RoundClock DNS Filter
Powered by Cisco Umbrella

mother
technologies

By stopping attacks at DNS level before they have a chance to cause harm, organisations can reduce cyber attack costs by up to 50%.

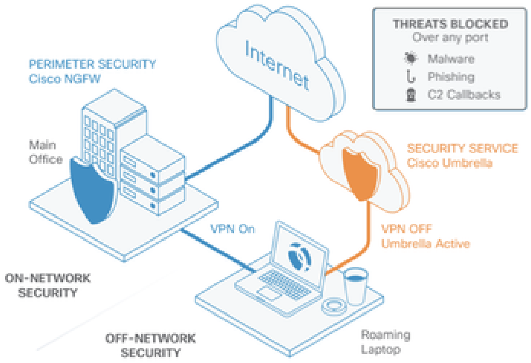
Securing internet access has never been more critical. With users connecting from various locations and devices and relying on the internet to perform their tasks, it is essential to protect against phishing, malware, and compromised accounts, no matter where your users are working. Our DNS solution can assist you with this.

RoundClock DNS Filter offers a robust first line of defence against online threats, providing visibility into all internet access being used within your environment and the capability to block anything that poses a threat.

What is DNS?

DNS Filtering is the process of using the 'Domain Name System' to block malicious websites and filter out harmful or inappropriate content.

When you try to visit a website, like mothertech.co.uk, your request first goes to a DNS resolver. The DNS resolver's job is to find the actual IP address of the website. Once it finds this IP address, it sends it back to your computer, which then connects to the website, allowing you to see its content.



With a DNS Filter in place, the process includes an extra security step. When you request a website, the DNS resolver checks if the site is safe. If the website is safe, the DNS resolver returns the IP address to your computer, and you can access the website as usual. However, if the website is not safe, the DNS resolver does not return the IP address of the website. Instead, it sends back a different address that shows a message saying access to the site is denied.

Key Features

Endpoint Coverage
Protects Windows, Macs, Chromebooks, and Apple smart devices.

On-Net and Off-Net Protection
Safeguards endpoints irrespective of location (Directly connected or roaming outside of the corporate network).

Comprehensive Web Security
Ensures safe and secure internet access by blocking domains associated with phishing attacks, malware, ransomware, botnets, and other high-risk or inappropriate categories before they reach the network.

Shadow IT Detection
Identifies and blocks unauthorised cloud applications.

Proxy and Deep Inspection
Enables deep inspection of risky domains, providing comprehensive protection against emerging threats.

Granular Policy Control
Allows tailored protection with granular policies for individuals or groups.

Why RoundClock DNS?

Our DNS Solution is powered by Cisco Umbrella, the worlds #1 DNS Filtering Engine. It protects more than 100 million users across 190+ countries.

Threat Intelligence
Every day, Cisco Umbrella handles more than 620 billion DNS queries, processing a large amount of data for threat intelligence.

No slow internet Speeds
For some solutions, increased security means slower internet access. However, with RoundClock, DNS requests are completed in milliseconds, resulting in minimal impact on internet performance.

Malicious Domain Detection
More than 7 million malicious domains and IPs are detected and blocked daily.

Easy to Deploy
As a cloud based solution, Cisco Umbrella can be deployed across an organisation within an average of 30 minutes.