c3group

# C3 WebSecurity

Protection even before an attack strikes.

## ANYWHERE, ANY DEVICE SECURITY

THREAT PROTECTION | MAINTANANCE FREE | HIGH PERFORMANCE

C3 WebSecurity is Cloud based security, delivering protection to any device, anywhere you use it. Whether you're working inside the office, at home, or away on business - you can have full peace-of-mind that you can browse the Internet safely, wherever you are. Many modern day cyber attacks are remotely executed viruses from websites (Domains). Cybercriminals use different ways to lure users to these domains, including through links in emails and website pop ups. Once the user reaches these pages, the embedded virus is deployed into their network - this leaves critical business data extremely vulnerable.

The way in which C3 WebSecurity works, is by scanning every Domain name before it is converted into an IP address. By enforcing security at the network level, we can prevent command and control call-backs, disabling virus attempts that aim to compromise your systems. These attempted attacks can include the likes of malware and phishing - both of which can have catastrophic impacts. One of the greatest things about C3 WebSecurity, is that it protects devices anywhere they're being used, and stays up-to-date without admin intervention, because there is no hardware to install or software to maintain. You can simply go about your day-to-day activities, without having to worry about your network safety.

C3 WebSecurity

## Why C3 WebSecurity?

✓ THREAT PROTECTION LIKE NO OTHER:
C3 WebSecurity enforces security at the DNS and IP layers to prevent malicious activities coming into your network and destroying your critical business data.

✓ ZERO MAINTANANCE:
There is no hardware to install, or software to maintain with C3 WebSecurity. Your network protection remains up-to-date without the need for admin intervention, thanks to advanced cloud-based technology.

✓ QUALITY PERFORMANCE AND RELIABILITY:
With a history of 100% up time, C3 WebSecurity has no added latency, as there is no need to reroute every connection through any gateways - meaning your usability is not affected in anyway, while receiving superior network protection.

## How it works:

1. CYBERCRIMINALS CREATE A NEW WEBPAGE THAT CONTAINS A VIRUS

2. C3 WEBSECURITY SEE'S A MASS AMOUNT OF TRAFFIC BEING DIRECTED TO THIS NEW PAGE

3. ANALYSIS TAKES PLACE TO DETERMINE WHETHER THE NEW SITE IS SAFE FOR OUR CLIENTS TO ACCESS

4. IF IT IS DETERMINED THAT THE SITE IS CARRYING A VIRUS, IT IS BLACKLISTED & NO LONGER ACCESSIBLE