DNSFilter

GETTING STARTED

A Guide to your DNSFilter Setup

This slide deck will provide you with set up links and instructions in alignment with those shared in the onboarding webinar, to include:

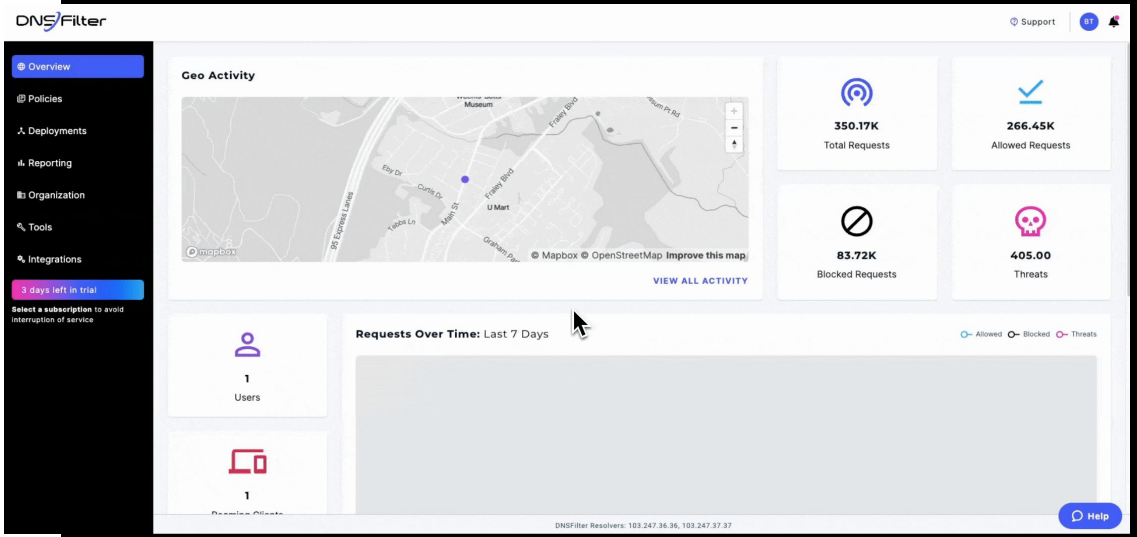
- **Part 1** Set up instructions
- **Part 2** Use case specific guidance
- **Part 3** DNS circumvention prevention

RESOURCE LINKS IN THIS DECK ARE UNDERLINED

CREATING FILTERING POLICIES

Policies are used to:

- Block broad domain types via Categories
- Create allow and block lists
- Set filtering schedules for time-of-day restrictions
- Customize block pages



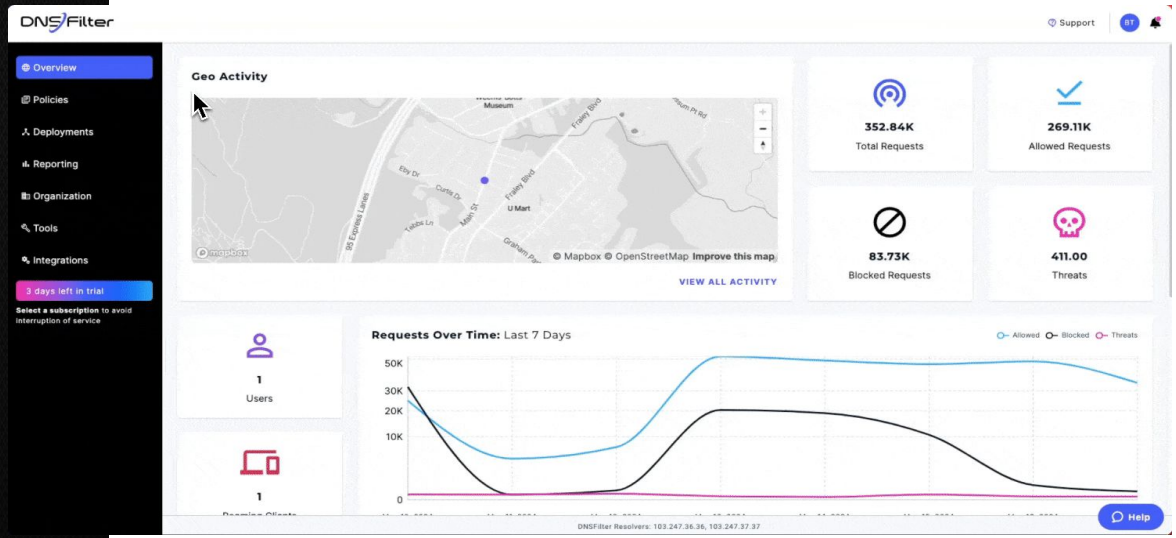
SETUP YOUR SITE

Different Network address abilities include:

