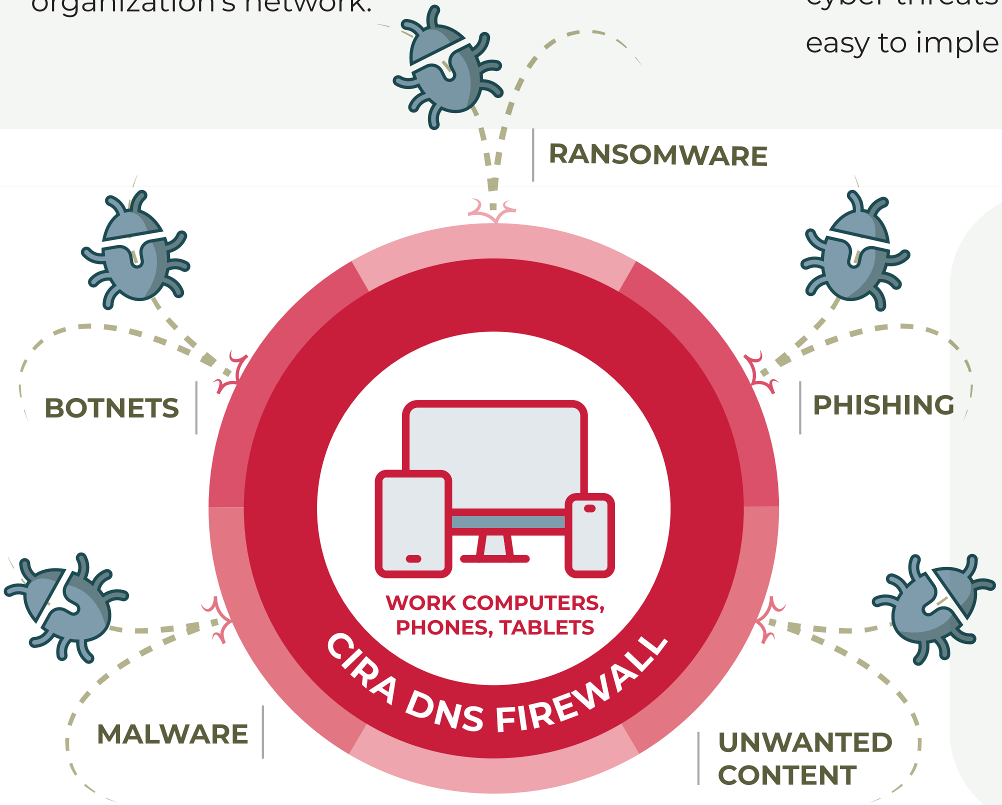
CIRA DNS Firewall

Protect your organization from malware and phishing threats no matter where users choose to work and learn

CIRA DNS Firewall puts you in control of your organization's cybersecurity by giving you the power to block malicious cybersecurity attacks from reaching your organization's network.

The service's powerful threat feeds block cyber threats like malware, phishing and botnets as they arise, while its customizability allows organizations to add specific sites they don't want users visiting.

The made-in-Canada solution protects more than 2.5 million Canadians from malicious cyber threats and is both simple to use and easy to implement.



> "Being able to quickly block new spear phishing threats using CIRA's DNS Firewall has reduced our impacted user rate by 80 - 90 per cent"
>
> TRENT UNIVERSITY

Top three reasons to use

- Effective cybersecurity that is transparent to end users, regardless of whether they are working in the office or not.
- Set up in minutes across a variety of devices with simple management.
- Block threats that other solutions miss, allowing for seamless integration and co-existence with other network-based security tools

Canadian cybersecurity

- Canadian infrastructure that is faster for your users
- Canadian data sovereignty and privacy-first operations policy
- Includes threat feeds from the Canadian Center for Cybersecurity and the Canadian Center for Child Protection.

Off-Network **Protection capabilities**

With remote work becoming more popular, employees are accessing company resources and data on public and home networks. CIRA's DNS Firewall Client is an application which enables DNS privacy, security and content filtering for roaming users.

Cloud-based endpoint protection works with on device applications (Client) that keep devices protected while on and off the VPN, without impacting device performance or requiring specialized hardware.

Benefits include:

- Full deployment in minutes
- Support for remote workers
- Manage users and groups
- Network management & policy management
- Block and traffic reporting
- Supports a full suite of systems and devices

Protection you can trust

85% of threats detected were undiscovered by others

51% of zero-day malware is undetected by anti-virus solutions

14 minutes from detection to inclusion in the cyberthreat feed

Operated by CIRA, Canada's registry

24x7 premium support

Powerful threat blocking

CIRA's DNS Firewall is built using Akamai's industry-leading recursive DNS technology and incorporates cyberthreat feeds from Akamai and the Canadian Center for Cybersecurity.

Dynamic threat feed produced from global DNS data – more than 100,000 malicious domains are added to the threat list daily.

Protection from phishing – new phishing domains detected and added to the block list in near real-time.

Disable malware by disrupting command and control – 80-90% of malware can be disabled at the DNS level (and most is distributed that way) by disrupting C&C communication

Customizable web content filtering – enforce acceptable internet use policies with easy-to-configure web content filtering, customizable down to individual URLs.

Full deployment in minutes – protection for all devices and users on the network(s) and also supports dynamic IPs.

API integration – easy to integrate into existing dashboards or SIEMs for policy management, logs, alerts, etc.