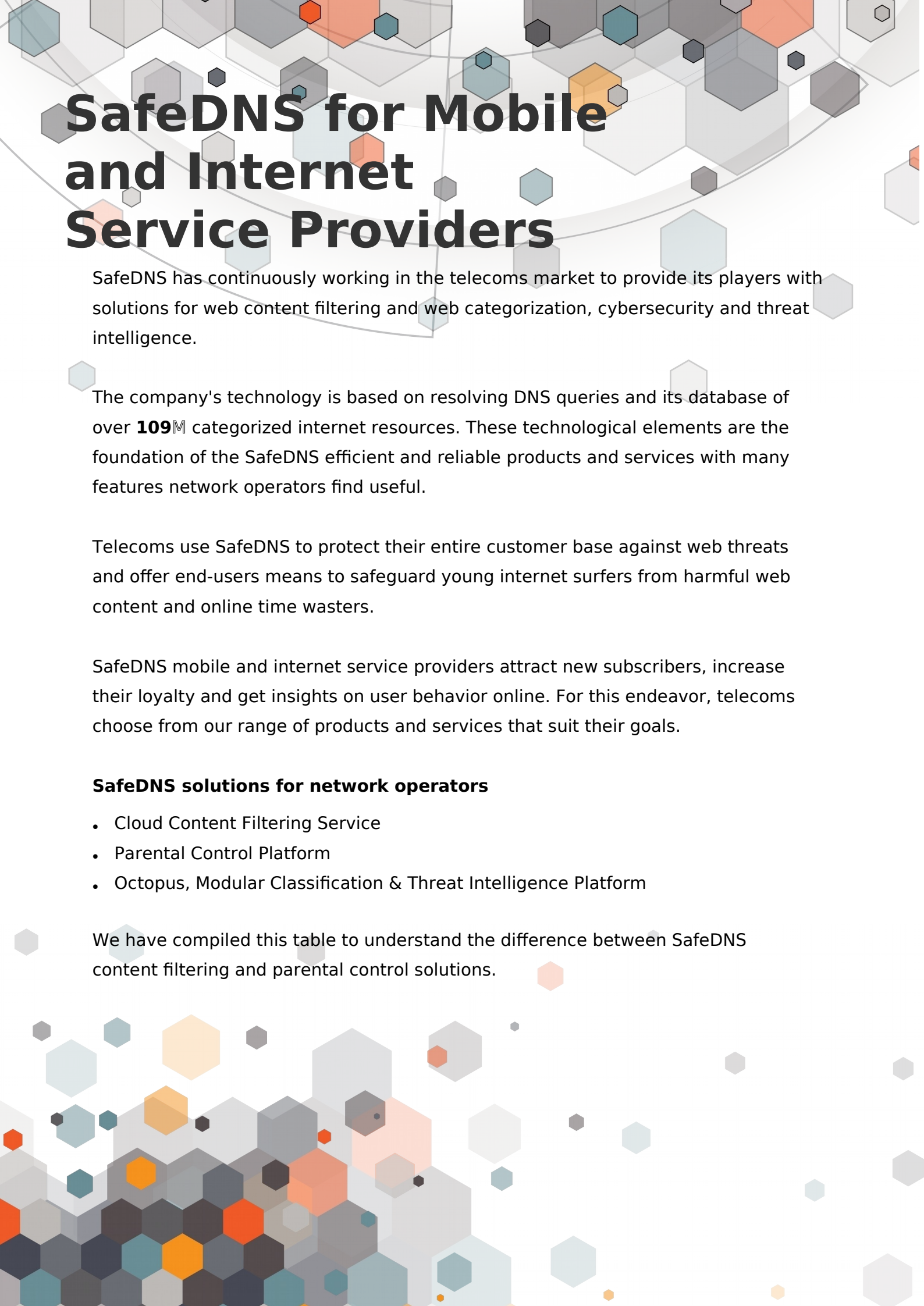




# SAFEDNS

**Solutions for  
Mobile and  
Internet Service  
Providers**



# SafeDNS for Mobile and Internet Service Providers

SafeDNS has continuously working in the telecoms market to provide its players with solutions for web content filtering and web categorization, cybersecurity and threat intelligence.