- **NAT IPs (LAN subnet policy assignment)**
- **Dynamic hostnames**
- **IP subnets up to /24**

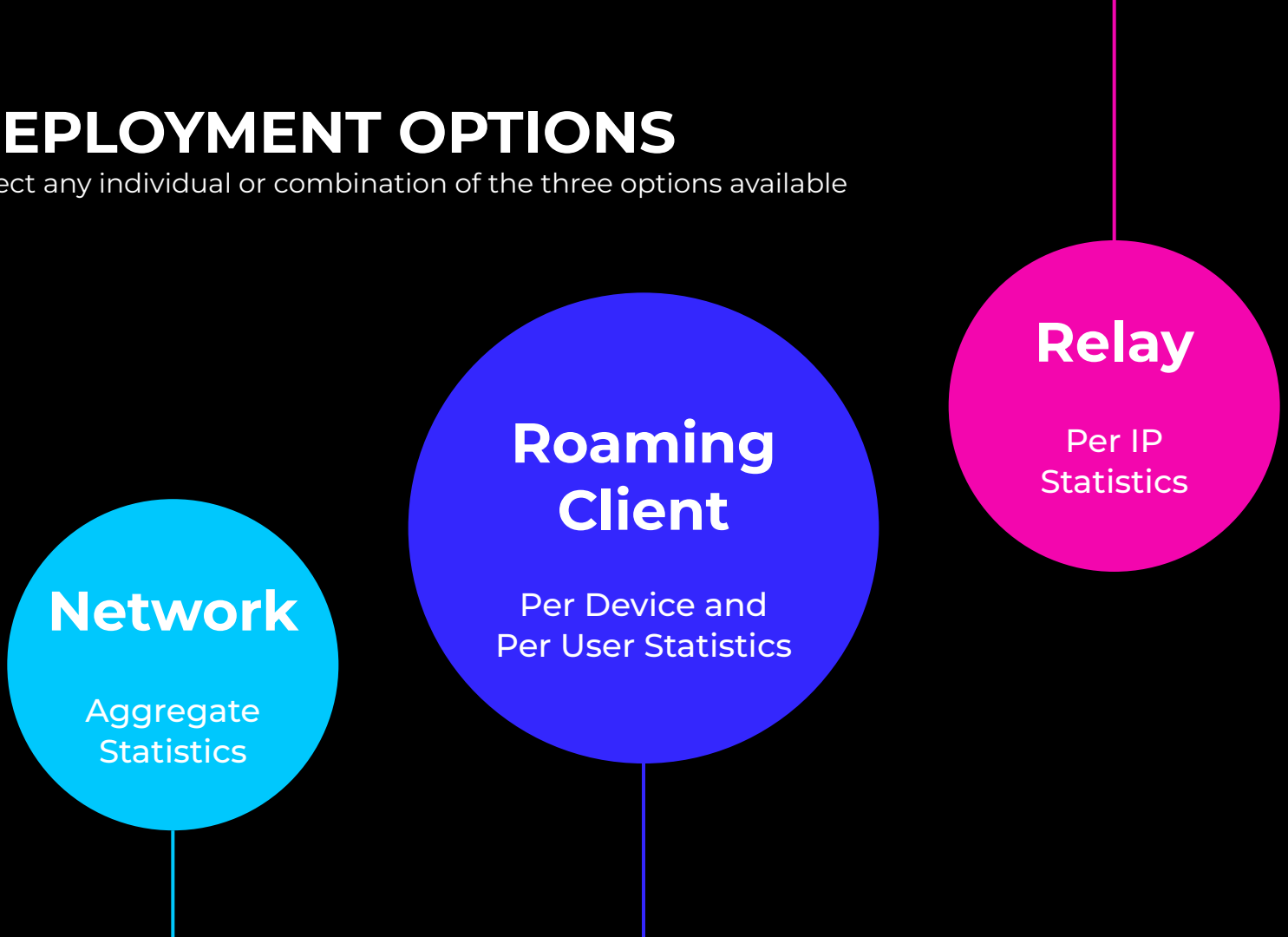
DNSFilter does not serve requests to unknown IP addresses

