DNS filtering Solutions

What is DNS filtering?

DNS filtering is the process of using the Domain Name System to block malicious websites and filter out harmful or inappropriate content. This ensures that company data remains secure and allows companies to have control over what their employees can access on company-managed networks. DNS filtering is often part of a larger access control strategy.

Before you delve into DNS filtering, let's understand the concept of Domain Name System (DNS) in the first place. DNS works as an internet phonebook. While visiting a website, you enter the site's domain name and access it easily. But, behind the scenes, a process is happening to make that access smooth for you. By entering a domain name, you are actually asking for the IP address of that particular site, for example, google.com. Next, the associated DNS server translates it into an IP address to take you to the site. Now, DNS filtering refers to the process of utilizing DNS to block harmful, inappropriate, and malicious websites. It ensures your network remains secure from cyber attacks while allowing you more control over your employees' internet accessibility to result in better productivity.

What is the Domain Name System (DNS)?

The Domain Name System, or DNS, matches domain names, like cloudflare.com, to IP addresses, like 192.0.1.20. DNS is necessary in order to allow users to access websites without memorizing confusing lists of numbers – just as a person is able to store their friends' phone numbers in their smartphone contacts list instead of memorizing every individual phone number.

Anytime a user opens up a website or accesses a web application, the process of loading the content only starts after the user's device has looked up the correct IP address. These are the steps of discovering an IP address so that a website can load:

- Once the user types a domain name into their browser, the user's device creates a DNS query and sends it to a specialized web server called a DNS resolver.
- The DNS resolver matches the queried domain name to an IP address either by querying additional DNS servers or by checking its cache.

- The DNS resolver sends a reply to the user's device with the correct IP address – this is called "resolving" the domain.
- The user's device contacts the server at that IP address to open a connection and begin loading the content.

DNS is an essential part of accessing web content – no content can load before the DNS process occurs. This makes DNS filtering an effective way to exert control over what content users can access.

How does it work?

If you have enabled DNS filtering on your network, both your incoming and outgoing web traffic is evaluated. As a result, only safe traffic is allowed to enter or leave your network. When you enter a site's domain, the enabled DNS filtering solution will filter the traffic between the IP address and the requested page. Next, the filtering process performs site categorization such as news, social media sites, inappropriate sites, illegal sites, malicious sites, phishing campaigns, etc. This way, the DNS filter inspects the incoming and outgoing traffic and blocks the suspicious or risky ones, based on certain set parameters while allowing only safe traffic. It can also protect your Wi-Fi from exploits apart from your internet network.

For example, if you have blocked your users from accessing facebook.com during work hours, and if they try to access the site, they cannot. It will show the permission is denied every time they do so during work hours.

How do DNS filtering services work?

All DNS queries go to a DNS resolver. Specially configured DNS resolvers can also act as filters by refusing to resolve queries for certain domains that are tracked in a blocklist, thus blocking users from reaching those domains. DNS filtering services can also use an allowlist instead of a blocklist. Suppose a company employee receives a phishing email and is tricked into clicking a link that leads to malicious-website.com. Before the employee's computer loads the website, it first sends a query to the company's DNS resolving service, which uses DNS filtering. If that malicious site is on that company's blocklist, the DNS resolver will block the request, preventing malicious-website.com from loading and thwarting the phishing attack.

DNS filtering can blocklist web properties either by domain name or by IP address:

By domain: The DNS resolver does not resolve, or look up, the IP addresses for certain domains at all.
By IP address: The DNS resolver attempts to resolve all domains, but if the IP address is on the blocklist, the resolver will not send it back to the requesting device.

What is a blocklist?

In the context of DNS filtering, a blocklist is a list of known harmful domains or IP addresses. DNS filtering vendors may rely upon blocklists that are shared within the cyber security community, generate their own blocklists, or do both. Some DNS filters will even evaluate webpages and add them to a blocklist automatically. For instance, if malicious JavaScript code is observed to run on example.com, example.com will be added to the blocklist. DNS filtering may also blocklist domains that are not necessarily used for malware or phishing attacks, but that host forbidden or inappropriate content. For instance, a company may wish to add websites that host adult content to their DNS filtering blocklist. The reverse of a blocklist, an allow list is a list of allowed domains or IP addresses. All domains or IP addresses that are not on the allow list are blocked.

