CIRA Cybersecurity Services

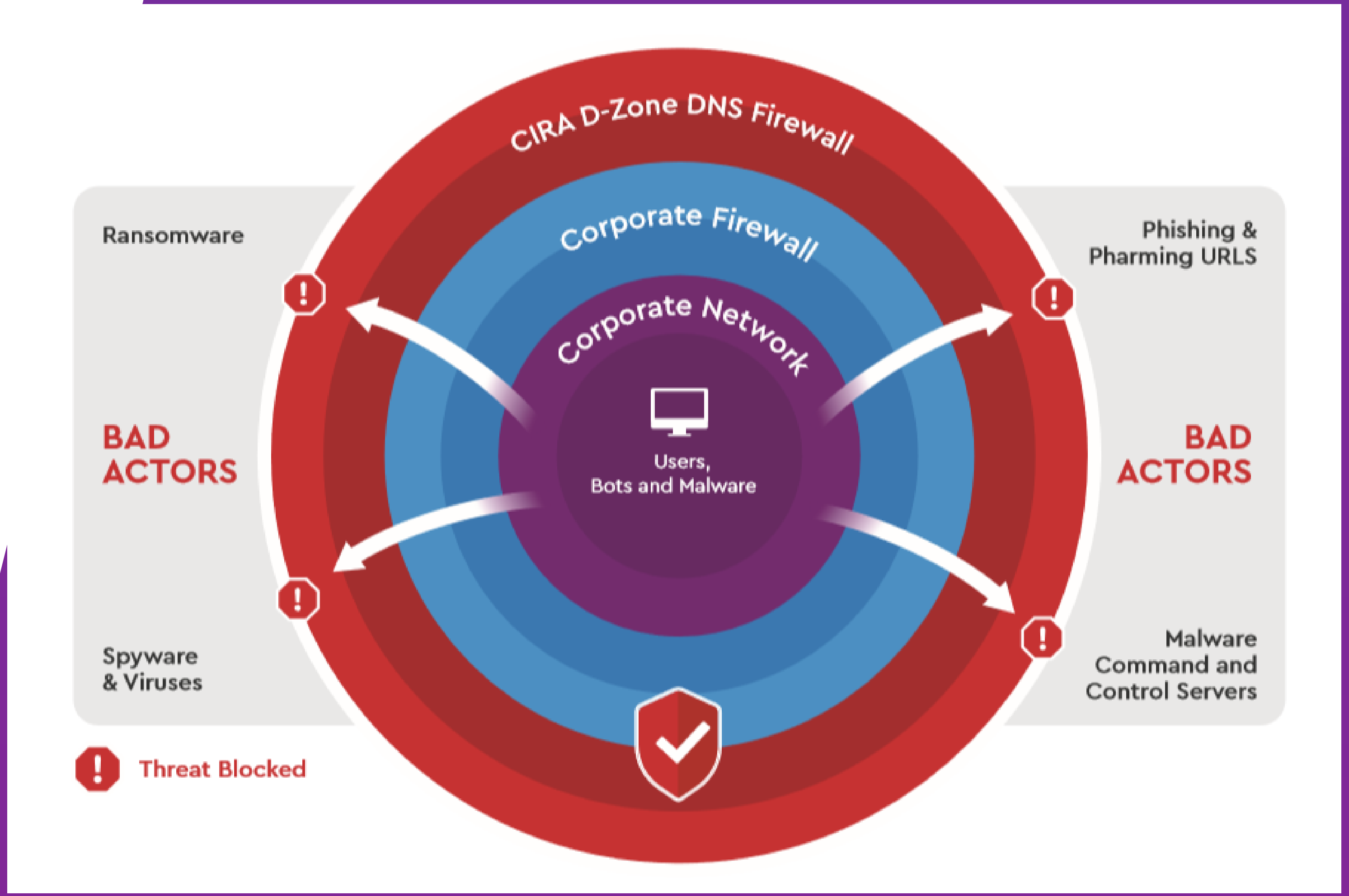
CIRA DNS Firewall

CIRA DNS Firewall

CIRA DNS Firewall

W W W . C I R A . C A

- ✓ A layer outside the organization that provides highly effective malware, phishing and botnet protection
- ✓ Already deployed at 57 research and education* organizations in Canada
- ✓ Over 2 million Canadian users across public sectors



