

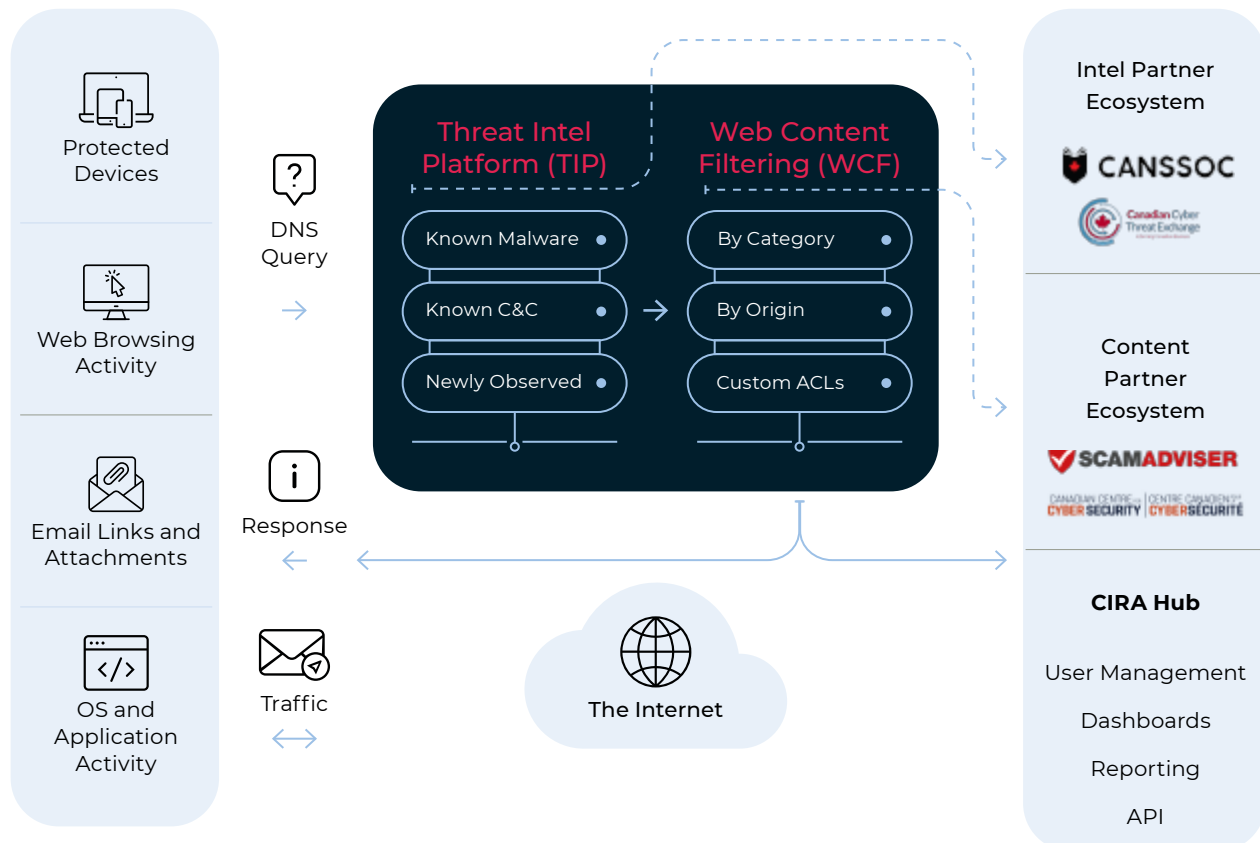


Reinforce your network and endpoint security with **DNS-powered threat intelligence**

CIRA DNS Firewall helps protect your network traffic by blocking emerging phishing attacks and malware threats as they arise. Business customers can also enforce Internet use policies, ensuring employees can use company resources safely by filtering prohibited and potentially malicious content.

“But we already have a firewall” Not all firewalls are created equal, and like any good Canadian you surely understand the value of layering up for protection. While Next Generation Firewalls use advanced technology to enhance network security and threat prevention capabilities, some DNS-based attacks can slip through and threaten organizations with potential data breaches, malware infections, botnet attacks, and more. By adding CIRA DNS Firewall on top of your security stack, your organization can establish an additional layer of defense to effectively counter DNS-based threats.

How CIRA DNS Firewall Works



CIRA DNS Firewall by the numbers

85%

of threats detected
were undiscovered by
other solutions

4.1M

Canadian users
protected with
CIRA DNS Firewall

90%

Reduction in
desktops impacted by
spearphishing attacks

100,000

New malicious
domains
blocked every day

WHAT OUR USERS ARE SAYING

It adds another layer of content and security control. Redundancy alone would be worth the price, but it also augments our other security tools. It is super simple to setup. Policies can be broad or granular as you needed. It catches malware payloads that have not yet been detected by other vendors.

I love tools that are simple, effective,
and affordable. CIRA's NS DNS Firewall
checks all 3 boxes.

— JAYMON, IT DIRECTOR



To learn more visit
cira.ca/firewall or scan
the QR code to book a free
no-obligation meeting **with**
one of our cybersecurity
experts.

DNS Firewall features



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%+ of malware can be
hampered by a DNS firewall
disrupting its command and
control communication.



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



Automated security – Enhanced
SOC capabilities via SIEM /
SOAR integration.



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



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



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