How does DNS filtering help block malware and phishing attacks?

DNS filtering can help keep malware, or malicious software, out of company networks and off of user devices. It can also help block some kinds of phishing attacks.

1. Blocking malicious websites

A website that hosts malware can either attempt to trick users into downloading a malicious program, or execute a drive-by download: a download of a malicious piece of software that is automatically triggered when the webpage loads. A number of other attacks are possible as well. For instance, webpages run JavaScript code, and as a full programming language, JavaScript can be used in a range of ways to compromise user devices. DNS filtering can prevent these kinds of attacks by blocking users from loading malicious webpages at all.

2. Blocking phishing websites

A phishing website is a fake website that is set up to steal login credentials in phishing attacks. The domain used could be a spoofed domain or just an official-looking domain that most users will not think to question. Regardless of the method, the goal is to fool the user into giving their account credentials to an attacker. These websites can be blocked using DNS filtering. These capabilities are dependent upon the DNS filtering system knowing to identify the malicious IP addresses or domains as bad. While DNS filtering can block this malicious activity, attackers generate new domains very quickly and it is not possible to blocklist all of them.

How does DNS filtering block prohibited content?

The process for restricting access to certain kinds of content is similar to the process described above; IP addresses or domain names that are known to host prohibited content are blocklisted, and users

cannot access them. Alternatively, company-approved websites can be added to an allow list, with DNS filtering blocking all other websites.

What are secure DNS servers?

A secure DNS server is a DNS resolver that blocks malicious or prohibited websites as part of a DNS filtering service. Some secure DNS servers also offer increased privacy to protect user data; Cloudflare, for example, offers a DNS resolving service called 1.1.1.1 that purges all DNS query logs after 24 hours.
Along with DNS filtering, there are additional ways of making the DNS process more secure, since DNS was not designed with security in mind. The DNSSEC protocol helps verify that DNS resolvers provide accurate information and have not been compromised by an attacker. The DNS over TLS (DoT) and DNS over HTTPS (DoH) protocols encrypt DNS queries and responses so that attackers cannot stalk a user's DNS queries and track the websites they visit.

DNS Filtering Service

A DNS filtering service is an alternative to traditional hardware and software-based web filtering solutions and is used to filter out harmful and malicious internet content. A DNS filter works by redirecting the IP address of an organization´s router to that of the service provider and then allowing administrators to set filtering parameters via an online browser-based portal. Because a DNS web filtering service is quick to implement, has low maintenance overheads, and is inexpensive to operate, it is quickly becoming the "go-to" solution for organizations wanting to increase their online security posture and protect their networks from web-based threats. A DNS filtering service has other benefits for organizations. It can be used to improve productivity by blocking access to social media networks and gaming websites and is important for compliance, managing legal risk, and controlling bandwidth use.

The Importance of a DNS Filtering Service with SSL Inspection

SSL inspection is a tool within a DNS filtering service that decrypts the content of a "secure" website, checks the content to make sure it does not violate internet access policies, and then re-encrypts the website before allowing an Internet user access to the site. The reason why SSL inspection is so important is because three-quarters of websites – including websites with SSL certificates – have been identified as having security vulnerabilities. That does not mean that three-quarters of websites harbor malware, but the potential exists for a hacker to exploit a vulnerability and install malware or phishing forms on the website. Without SSL inspection, an Internet user – even one trained on the dangers of web-based threats – could inadvertently download malware onto their device from an apparently "safe" website, and then infect the whole of an organization´s network.