cira

* Excluding K-12

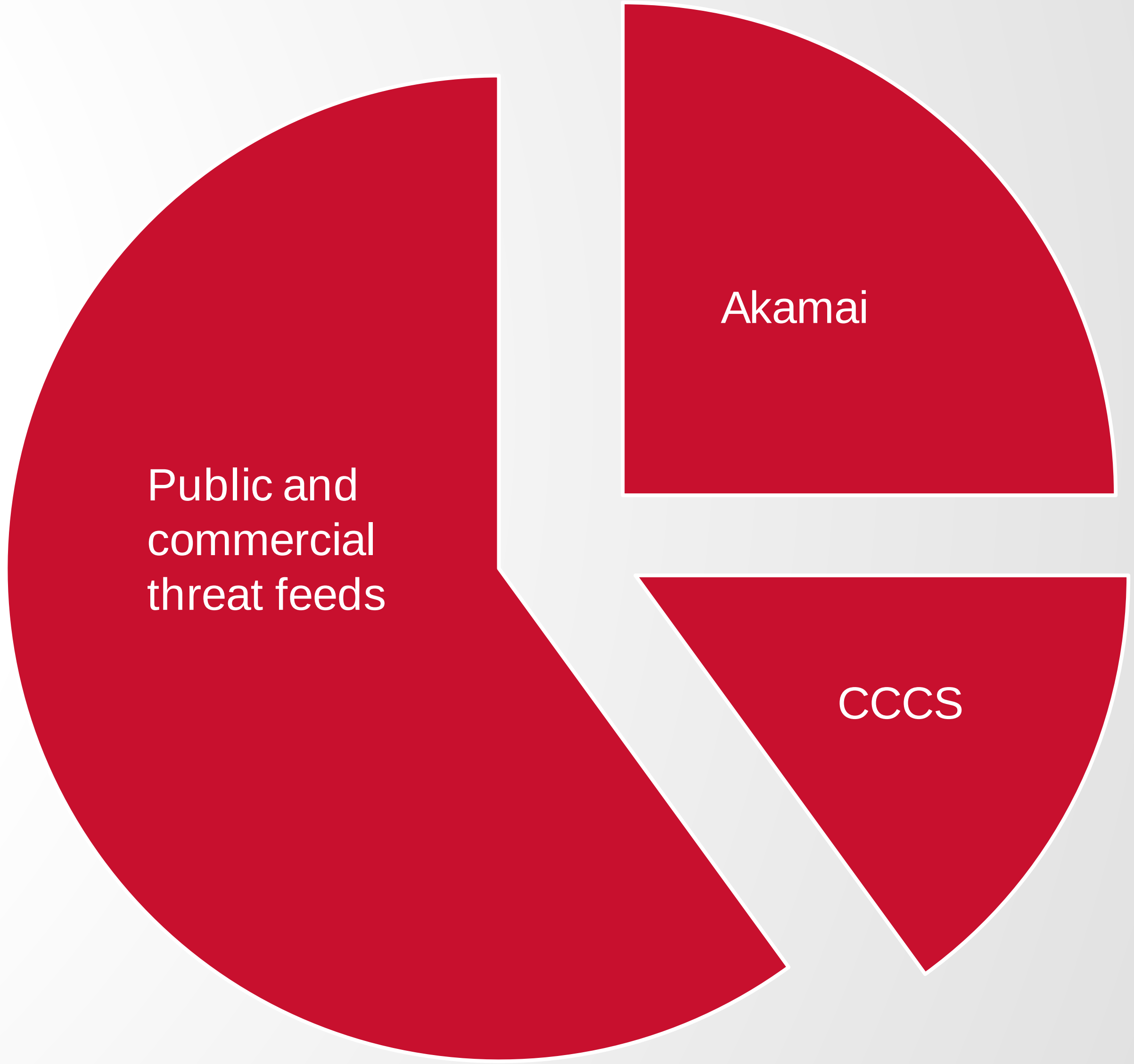
CLASSIFICATION:PUBLIC

W W W . C I R A . C A

CIRA DNS Firewall is delivering

High performance DNS delivering 5x higher block rate than seen in other public sector peers.