💡 **A site must be added to recognize and respond to network queries**



DEPLOYMENT OPTIONS

Select any individual or combination of the three options available



Tip 💡 Search “how to change DNS on *Your ISP’s Name*”

DEPLOYMENT OPTIONS
Network Forwarding

PROTECTION GOALS

- Protection on your network
- No need for offsite protection
- Public or Guest Wi-Fi
  - E.g. hotels, airports, restaurants, schools, stores, and more
- Simple deployment without extra software
- Complete coverage of LAN devices

IMPLEMENTATION

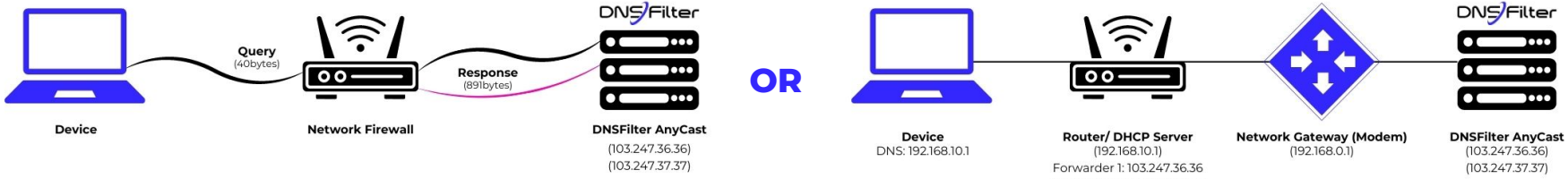
- Limited to 1 policy (up to 7 with NAT IPs)
- Reporting at the WAN level

DATA VISIBILITY

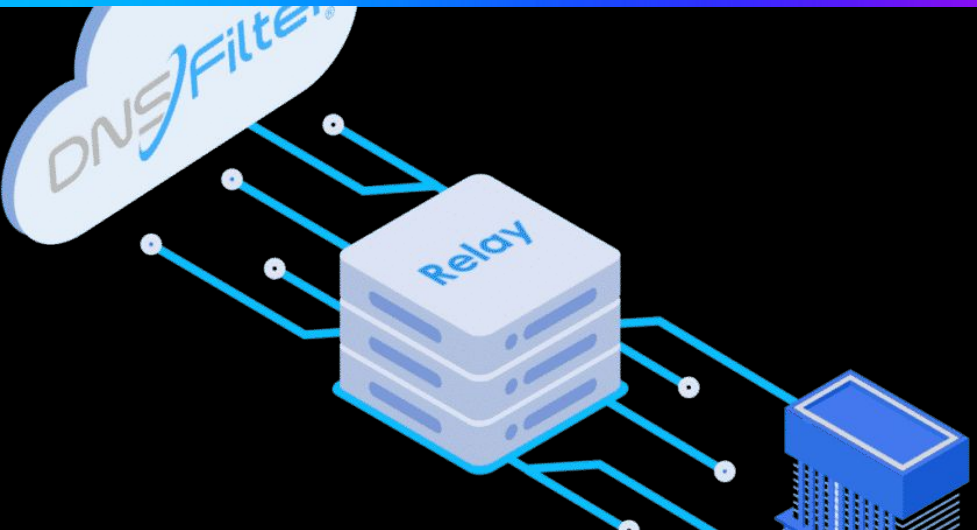
- Aggregate data with traffic visibility for the whole network

PREPARE YOUR ENVIRONMENT

- Check that your ISP is not transparent proxying DNS traffic or using CGNAT
- Confirm it is free of conflicting software or hardware settings:
  - Any existing firewall, VPN, and security app rules or settings are set to allow traffic to the correct IPs
  - End users cannot circumvent the filtering policies
- All of the necessary IP address are accounted for in the DNSFilter dashboard



DEPLOYMENT OPTIONS
Relay



PROTECTION GOALS

- Apply filtering policies by IP or subnet on your network
- Desire for per-machine reporting and protection
    - When Roaming Client can't be installed

IMPLEMENTATION

- Requires machine, VM, or docket to run high availability
    - No user-level filtering or user-level reporting