The company's technology is based on resolving DNS queries and its database of over **109M** categorized internet resources. These technological elements are the foundation of the SafeDNS efficient and reliable products and services with many features network operators find useful.

Telecoms use SafeDNS to protect their entire customer base against web threats and offer end-users means to safeguard young internet surfers from harmful web content and online time wasters.

SafeDNS mobile and internet service providers attract new subscribers, increase their loyalty and get insights on user behavior online. For this endeavor, telecoms choose from our range of products and services that suit their goals.

## **SafeDNS solutions for network operators**

- Cloud Content Filtering Service
- Parental Control Platform
- Octopus, Modular Classification & Threat Intelligence Platform

We have compiled this table to understand the difference between SafeDNS content filtering and parental control solutions.

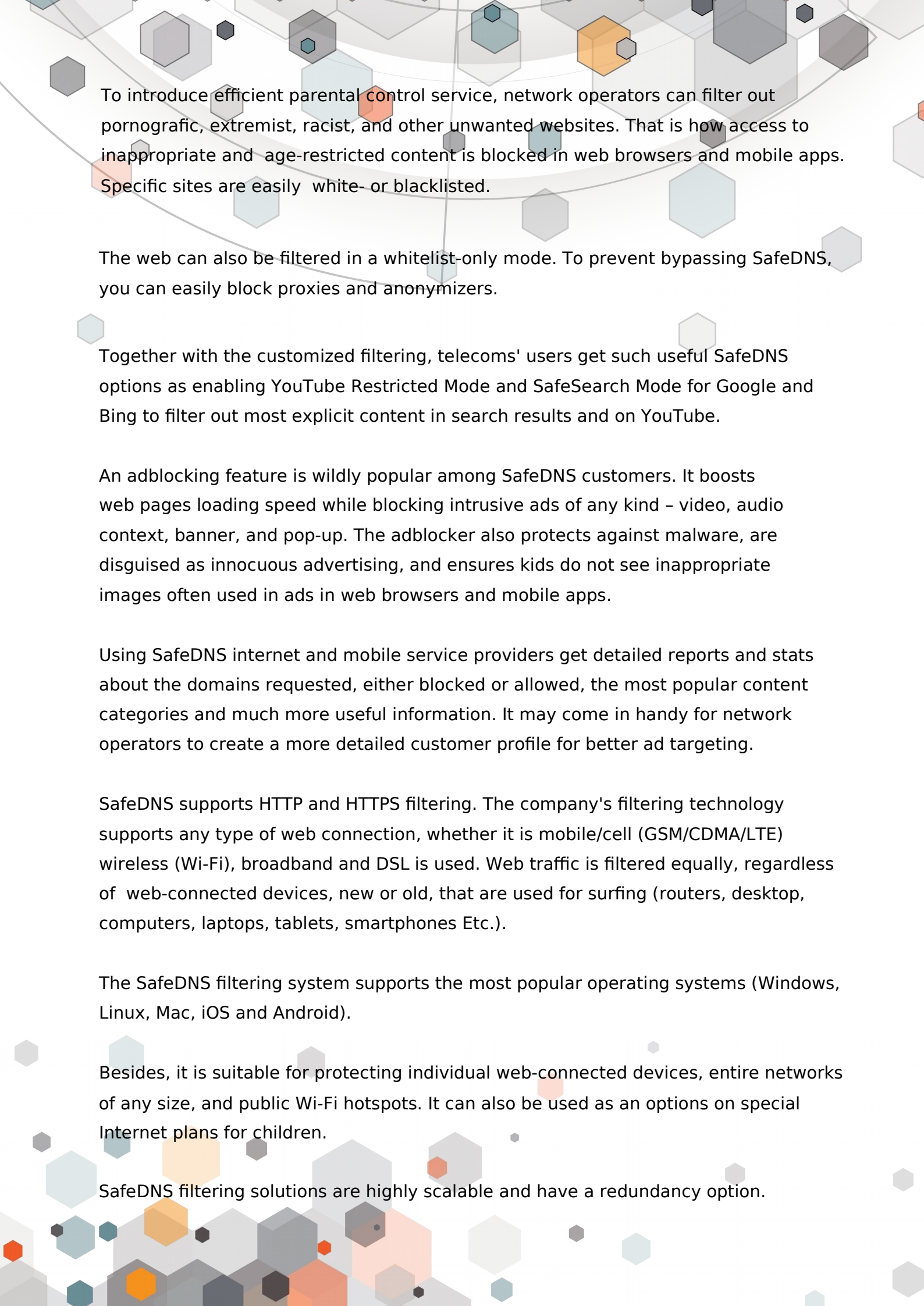
	Cloud Filtering Service	Parental Control Platform
Protection against web threat	!	!
Internet content filtering	!	!
OSS/ BSS integration	!	!
Protection of users behind NAT	!	!
Regulation compliance	!	!
Internal IP addresses visibility		!
User dashboards	!	
Full IPv6 support		!
The fastest to deploy	!	
Multiple customization opportunities	!	!
White labeling	!	!
Detailed reports and stats	!	Minute-by-minute stats
Scalability	!	!