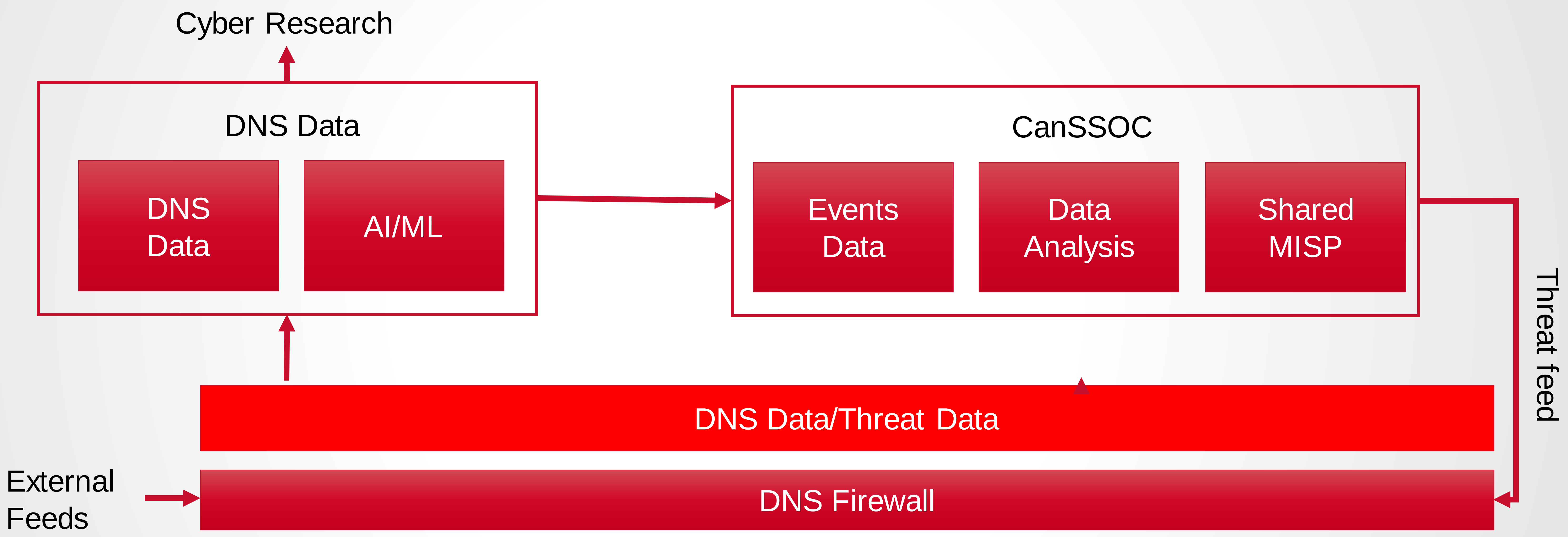
- ✓ Top quality DNS answering 13 billion queries per month with a **median response time of 18 ms** – better than Google 888*.
- ✓ On average more than **100,000 new threats are added** to the block list daily
- ✓ NREN networks saw **1.3M threats blocked last month** or 2 blocks/network user**



Sources of threat blocking

* Tests performed using RIPE Atlas from Canadian servers
**COVID-times data. For comparison, pre-COVID was just under 3 blocks/user in higher-ed, 5 in K-12, and 1.6 in municipalities.