DNS Filtering Service

A DNS filtering service is an alternative to traditional hardware and software-based web filtering solutions and is used to filter out harmful and malicious internet content. A DNS filter works by redirecting the IP address of an organization´s router to that of the service provider and then allowing administrators to set filtering parameters via an online browser-based portal. Because a DNS web filtering service is quick to implement, has low maintenance overheads, and is inexpensive to operate, it is quickly becoming the "go-to" solution for organizations wanting to increase their online security posture and protect their networks from web-based threats. A DNS filtering service has other benefits for organizations. It can be used to improve productivity by blocking access to social media networks and gaming websites and is important for compliance, managing legal risk, and controlling bandwidth use.

The Importance of a DNS Filtering Service with SSL Inspection

SSL inspection is a tool within a DNS filtering service that decrypts the content of a "secure" website, checks the content to make sure it does not violate internet access policies, and then re-encrypts the website before allowing an Internet user access to the site. The reason why SSL inspection is so important is because three-quarters of websites – including websites with SSL certificates – have been identified as having security vulnerabilities. That does not mean that three-quarters of websites harbor malware, but the potential exists for a hacker to exploit a vulnerability and install malware or phishing forms on the website. Without SSL inspection, an Internet user – even one trained on the dangers of web-based threats – could inadvertently download malware onto their device from an apparently "safe" website, and then infect the whole of an organization´s network.

Other Benefits of a DNS Filter Service

In addition to protecting an organization´s network against the risk of web-based threats, a DNS filter can be used to restrict access to productivity-sapping websites that employees may utilize for "cyberslacking". Studies have shown that the average employee wastes around two hours each day on gaming websites, online shopping portals, social media platforms, and – significantly – pornographic content.

It has been suggested some personal web time at work can promote productivity; however, openly viewing pornographic and other objectionable content can cause HR issues. An organization could even be taken to court by an employee for failing to provide a safe working environment. A DNS web filtering service can prevent these problems by restricting access to these NSFW websites. Controls can be applied for individual users, groups, departments, or organization-wide. It is also possible to apply time-based controls. For example, social media sites could be blocked during working hours, with access allowed during lunch breaks.

The time-based controls on a DNS filtering service are particularly useful if your organization regularly has bandwidth issues. By setting the filtering parameters to block access to video streaming websites and online bandwidth-hogging applications, organizations can prevent bandwidth wastage at key times during the working day.

Finally, for organizations in the retail industry, a DNS filter enables you to offer a protected WiFi service to your customers. Free WiFi services are a great marketing tool in an age when consumer decisions are influenced by where they can access the internet free of charge. However, if customers´ devices are infected by malware – or if customers are exposed to objectionable content due to an organization offering an unprotected WiFi service – the organization will likely lose more customers than it gains. By using DNS-based web filtering, businesses can ensure that all WiFi users – employees, guest users, and customers – are protected from online threats and are not permitted to use a WiFi network for accessing harmful or unsavory web content.

Features DNS Web Filtering Service

The primary features and benefits of TitanHQ´s DNS web filtering service – Cloud – are worth highlighting because many organizations evaluate web filtering solutions based on cost and maintenance overheads – rather than how effective the solutions are.

Filtering Mechanisms

Cloud has a three-tier mechanism for filtering the Internet: Blacklists, category filters, and keyword filters. Blacklists blanket-block access to websites known to harbor malware and websites that disguise their true identity behind a proxy server. Category and keyword filters restrict user access to websites that fall within a certain category and will block access to sites that contain certain keywords. Organizations have the option to apply whichever category and keyword filters they wish and – with Cloud – have the opportunity to create their own customized categories. The three-tier mechanism delivers an exceptional level of granularity allowing organizations to fine-tune the content employees and visitors to their business can access.

Malicious URL Detection and Phishing Protection

Our malicious URL detection software checks each request to visit a website against a blacklist of IP addresses from which spam emails are known to have originated and blocks access to those sites. Websites that have been discovered to have been used for phishing or have been detected as hosting exploit kits or malware are similarly blocked. IP address blacklists are updated in real-time as new threats are identified.
Similarly, our phishing protection software is updated in real-time as new websites are discovered to be used for phishing. 99.5% of websites with the word “PayPal” in their URL are fake sites and, due to the sophistication with which cybercriminals are constructing their phishing emails and their fake websites,

phishing attacks are getting harder to identify and block. A DNS filter provides an important extra layer of security to block the web-based component of phishing attacks.