Now we'd like to speak about all of these solutions in more detail.

## Content Filtering Solutions

Regardless of telecoms' implementation with SafeDNS product, our filtering technology ensures their end-users only access the allowed websites. To fine-tune the filtering to individual needs, SafeDNS customers choose what online resources to block or allow among the 61 categories containing the most popular internet resources, and almost all of the most dangerous ones.





To introduce efficient parental control service, network operators can filter out pornographic, extremist, racist, and other unwanted websites. That is how access to inappropriate and age-restricted content is blocked in web browsers and mobile apps. Specific sites are easily white- or blacklisted.

The web can also be filtered in a whitelist-only mode. To prevent bypassing SafeDNS, you can easily block proxies and anonymizers.

Together with the customized filtering, telecoms' users get such useful SafeDNS options as enabling YouTube Restricted Mode and SafeSearch Mode for Google and Bing to filter out most explicit content in search results and on YouTube.

An adblocking feature is wildly popular among SafeDNS customers. It boosts web pages loading speed while blocking intrusive ads of any kind – video, audio context, banner, and pop-up. The adblocker also protects against malware, are disguised as innocuous advertising, and ensures kids do not see inappropriate images often used in ads in web browsers and mobile apps.

Using SafeDNS internet and mobile service providers get detailed reports and stats about the domains requested, either blocked or allowed, the most popular content categories and much more useful information. It may come in handy for network operators to create a more detailed customer profile for better ad targeting.

SafeDNS supports HTTP and HTTPS filtering. The company's filtering technology supports any type of web connection, whether it is mobile/cell (GSM/CDMA/LTE) wireless (Wi-Fi), broadband and DSL is used. Web traffic is filtered equally, regardless of web-connected devices, new or old, that are used for surfing (routers, desktop, computers, laptops, tablets, smartphones Etc.).

The SafeDNS filtering system supports the most popular operating systems (Windows, Linux, Mac, iOS and Android).

Besides, it is suitable for protecting individual web-connected devices, entire networks of any size, and public Wi-Fi hotspots. It can also be used as an options on special Internet plans for children.

SafeDNS filtering solutions are highly scalable and have a redundancy option.



# Cloud Filtering Service

Need to improve network-wide protection against botnets, malicious, and phishing resources in an hour? Deploy the SafeDNS cloud filtering service!