National DNS Firewall Vision



Cyber Research

DNS Data

DNS Data

AI/ML

CanSSOC

Events Data

Data Analysis

Shared MISP

Threat feed

DNS Data/Threat Data

External Feeds

DNS Firewall

Ryerson University

McGill University

University of Alberta

University of Toronto

UBC

McMaster University

(founding CanSSOC members shown)

W W W . C I R A . C A

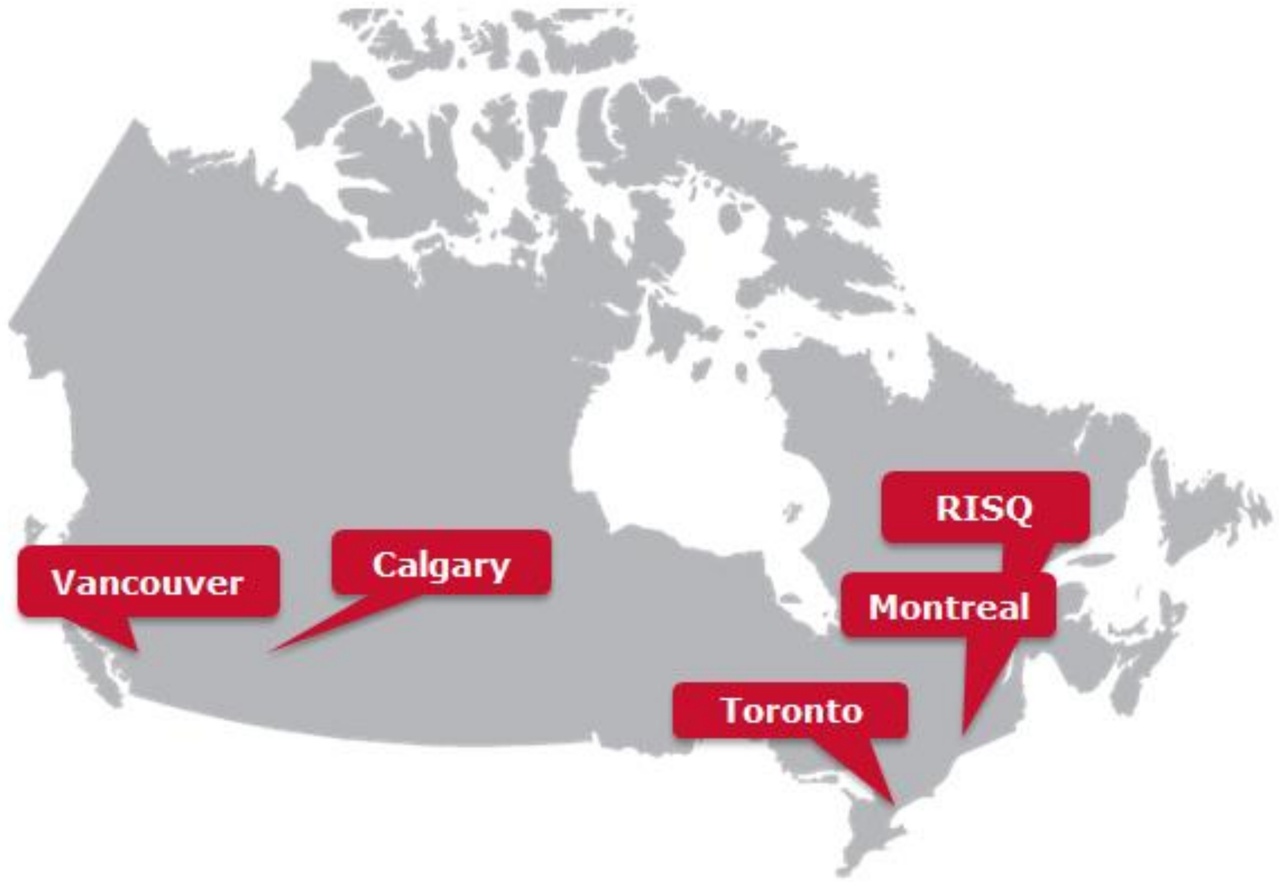
cira

CIRA DNS Firewall

Architecture Highlights

W W W . C I R A . C A

- ✓ Two anycast clouds
- ✓ Server redundancy at nodes
- ✓ Network redundancy
- ✓ Peered to Canadian IXPs
- ✓ 18 ms median DNS response time seen in NREN customers
- ✓ 13 billion queries answered per month across the service