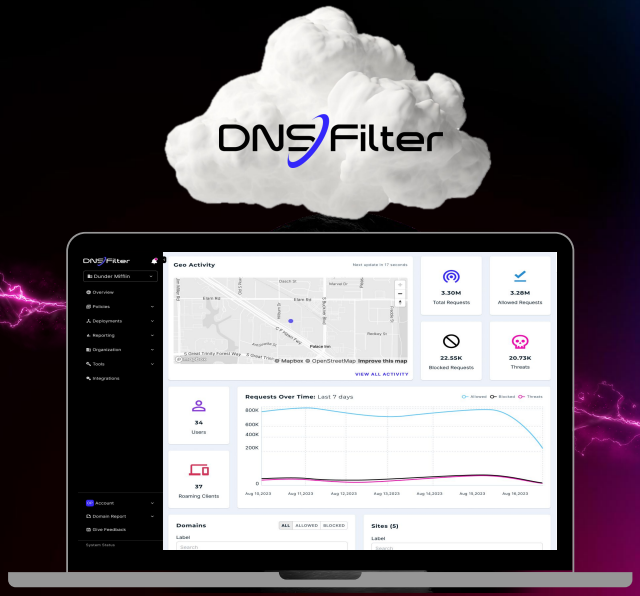
DATA VISIBILITY

- Per machine or per IP statistics

PREPARE YOUR ENVIRONMENT

- DNS traffic isn't able to reach DNSFilter without issue:
    - DNS response time is slow
    - Dashboard Sites show inactive or do not come online
    - End users cannot circumvent the filtering policies
- Relay deployment isn't auto-updating as expected

DEPLOYMENT OPTIONS
Roaming Client



PROTECTION GOALS

- Protection on your network and when traveling or remote
- Easily set or change policies for large groups of computers
    - E.g. teachers/students, corporate departments, public/private computers
- Available on all platforms
    - Windows, Mac, iOS, Android, and Chromebook

IMPLEMENTATION

- Requires software installation and ongoing maintenance (either through manual or automatic updates)

DATA VISIBILITY

- Granular per device and per user reporting

PREPARE YOUR ENVIRONMENT

- Losing Wi-Fi access in public places like airports or hotels
- VPNs are set to allow DNS traffic to reach DNSFilter
- Roaming Client connectivity issues:
    - It cannot bind to the correct port
    - There's limited internet connectivity once installed and online
    - macOS listener address and port conflict

TESTING YOUR CONNECTION

Once you've configured your deployment, you can test your network connection by:

1

debug.dnsfilter.com

You can test all categories at once by visiting debug.dnsfilter.com

2

Browse an allowed domain

Attempt to browse a well-known domain that is allowed by your policy (google.com)

3

Visit a blocked domain

Attempt to visit a domain in your Block list in Incognito Mode

USE CASES FOR YOUR ENVIRONMENT

Click the title of your use case to explore recommendations

01

Organization

Protect against cyber threats and enforce content filtering to maintain productivity and security across your network.

02

Church or Non-Profit

Block inappropriate content and ensure that their networks are secure and in alignment with your organizational values.

03

Hotels

Safeguard guest Wi-Fi networks from malware and phishing attacks while providing a family-friendly browsing environment.

04

Education

Enforce safe browsing, block harmful content, and protect students from online threats, ensuring a secure and compliant learning environment.

05

MSP

Provide your clients with robust threat protection, content filtering, and compliance reporting as part of a comprehensive managed service offering.

06

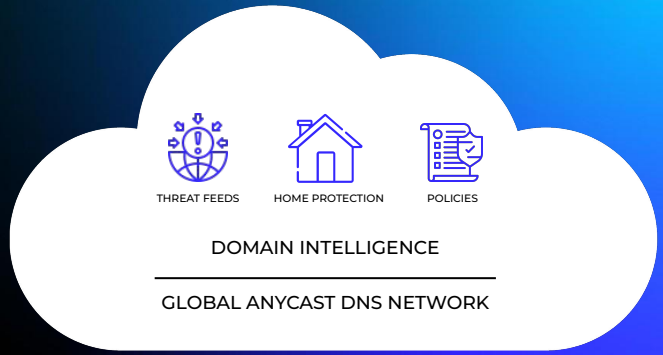
Home Users

Create a safe online environment by blocking malicious sites and inappropriate content, ensuring a secure internet experience for the whole family.

DNSFilter

HOME USERS

Focus on creating a safe and secure browsing environment, protecting against common online threats, and blocking inappropriate content.



POLICY SETTINGS:

An average policy for home users typically blocks adult content, malware, phishing, violence, gambling, and possibly certain social media sites based on the needs of the household.