Parameter Settings

As mentioned at the top of this page, Cloud´s filtering parameters can be set and adjusted via an online portal that can be accessed through any web browser. This makes it possible to fine-tune the DNS filtering service from any Internet-enabled device and eliminates the necessity for organizations with multiple offices to visit each location every time there is a change to their acceptable internet use policy.
The Cloud DNS filter has the all-important SSL inspection that was discussed earlier, plus accommodates multi-lingual filtering. The flexibility of our DNS web filtering service allows the blocking of web applications, without blocking access to the website itself (useful for organizations that engage in Facebook marketing but do not want their employees to be able to use Facebook Messenger).

Compatibility and Scalability

As Cloud is a DNS filtering service that works by redirecting a router´s DNS, there are no compatibility issues. If you want to integrate Cloud with existing management tools our DNS web filtering service is provided with a suite of APIs for backend integration. MSPs can easily integrate the solution into their auto-provisioning and management systems. Scalability is not an issue either. There is no upper limit to the number of devices that can be protected by our DNS filtering service. Consequently, Cloud will always be an appropriate web filtering solution should your organization expand. If you n eed to reduce your workforce, this can easily be accommodated by TitanHQ to ensure you do not pay for a subscription you are not using. Details of how this works are provided in the “DNS Filtering Service Pricing” section below.

Imperceptible Latency

Due to the SSL inspection process being performed in the cloud, Cloud filters the Internet with imperceptible latency. This means that, irrespective of how many devices are using the DNS filter, any delay between typing in a URL or clicking on a hyperlink and having a permissible website opened in the browser is unnoticeable. There are no bandwidth restrictions on our DNS web filtering service; so, if you decide not to block video streaming websites, Cloud can cope with the volume of Internet traffic. This can be of particular importance to organizations that operate a WiFi service with multiple hotspots or for an organization with multiple Internet users that are visiting streaming websites.

Automated Reporting

There are a number of good reasons for taking advantage of Cloud´s automated reporting. Firstly, the reports inform administrators of any web-based threats that have been blocked and where they originated from. This information can help shape future acceptable use policies or be used to nip potential HR issues in the bud before they develop into more serious problems. The reports also advise administrators of any attempts to circumnavigate the filtering parameters.

DNS Filtering Solutions

1. **Sophos**
2. **CleanBrowsing**
3. **ESET Parental Control**
4. **Perimeter 81**
5. **Open DNS**
6. **Cloudflare Gateway**
7. **DNSFilter**
8. **SafeDNS**
9. **Webroot**
10. **DNSCyte**
11. **Cisco Umbrella**
12. **CIRA DNS Firewall**
13. **MXToolbox**
14. **ScoutDNS**
15. **NordLayer**
16. **Heimdal**
17. **Mimecast Web Security**
18. **Barracuda Content Shield**
19. **Avast Secure Web Gateway**

Sophos

Praised by companies like IGN and Mac World, Sophos Home is an excellent DNS filter that comes with artificial intelligence blocking viruses, malware, and other harmful threats with ease. It is available for both Mac and PC and offers a wide range of protection including:

- Parental control
- Banking security
- Identity protection
- Browsing protection
- Privacy protection
- Malware protection
- Real-time antivirus

It is made to keep up with the real-time threats that occur on a day-to-day basis via your browsing habits.

CleanBrowsing

Allowing you to browse the internet without any "surprises,"CleanBrowsing is one great DNS-based filtering tool that will keep your kids and the entire family free from malicious attacks. Since it is DNS-based, you won't need to download any additional software to use it. All you do is change the DNS from your internet service provider. It's that simple.