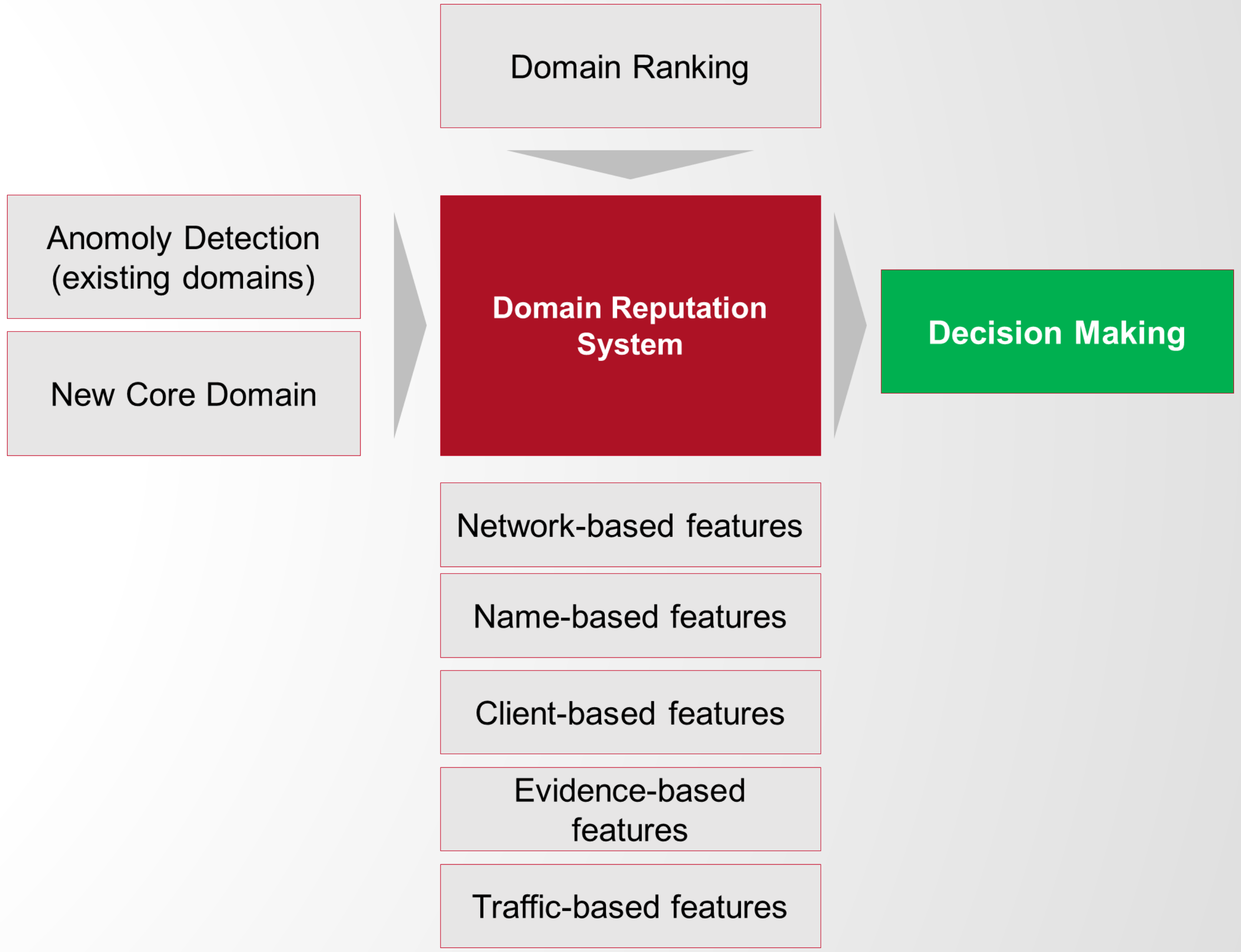
cira

CLASSIFICATION:PUBLIC

Defence in depth

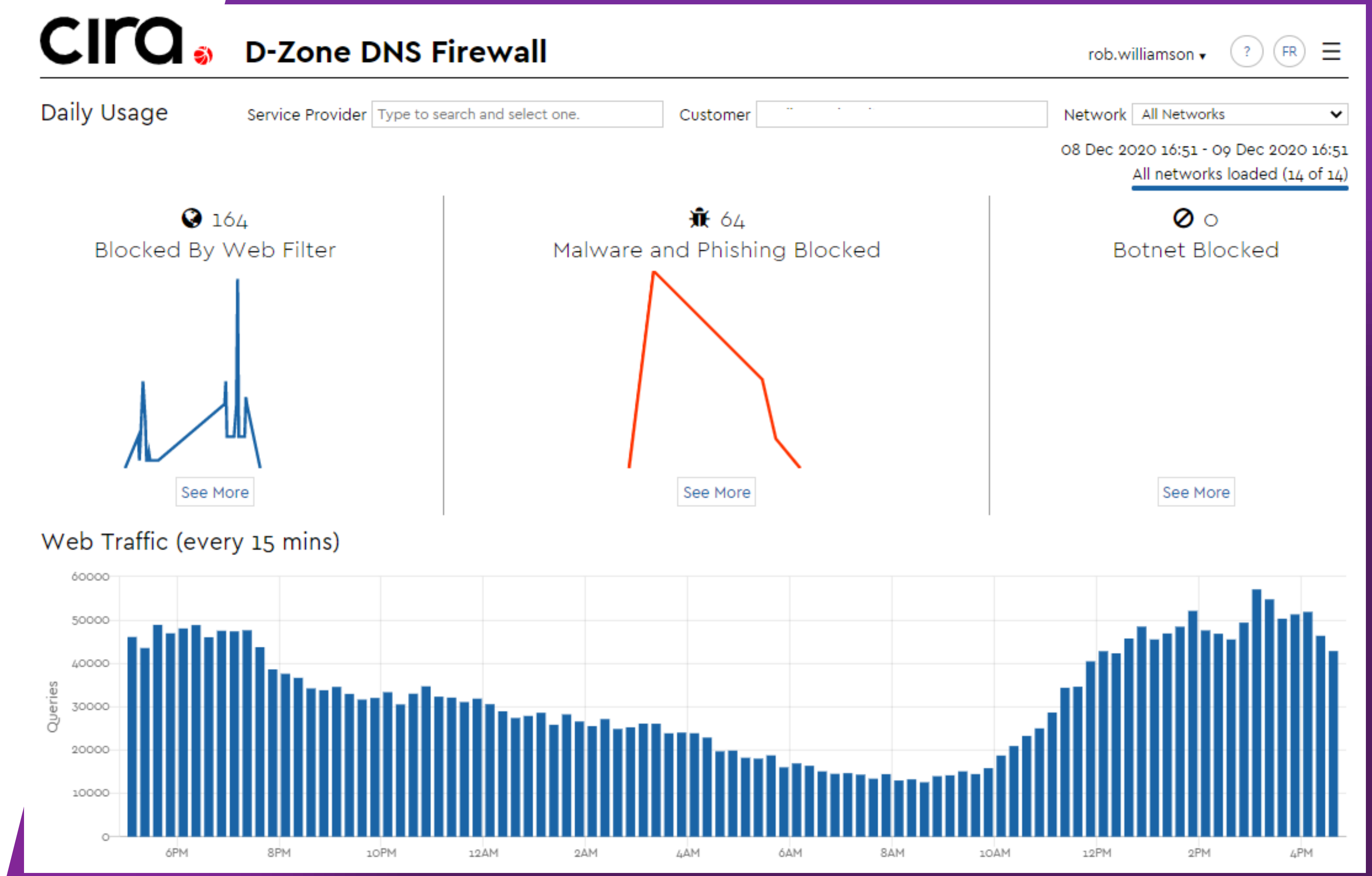
Greater than 40% of threat detection is exclusive to the CIRA DNS Firewall platform. 60% are from public and commercial feeds.

