Threat Protection

What kind of threats does N-able DNS Filtering protect my customers against?

The cybersecurity landscape is always evolving, with new threat vectors and sophisticated scams emerging every year. The one thing they all have in common is where they originate—online. DNS protection is the only security layer designed to shield your company from all threats that originate online via scanning, categorizing, and blocking hacked websites. Having a proactive risk mitigation plan starts with an aggressive web protection strategy.

Q. What is the value of DNS Filtering from a security standpoint?

DNS is the first line of defense in protecting your business. We block threats before your employees gain access to them. We are an extremely effective security solution for preventing requests to malicious domains, illegal activity, and phishing. We have a constant stream of security feeds that allow us to respond instantly to internet threats. Because our servers receive federated updates within a second, any updates will immediately protect all our customers. There are no software or definition files to install.

Q. How can I prevent phishing attacks?

Phishing and spear phishing attacks are a favorite among hackers because they are relatively easy to implement. They use email or chat (such as public Slack® channels or Discord) to lure victims into a scam or, more commonly, to a link where they will enter data or download malware. Phishing attacks can be broad and general, impersonating institutions like banks or hospitals, or they can be targeted and sophisticated, often impersonating employees inside your own organization. Because N-ableTM DNS Filtering is constantly scanning the web for new malicious sites, we can prevent phishing attacks by stopping your employees before they hit a malicious site or give a phisher their data. Our solution also uses domain greylisting, which blocks newly registered domains for 30 days. This is invaluable, as a majority of phishing sites are brand new.

Q. How do I protect my customers against ransomware?

Ransomware is software that allows hackers to encrypt files, networks, and computers remotely. They then hold your data hostage until your company pays a ransom. With the evolution of ransomware in key sectors, like healthcare, as well as the ubiquity that ransomware as a service offers, this threat technique has become one of the top causes of cybersecurity incidents worldwide. In 2020, the average ransomware demand was $233,000, and they now make up around one third of all security breaches*. The key to ransomware protection is stopping the malware from being downloaded in the first place, which usually requires blocking the site that hosts the malicious content before an unsuspecting user can visit it and become infected.

*"Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues," Coveware. https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (Accessed September 2021).

Q. How can I secure my users against cryptojacking?

A true twenty-first century threat, cryptojacking is the unauthorized takeover of a computer or network to "mine" cryptocurrency. Because new currency is created by computers using massive amounts of computing resources, computational bandwidth is at a premium. Cryptojacking infects a distributed network of computers to utilize their computational bandwidth, slowing down the device and, at scale, driving up your energy costs. DNS Filtering has a robust catalog of known cryptojacking sites, and domains that contain cryptocurrency references can be blocked with a single click.

Q. How do I prevent typosquatting?

Thousands of people type Amazan.com® into their browser every day. Turns out, the average internet user isn't always the best speller. Bad actors take advantage of this by setting up malicious sites with domain names that feature common misspellings of familiar sites. Every day, we seem to discover new "chase" login pages with an increasingly creative variety of typos (check out the fake sites here). DNS Filtering protects the user from typosquatting by blocking access to domains that are known to contain malware or malicious content. Never worry about misspelled domain names again.

Q. How can I block torrents?

We categorize torrent tracking sites under "P2P & Illegal" content. We can prevent users from getting to these sites and getting the seed files necessary to torrent. We have an article on blocking torrents.

Q. How can I block TOR and .onion sites?

We categorize TOR and .onion sites on the clear web under "P2P & Illegal" content. We can prevent users from getting to these sites and getting to the download pages of these sites, but if someone already has the TOR browser installed on a device, they can bring it onto the network. There are ways to block TOR traffic through firewalls, and we recommend looking at the manufacturer's documentation on how to achieve this.

Because we operate on DNS traffic, we don't stop torrent traffic. However, we categorize torrent tracking sites under "P2P & Illegal" content. We can prevent users from getting to these sites and getting the seed files necessary to torrent. We have an article on blocking torrents.

Q. How can I tell which users are accessing which websites?

The users feature will allow administrators to apply specific policies, schedules, and block pages to an organization's users on a granular level. Reports and query logs can also be filtered on a per-user basis, to enable more detailed reporting and troubleshooting.

You may also decide to utilize our roaming clients, which are available for many different operating systems and device types. With the roaming client, you can have granular control and visibility over each computer. Often computers are assigned to a specific person within the organization, which allows you to easily associate data from the reports to a user

Q. Is my information safe on your network?

The nature of our service is akin to a constantly changing phonebook. We match internet names to IP addresses, and where those names are a security threat or are blocked by your policy, we don't allow a connection. However, once the connection is made, we have no further part. So the information you are transferring never touches our servers. We perform the translating.