Personally Identifiable Information (PII). There are two ways that we ensure the maximum safety and security of customer data:

**1.** Authentication and Payments are processed externally. DNSFilter does not process or store customer credentials or payment information on our servers. We use industry-leading authentication and payment processor solutions. These vendors only store password and payment information in a hashed format.
**2.** DNSFilter data is siloed. Customer data is split among disparate systems. Our customer database, statistics database, and routing nodes all only hold separate pieces of customer data. This ensures maximum difficulty in any attempt to exploit our systems. Much of the customer information that we hold, such as location and network addressing information, is more readily available to potential attackers in the public domain and is not of a sensitive nature.

# Customer Data Privacy

DNSFilter publicly posts how customer data is utilized internally, as well as by all 3rd party applications which are used by our staff. This information can be found at dnsfilter.com/privacy-policy/.

# FAQ

### Do you have PCI compliance?

PCI compliance is not necessary for DNSFilter, because we do not process or store payment information.

### Are you in compliance with the GDPR?

Yes.


© DNSFilter, Inc. All rights reserved.