- 1 million QPS are analyzed on a global network of DNS servers
- Time from first query to the block list is < 14 mins
- On average more than 100,000 net new threats are added to the list daily



Features

- ✓ Manage multiple networks from a single portal
- ✓ Over 60 custom content filter categories plus whitelist and blacklist management
- ✓ Customizable block pages for content and malware threats
- ✓ Full API for further integration of reporting



D-Zone DNS Firewall

rob.williamson ▾ ? FR ☰

Daily Usage

Service Provider: Type to search and select one.

Customer:

Network: All Networks

08 Dec 2020 16:51 - 09 Dec 2020 16:51

All networks loaded (14 of 14)

164 Blocked By Web Filter

64 Malware and Phishing Blocked

0 Botnet Blocked

Web Traffic (every 15 mins)

W W W . C I R A . C A

Configuration

1

Get access

1. Complete CANARIE OCCA form.

2. Book onboarding meeting OR simply request your portal access.

https://www.cira.ca/cybersecurity-services/canarie-cybersecurity-initiatives-program

2

Configure network profiles

1. Add network IP addresses

2. Customize block pages

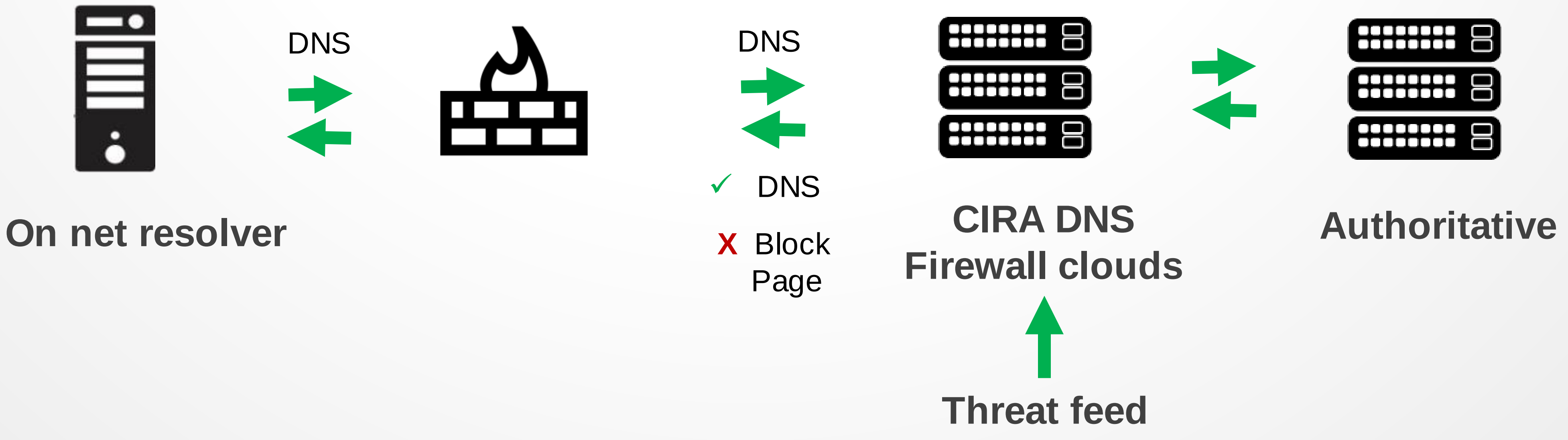
3. Configure content filtering and upload any block lists already maintained and enable CanSSOC*

3

Forward DNS queries

1. Turn off or set cache to short time

2.	IPv4	163.219.51.2 169.219.50.2
	IPv6	2620:10a:8054::2 2620:10a:8055::2
	DoH	https://dns.cira.ca/dns-query



*CanSSOC members only