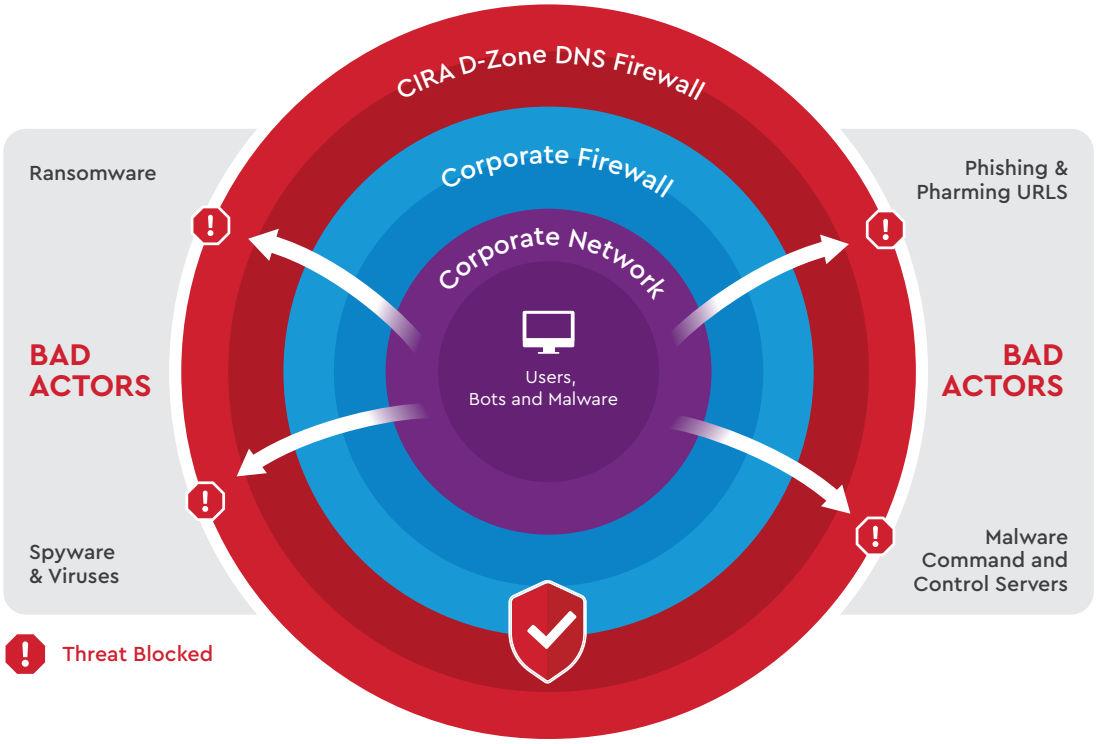
D-Zone **DNS Firewall**

Uncover the malware
that's already on your network –
and keep it from coming back!



Detect

Real time and historical analysis of global DNS data to detect security threats

Feed

Policy enabled recursive DNS servers are updated with real-time threat feeds

Enforce

Servers examine DNS transactions and block domain and IP security threats and filtered sites and categories

Report

Malicious activity is identified and reported

Mitigate

Locate and quarantine infected devices

Key Features

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

Disable malware by disrupting command and control – more than 90% of malware can be disabled at the DNS level by disrupting communication to command and control servers.

Full deployment in minutes – protection for all devices and users on the network with no hardware or software to install.

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

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.

Powered by AKAMAI

CIRA's DNS Firewall is built using Akamai's industry-leading recursive DNS technology and dynamic cyberthreat feed.

Learn more and try!

Visit **cira.ca/cybersecurity-services** or contact us to book a demo at **info@d-zone.ca**

At the core of any security solution is the data and data science used to produce the threat feed. By combining advanced data science with visibility on 3% of global DNS traffic and 30% of global web traffic, Akamai's threat feed provides a powerful incremental layer of protection.

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

Attackers deploy multiple strategies—so should you

No single solution addresses all exploits. Attackers will target the network, BYOD, shadow IT, and more with multi-vector strategies. The DNS layer is critical to your defence in depth strategy:

- Effective, fast, low-cost
- Protects all devices with no additional hardware or software
- An additive layer of protection with a threat feed produced from internet traffic

See what you are missing
Almost every new customer discovers malware on their network that they didn't know they had.