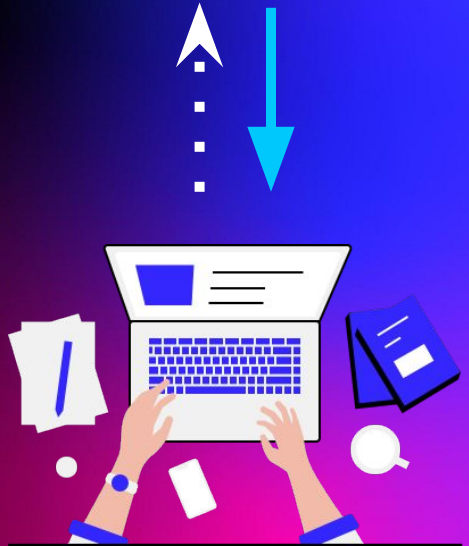
SAFESEARCH and YOUTUBE RESTRICTED MODE:

Optional **Depending on the priorities of your home protection and settings**

DEPLOYMENT:

Configuring directly on the home router or gateway.

Optional **Roaming Clients for mobile phones or laptops, particularly for those that frequently leave the home network.**



DNSFilter

CHURCHES & NONPROFITS

Focus on maintaining a secure, respectful, and productive online environment that aligns with the organization's values and mission.

POLICY SETTINGS:

An average DNSFilter policy for churches and nonprofits would typically block adult content, malware, phishing, violence, hate speech, and illegal activities.

Optional restrictions on gambling, social media, and streaming media based on the organization's needs.

SAFESEARCH and YOUTUBE RESTRICTED MODE:

Enabled

DEPLOYMENT:

Configuring directly on the organization's main router or firewall for easy management of content filtering and security settings.

Optional Roaming Clients on specific devices that are frequently used outside of the network.

DNSFilter

EDUCATION

SUPPORTING CIPA COMPLIANCE

As students progress from grade school to university, policies generally evolve to offer more flexibility and access, aligning with the increasing level of maturity and autonomy, while maintaining necessary security and content protections.

PRE-K THROUGH 8TH:

Policy settings are normally aligned with our default policy for students and additional categories are enabled for faculty/guest Wi-Fi on separate IPs

YOUTUBE RESTRICTED MODE:

Enabled, Strict

SAFESEARCH:

Enabled

DEPLOYMENT:

Configuring directly on the school's primary router or firewall.

Optional Roaming Clients for take-home devices or a BYOD (Bring Your Own Device) policy

HIGH SCHOOL:

Default policy restrictions are normally set along with categories such as shopping, social networking, search engines, drugs, alcohol, etc.

YOUTUBE RESTRICTED MODE:

Enabled, Moderate

SAFESEARCH:

Enabled

DEPLOYMENT:

Configuring directly on the school's primary router or firewall.

Optional Roaming Clients for take-home devices provided by the school

COLLEGE/UNIVERSITY:

Blanketed protection from Threats but overall open access to general domain categories

YOUTUBE RESTRICTED MODE:

Optional Enabled, Moderate

SAFESEARCH:

Optional Enabled

DEPLOYMENT:

Configuring on the university's core routers, firewalls, or DNS servers.

Optional Roaming Clients for take-home devices on loan to students or faculty

DNSFilter

HOTELS & HOSPITALITY

Focus offering a secure, reliable, and guest-friendly Wi-Fi service, protecting both the hotel's network and its guests while providing a seamless online experience.

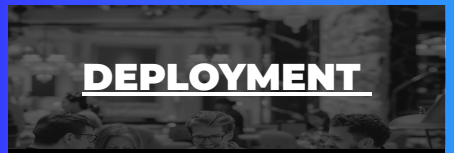
POLICY SETTINGS

A standard setup blocks our Threat categories at a minimum, with additional adjustments to adult content made to align with the access to Wi-Fi on premises

Optional Some end-users have a blank policy strictly for CSAM monitoring and prevention without additional preset limitations

SAFESEARCH & YOUTUBE

Optional Enabled, Moderate



DEPLOYMENT

Apply policies to specific VLANs or subnets within the network, segmenting traffic based on different user groups or areas, such as guests and employees.

Optional Install as an agent on specific devices, that often go off-site and require protection.

DNSFilter

ORGANIZATION & BUSINESS

Focus on maintaining a secure, respectful, and productive online environment that aligns with the organization's values and mission.