You redirect user DNS requests to our filtering servers and define which categories of resources should be available to your subscribers. With 100% up-time during the last five years, our distributed network of servers located in Europe, Australia, the Americas, and the Far East, provides a fast response worldwide with no latency. Our servers process over 1 billion DNS queries monthly, therefore, preventing 9 million web attacks daily like malware and botnets.

## **With the SafeDNS cloud service, you can offer customers**

- Parental control service allowing parents to protect children against harmful content and spending too much time online
- Content filter for educational institutions and libraries
- WiFi protection necessary to prevent kids from visiting inappropriate resources from public WiFi networks
- Corporate filter enabling employers to manage, monitor, and control staff online activity
- Extra protection against phishing, malware and botnets

## **Benefits of the cloud service**

- Very easy to deploy and manage
- The fastest way to introduce network-wide protection against web threats
- Multiple opportunities to customize the service like SafeSearch for Google and Bing, YouTube Restricted Mode, etc.
- Apps to monetize products and services based on the SafeDNS filter and to brand them
- No added latency due to SafeDNS distributed network of filtering servers
- No hardware to buy, no software to maintain
- No CAPEX
- Little service overhead
- Can be integrated via special API with operator's systems like OSS/BSS and a self-care portal
- Can be whitelabeled and working under the operator's brand

# Parental Control Platform (ISP Go)

It is a sophisticated parental control service which can be managed by both internet service providers and their end-users. SafeDNS Parental Control Platform is a unique standalone solution installed inside the operator's network on a dedicated physical or virtual server.

This software solution, called SafeDNS ISP Go, is designed for web content filtering and is a DNS-based platform with a dynamically updated categorization database and an open API for integration with the operator's systems.

Parental Control Platform was designed with an open architecture in mind. ISP Go is totally brand free. After integration via a special API with operators' system like OSS/BSS and selfcare portal, the platform provides a parental control service under the operator's brand.

The software platform is intended to overcome NATed internet access limits, as it is deployed inside operators' networks to access internal IPs.

ISP Go uses the same technology and database as the SafeDNS cloud service. It guarantees high performance, stability, and filtering quality for SafeDNS customers.

## **The SafeDNS content filtering technology is adapted to specific needs of internet and mobile service providers allowing them to:**

- Provide a safer web connection free from botnets, phishing and malicious resources, including those from infected end-users' devices
- Provide a reliable and fast DNS resolving
- Provide an efficient parental control service
- Find an easy-to-deploy and cost-effective solution to expand the range of packages, products and services
- Introduce new products and services and brand them with the provider's own brand
- Avoid CAPEX and high TCO
- Get new customers and additional revenue
- Comply with regulation concerning blocking resources deemed illegal, harmful, and dangerous by the authorities



The modular architecture of the SafeDNS solution allows telecoms to select only needed features and implement the parental control service as:

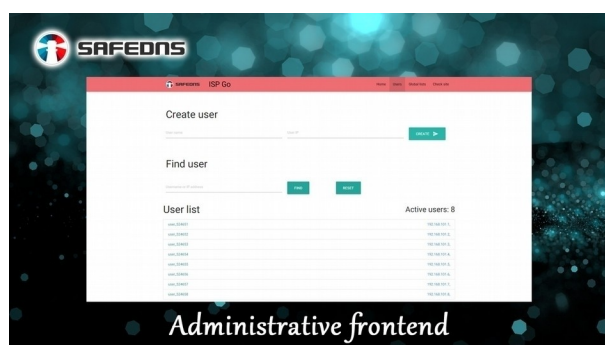
- A parental control service for residential users
- An internet filtering service for educational institutions and businesses

ISP Go Platform can be deployed fast

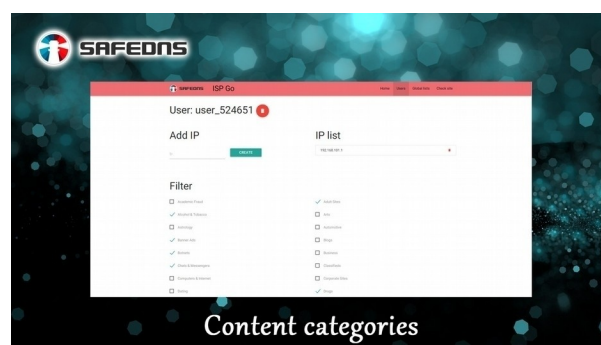
Straightforward integration of ISP Go with systems and websites of network operators allows them in a short time – from a couple of hours to 2 business days – to introduce options of content filtering and parental control service.