The free plan itself offers some great features like:

- Security filter that blocks phishing, ransomware, and malicious sources
- Blocks inappropriate adult content
- Specially designed family filter for proper usage as per age groups

If you'd like to access more advanced features, you can sign up for one of their paid plans, starting at less than one Starbucks coffee cost per month.

ESET Parental Control

Another very impressive DNS-filtering service, ESET Parental Control, works seamlessly on desktop and mobile devices. In a nutshell, here's what this service does:

- Blocks inappropriate adult content
- Limits screen time
- Prevents downloading suspicious software
- Tracks browsing behavior
- Tracks your child's phone location

With all these impressive features, you get a 30-day free trial as well

Perimeter 81

One of the best DNS Filtering services is Perimeter 81. It blocks access to malicious sites and prevents phishing attacks. The most powerful feature of the tool is the dynamic category-based filtering which lets IT restrict or completely block out harmful sites such as gambling, social media, malware, and adult content. Users will receive alerts letting them know that the content they attempted to access has been blocked. You also have total control over what sites employees are able to access for safer browsing across your network and you can increase your employees' productivity by restricting access to time-wasting sites such as social media.

Perimeter 81's DNS Filtering tool is compatible with Windows, Mac, and Linux.

Open DNS

You can safeguard your business network by using Open DNS, which includes filtering which safeguards your network from malicious websites and adult content. According to research one in every three public grade schools in the US is using OpenDNS. It also delivers a faster Internet; any device

connected with Open DNS will be protected from various threats. Open DNS network process estimates around 100 billion DNS queries daily from 85 million users through 25 data centers worldwide.

Cloudflare Gateway

It makes slowdown down your site via centralizing the firewall and controlling traffic. This is one type of advanced technology which provides comprehensive security with the best performance. You get the threats like phishing campaigns and crypto-mining. Through SSL inspection, you can control. You can also stop downloading other harmful files. Any threat which can come from the site, you can easily block that. This gateway also shows you unapproved SaaS application usage. It offers a wider sneak peek at web traffic, and it can be used in any location.

DNSFilter

It has the capacity to safeguard your employee from malware and phishing threats. This detects the threat and kills them and provides the enterprise-level filter and protection. This is the cloud-based DNS filter that protects your business and prevents intrusion. It provides an international network that gives you the best scale and durability. It helps K-12 and university networks so that it can comply with CIPA. They can control at a time 30 data canter from the various part of the globe. As soon as you enter the data, it gets started within a minute. You can block anything through this, like instant messaging, social sites, adult content, etc. For any reported problem, it gives an immediate troubleshoot solution.

SafeDNS

This is another good option that makes your security strong. It also protects your internal network by controlling your Wi-Fi hotspots and give you safe online browsing. It also protects in large public events, and it makes sure that nothing could break due to heavy traffic. It categorized the database and gave you a cloud-based filtering service. This system is automatic, which detects botnets and malware quickly. It automatically blocks adult content and also other harmful content. It maintains BGP protocol, and this server provides faster access to everything.

Webroot

If you get complete visibility and safeguard your DNS network, then Webroot is best. It enforces the internet so that it can reduce security risks. This full cloud base service takes few minutes to deploy. You may get many threats in your business that you can solve by configuring some policies like IP address, device, and group. It automatically controls the dangerous site. It consists of DoH and IPv6, which help to prepare the next-gen internet and protocols. You can safeguard your security, admin control, privacy, visibility, etc. this network is spread to more than 16 global locations.

Dnscyte

It is CyberCyte cloud-based security that has leveraged machine learning capacity which blocks online threats immediately. It can protect huge databases with intelligence so that it can work against any malicious activities. It does not allow you to reach any harmful request to the IP address and protects you from pre and post-infection. It also provides tight security to your ports and protocols. DNS server is so vital for the corporate network that it receives queries before local DNS. After doing the complete analysis, it sends to the local DNS. It handles the categorization and identification of the traffic.