POLICY SETTINGS:

An average policy setup for organizations would typically block all threat categories, adult content, violence, terrorism & hate, and illegal activities

Optional restrict social media, streaming media, and gambling based on company policies as well as advanced settings

SAFESEARCH and YOUTUBE RESTRICTION MODE:

Optional Enabled, Moderate

DEPLOYMENT:

Configuring directly on the primary routers, firewalls, or DNS servers and as an agent on specific devices that are for remote or mobile users depending on protection and data visibility needs.

SYNC TOOLS for ENTRAID (aka ACTIVE DIRECTORY):

Synchronize groups of users to the DNSFilter Dashboard and apply policies, schedules, and block pages at the User or Collection Level

- ↬ Any changes you make to your on-prem or cloud AD will be reflected in your Dashboard

DNSFilter

MANAGED SERVICE PROVIDERS (MSP)

POLICY SETTINGS:

The global policy setup ensures a secure, compliant, and productive environment for clients, while also providing MSPs with the flexibility to assign tailored policies to each client's specific requirements.

SAFESEARCH and YOUTUBE RESTRICTED MODE:

Optional Disabled

DEPLOYMENT:

Preferred Install agents on individual client devices, such as laptops, tablets, and mobile devices, particularly for clients with remote or mobile workforces.

Alternative Configuring directly on each client's primary routers, firewalls, or DNS servers.

MULTI-TENANCY DASHBOARD PROVIDES YOU ACCESS TO

- Sub-organizations
  - Manage multiple client networks separately under a single account, providing tailored DNS filtering policies and reporting for each client
- Whitelabeling
  - Rebrand and customize our service with your own branding, enabling you to offer DNSFilter as a part of your portfolio
- View activity for all clients at once
  - Easily monitor, configure, and report on DNS filtering policies across all clients from a single dashboard

SYNC TOOLS for ENTRAID (aka ACTIVE DIRECTORY)

- Synchronize groups of users to the DNSFilter Dashboard and apply policies, schedules, and block pages at the User or Collection Level
  - Any changes you make to your on-prem or cloud AD will be reflected in your Dashboard

NAVIGATING PUBLIC WI-FI

PROTECT YOUR USERS AND YOUR ENVIRONMENT

BLOCKING ACCESS TO

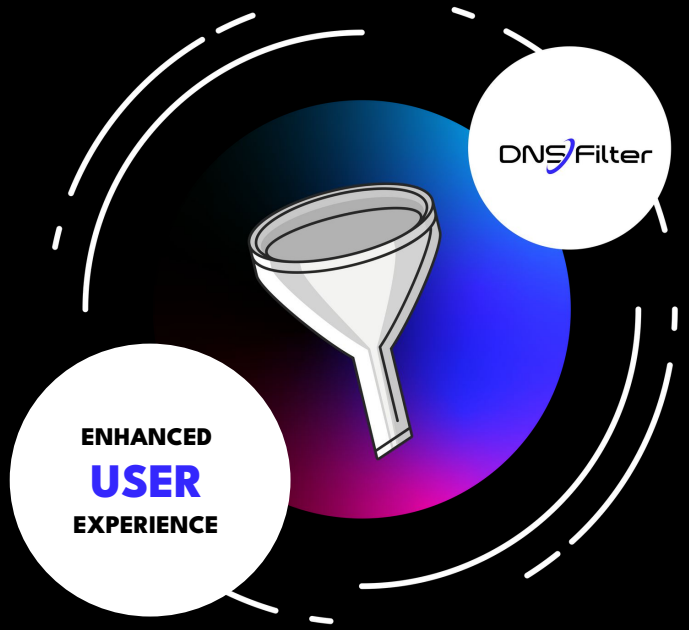
Safeguard users on public Wi-Fi from threats common to unsecured networks

PREVENTING ACCESS TO

Inappropriate or harmful content, important in family-friendly or business environments

BLOCKING MALICIOUS SITES

Helps protect users' privacy and secure their data on public Wi-Fi networks



DEPLOYMENT IS EASY

Begin protecting your environment with Network Forwarding. This provides a blanket policy that covers all devices on your network.

CONFIGURE YOUR NETWORK

Depending on the size of your business, you'll likely configure your network traffic to point toward DNSFilter from the DHCP Server, though small businesses may find it easier to configure from a router.

QUESTIONS?

If you have questions later, you can always reach out to us in the Community!

help.dnsfilter.com
DNSFilter Knowledge Base

Direct download link
New Customer Roadmap Checklist

Understanding DNS Insights
Reporting Dashboard Guide

Review the guides below
Migrating to DNSFilter

- Cisco Umbrella
- Cloudflare
- ZScaler
- Webroot