With API and a ready-to-use administrative frontend, ISP Go is easily managed – network operators can create and delete user accounts, configure the filtering, etc.

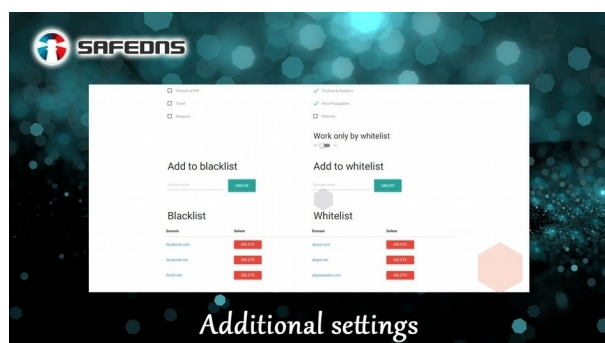
With the SafeDNS platform, network operators are free to decide whether to introduce fixed filtering rules for all end-users and groups or allow end-users to set individual filtering rules in a personal web-based dashboard.



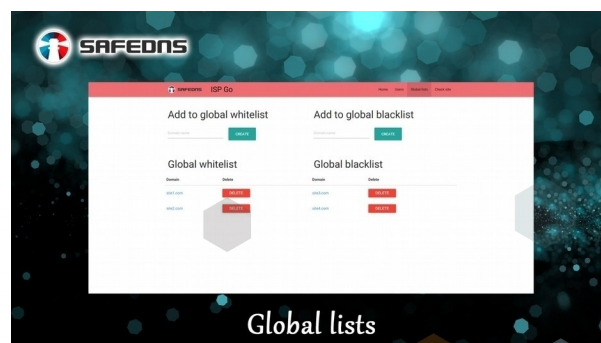
Administrative frontend



Content categories



Additional settings



Global lists



## **Platform's benefits you get**

- New sources of revenue as network operators set their price on services generated via the platform
- New users and increased customer loyalty. People would appreciate that their mobile and internet service providers care about online safety
- Simple implementation requiring no additional high-end equipment on operators' networks. No need for DPI systems to use SafeDNS
- Open API and a ready-to-use administrative frontend for managing the use of platform
- Seamless integration with network operators' OSS/BSS and self-care portal to provide customers with services under the operators' brands
- Multi-policy filtering for operators' users and groups of them
- Accommodation of any number of users due to platform's scalability
- Opportunity to brand the filtering services
- Fully customizable block page to show end users only the necessary information and contact details
- Regulation compliance. It is essential for network operators who are made responsible in many countries for blocking harmful online content
- No over-blocking issues as there are zero false positives
- Tailor the service to any individual needs by fine-tuning the filter. Just choose which of the 61 content categories to block or allow
- Powerful reports and stats of the filtering service available to operators and their customers. An opportunity for operators to use service statistics to create a more precise customer profile and identify any request to botnets and malicious resources from providers' networks
- Protection against botnets, phishing and malware for individual web-connected devices and entire networks of any size
- Enhanced filtering of adult and child sexual abuse images as SafeDNS is a Member of the Internet Watch Foundation (IWF), a leading organisation for reporting and removing online child sexual abuse images and videos.