Cisco Umbrella

This tool helps you to manage internet access, and it also keeps your organization safe by controlling DNS filtering, request, blocks, SafeSearch browsing, etc. It can control 80+ categories, and it provides you complete control where you can select the mode like high, low, and moderate settings. You can also customize your list based on the requirements. It also allows bulk uploads and unlimited entries so that easy admission can be made. You can also filter YouTube, Bing, Google, but you need to make sure that users can access productive information only.

CIRA DNS Firewall

This is the Canadian Cybersecurity system that delivers protection against malware. It also blocks the access of malicious websites through the DNS layer. It combines advanced data science which proves a global network that threat detection and manages critical infrastructure to deliver a cost-effective result. It also provides multiple additional feeds, which show you in-depth if you have a threat. On average, it blocks 100,000 net new malicious URLs every day. It can control everything, and within 14 minutes, it can detect the threat.

MxToolBox

This is one of the best leading tools for email delivery. It has over the decade's experience to deliver the email whether it is a small or big company. This works as a delivery center that gives a comprehensive service where it understands the email and 'From' your domain. It also searches the sender's Ips and Geolocation of the sender. If it feels that it is fake, it blacklist the sender and it also provides few verification like SPF, DKIM and DMARC. This will maintain your email by increasing the deliverability and monitor those so that you will have control over the mail.

ScoutDNS

This is a cloud-based content filtering option where it protects your database from malware. It mainly operates through DNS Layer. This is a very powerful domain which content data feeds and DNS layer insights. It understands the network administrator so that it can protect its network in an innovative

way. ScoutDNS is so much powerful that it identify the threats and protect your system from DNS layer threats.

NordLayer

Nordlayer offers you a highly sophisticated DNS filtering service. You can use this solution to block harmful and phishing websites and thus protect your business environment and teammates against online threats. Whether you need to filter web access for your SMB or deploy device-level DNS protection for thousands of enterprise employees, you can choose this application without worry.

Heimdal

Heimdal Threat Prevention – Endpoint is a DNS filtering solution that prevents access to malicious domains and webpages. Its DNS filtering component checks each request that is made on an endpoint, protecting enterprises against malicious websites that can potentially infect systems with malware. By maintaining an ever-evolving blacklist of malicious domains, Threat Prevention – Endpoint knows which websites to block almost instinctively. Empowered with proprietary AI-based traffic pattern recognition technology, the solution is constantly learning everything there is to know about the darkest corners of the digital world. Using machine-learning algorithms that were specifically designed for threat hunting, Heimdal's threat prevention solution enhances its traffic-filtering capabilities by also predicting on top of pursuing. This neural AI feature combined with up-to-date intel, is what allows the tool to protect systems against APTs. Constantly identifying new TTPs (tactics, techniques, and procedures) allows Threat Prevention – Endpoint to nip infiltration attempts in the bud.

- Heimdal Threat Prevention – Endpoint uses machine learning, adding Host Intrusion Prevention and Detection capabilities to your digital defenses (HIPS) and (HIDS). It is fully customizable, allowing system administrators to block selected pages and create special allow and block lists, as well as block content based on Web-Categories such as Advertising, Social, Adult etc.
- Heimdal Threat Prevention – Endpoint is a strong DNS security tool that provides extensive filtering options with artificial intelligence for around-the-clock protection.

Mimecast Web Security

Mimecast Web Security provides a comprehensive, cloud-based web security platform. It adds monitoring and security at the DNS layer, to protect users against malicious web activity and malware. With Mimecast, admins can also ensure compliance with acceptable use policies, stopping users from accessing harmful web pages. Mimecast stops users from being able to access malicious or harmful websites, by inspecting all web traffic in real time. Admins are also able to select policies which control what categories of web pages users are able to visit to enforce acceptable use policies. This helps to protect your organization from web based cyber-attacks, include credential phishing pages. Mimecast provides fast

implementation, with web security able to be installed organization wide in less than an hour. Mimecast has advanced cyber threat intelligence, which means they can offer a high standard of threat protection. Their multi-tenant. Cloud infrastructure provides visibility across tens of thousands of customers globally, meaning they have strong intelligence into emerging threats. Mimecast's Web Security works well with their email security solution, working across one single, easy to manage platform.