## SafeDNS Licensing

Telecoms can choose whether to deliver web filtering services for free or for a fee and how much to charge for it. There are two types of SafeDNS licensing to choose from. One is a pay-as-you-grow model based on the number of active users of the filtering service. The other one is based on the overall amount of network operator's users – the more users it has, the less the operator pays for each one of them.

A revenue sharing model is also available. It allows any network operator to price their filtering products and services as they see fit, with revenues shared proportionately between SafeDNS and the network operator.

# Octopus for Telecoms

With our Modular Classification & Threat Intelligence Platform, SafeDNS provides big data analysis of DNS requests from operators' networks to identify malicious resources and infected end-user devices.

Based on machine learning and behavior analysis, our classification system, already deployed in the SafeDNS core service, is highly precise in:

Identifying malicious resources and infected user devices requesting those resources  
Creating a precise user advertising profile.

## Octopus makes it easy for you to

- Get web traffic categorized so that any URL reached is assigned to appropriate categories
- Increase network visibility and make sure your users comply with internet usage policies
- Detect cyber threats and reduce time to remediation
- Identify zero-day vulnerabilities and get protected against them
- Customize the platform to get the data you need

We welcome telecoms to our 'beta test Octopus' to reach their goals.



# Why SafeDNS

We provide cloud solutions for web content filtering and internet security focusing on the telecoms market and network equipment manufacturers. Our products and services are used by over 100 mobile and internet service providers to block and monitor access to the web and increase customers' safety online. The SafeDNS filtering solutions are integrated into networking hardware of vendors selling it internationally.

The SafeDNS highly scalable distributed network can accommodate many users and provides fast response worldwide with no latency. We process over a billion requests daily blocking access to 9 million queries to malware and botnets. We have a global coverage with SafeDNS filtering servers located throughout data centers in Europe, both Americas, and Asia, with 100% up-time during the last five years.

Our farm of web crawlers gathers considerable amount of data off the internet. That is why our internal database covers billions of URLs and over 109 million websites.

Since 2015, the efficiency of the SafeDNS web filtering system has been proved multiple Times by AV-Comparatives, a world leading test lab.

For five years straight, our filtering service is named Approved Parental Control Product. According to the latest test results, SafeDNS blocks adult content requests with near-perfect precision and zero false positives.

SafeDNS is Editor's Choice for Content Management & Filtering Solutions in 2016 Cyber Defense Magazine Infosec Awards. We create a next-generation innovation and advanced technology to protect users against web threats and make the internet cleaner and safer all our users.

This fact is recognized and emphasized with this award by the industry's leading electronic information security magazine. The award further validates our company as an innovator in online security and web content filtering.

SafeDNS is an Internet Watch Foundation Member, As a result, Child Abuse Image and content list (CAIC) informs the SafeDNS web Filtering system, since SafeDNS supports the IWF efforts to stop child abuse and exploitation online.



SafeDNS is also Friendly WiFi Partner, which means our content filtering solution are recommended for public WiFi owners and providers to ensure a safe web connection for their users.



### AV-Comparatives

For 5 years in a row, SafeDNS has been acknowledged as an Approved Parental Control Product by AV-Comparatives, a world-known Independent test lab. For the 2020 testing by AV-Comparatives, SafeDNS blocked 98,5% of adult content. It did not have false positives

### Cyber Defense Magazine

«We're thrilled to recognize next-generation innovation in the Information security marketplace, And that's why SafeDNS has earned This award from CDM.»

SafeDNS was founded in 2010 for develop internet security and web filtering solutions for the telecom market and end users. SafeDNS provides products and services for educational institutions, home and corporate users like network operators, MSPs and VARs. Now SafeDNS solutions are used by more than 4000 businesses and institutions and hundreds of thousands of home users worldwide.

## Contact us

[www.safedns.com](http://www.safedns.com)

[mail@safedns.com](mailto:mail@safedns.com)

+1-800-820-2530

+1-571-421-2990 (outside US)

901 North Pitt Street Suite #325

Alexandria VA 22314



**SAFEDNS**