Barracuda Content Shield

Barracuda Content Shield is a cloud based web security platform that provides content filtering, file-based protection, policy enforcement and reporting. Content Shield provides DNS filtering and URL reporting to protect users from malicious web content. It uses agent-based filtering to ensure that remote users are fully protected, even when they are off the network. Content Shield provides real-time protection against online threats, powered by Barracuda's threat intelligence network. It protects users against downloaded files, endpoint files, and malicious web content. Content Shield also provides businesses with visibility at a per user level at activities, and gives admins customizable alerts when malicious activity is detected. One of the main benefits of the Barracuda platform is its ease of set up and deployment. Users say that the platform is easy to use, with strong visibility into web based threats.

Avast Secure Web Gateway

The Avast Secure Web Gateway is a cloud-based web security platform that protects users from web threats before they can enter your network. It allows organizations to secure their network traffic in the cloud, with one easy to use platform. The Avast threat detection network draws from 21 different threat feeds to protect users from threats in real time. The platform has a focus on ease of use and deployment, able to be set up in three easy steps. Avast's Secure Web Gateway blocks malicious downloads and known malicious URLs from entering your network, using their intelligent proxy to classify sites as safe or unsafe. Admins are also able to modify sizes of pre-configured block/allow lists and set content filtering rules to ensure safe practices are followed at work. Avast has a strong threat intelligence network, with valuable data from the millions of devices using Avast's endpoint security solutions. Avast is designed for use by small security teams and organizations, so it has a focus on ease of deployment and use. The gateway can be deployed within minutes, with a range of security services that are all managed through one admin console.

Net Nanny

Another DNS service that uses artificial intelligence to block malicious sources online with ease. As per Tom's Guide, Net Nanny has been listed number 1 among other parental control apps. That itself tells you how good of a service this is.

It offers a ton of great features including:

- Ability to monitor your child's browsing habits
- Limit kids' screen time with a finger touch

- Blocks suspicious websites
- Manage what kids can browse on the internet
- Blocks adult content
- Ability to disallow specific URLs

You can use Net Nanny on Mac OS, Android, IOS, and Kindle. It has different plans for different devices,

Circle

A phenomenal device that comes with an interactive app, Circle has got to be one of the best options in this list. It is praised by brands like Forbes, TechCrunch, and USA Today. It provides a variety of protection to your kids' browsing habits such as:

- Setting limitations on using their phone
- Review what your child has been browsing throughout the day
- Ability to turn the internet off during bedtime or when studying
- Ability to reward your kids with additional screen time whenever needed
- Pause/resume internet whenever you like

I believe the biggest selling point of this service is the app that comes along with it. It is super fun and intuitive that you'll want to keep using it. The app works on both IOS and Android. Unlike some of the other DNS filters in this list.

Benefits of using DNS filtering

There are a ton of benefits behind using DNS filtering for you and your family. You've probably got a taste of it already by now but here are some more you need to know:

Ensures safe Internet browsing

Using DNS filtering means putting a roadblock to malicious websites that can potentially steal your personal information. Some other threats include:

- Ransomware
- Phishing
- Spyware
- Virus
- Malware

You can avoid all the above risks by just applying the DNS filter.

Protects your data

We all have important data on our devices, and most of the time, we're ignorant when it comes to backing it up. If that is the case with you, you're at risk of losing all of it if you visit dangerous online sources. Thankfully, the following software takes care of that for you.

Protects your device

No matter if you're browsing from your phone, tablet, or computer, visiting malicious websites will potentially harm your device. Some websites can install viruses on your device remotely, which can spoil the functionalities and make it partially useless.

Conclusion

I hope the above DNS filtering tools help you avoid becoming a victim of cyber threats again. Along with filtering tools, you may also want to use VPN services to protect your identity.