INDEPENDENT ASSESSMENT / CANADIAN CYBERSECURITY

CIRA Cyber Stack

Canadian control, dependencies and evidence

An independent assessment of CIRA Cyber Stack and its Canadian sovereignty proposition.

PUBLIC PROFESSIONAL RESOURCE / 3 SEPTEMBER 2026

JUNIOR WILLIAMS

Summary

CIRA Cyber Stack is the name CIRA uses for a portfolio of cybersecurity services. It includes XDR, MDR, DNS security, Anycast DNS, awareness training and a shared customer portal.

The Canadian-control claim is clearest for XDR and MDR. CIRA says the data, infrastructure and personnel for those services remain in Canada. CIRA already operates .CA and DNS services, provides bilingual support and has Canadian not-for-profit ownership.[3][4]

The dependencies differ by service. Awareness training uses a third-party platform and processes data in Canada and Europe. Anycast DNS uses a global network. XDR integrations can send customer data to other providers under their terms.[6][8][10]

CIRA targets municipalities, universities, schools, hospitals, non-profits and small or mid-sized organizations with lean security teams.[14]

> **For each service, record jurisdiction, data locations, operators, suppliers, recovery commitments and exit terms.**

What the record shows

1. **Cyber Stack gave existing products a shared name.** CIRA launched the name on 1 October 2025 for XDR, awareness training, Anycast DNS and DNS Firewall. Each service remained available separately.[1]
2. **XDR and MDR cover detection and response.** XDR collects and analyzes telemetry. MDR, launched in February 2026, adds 24/7 Canadian monitoring, investigation, threat hunting and coordinated response.[3][4]
3. **The DNS services have the longest operating record.** CIRA reports 4,050,984 active DNS Firewall users, 413 Firewall customers and more than 145 billion average Anycast queries per day. These figures use different measures and are not Cyber Stack subscription counts.[13]
4. **CIRA Hub is unfinished.** CIRA's FY27 plan lists continued Hub development. Its FY26 annual report also says XDR missed the original market forecast and that CIRA revised its approach.[13][15]

Acknowledgement

This review was prompted by Jamie Hari, who pointed me toward CIRA Cyber Stack. The analysis and conclusions are my own.

The portfolio

Cyber Stack is a shared name for several CIRA security services. CIRA Hub is its customer portal. CIRA documents reporting, device views, user management and single sign-on for DNS Firewall. Its FY27 plan says development continues, so buyers should ask what the portal covers today.[2][5][15]

CIRA is a Canadian member-based not-for-profit that operates .CA. It is not a federal security or intelligence agency. Buyers should still review CIRA's security, contracts, partners and suppliers.[16]

Services and dependencies

Function	Service	Documented capability	Canadian-control factors	Questions for CIRA
Detection and response	**CIRA XDR**	Collects telemetry from endpoints, identities, cloud services, email and network logs. Provides incident management, log analysis and automated playbooks.	CIRA says XDR is built, managed and hosted in Canada, with data under Canadian jurisdiction.	Which connectors, endpoint types, ingestion limits, retention periods, tuning services and response actions are included? Where do integrations send data?
Managed monitoring	**CIRA MDR**	Adds 24/7 monitoring, investigation, threat hunting and coordinated response to XDR.	CIRA says the data, analysts and infrastructure remain in Canada. Calian's Canadian SOC supports the initial service.	Who provides the service, where are analysts located, who handles evidence and what actions can analysts take? What response times apply?
DNS filtering	**CIRA DNS Firewall**	Filters recursive DNS requests and blocks malicious or prohibited destinations. Supports remote users, reporting, APIs and content controls.	CIRA operates the service and publishes a privacy policy. It collects query and IP data and may share some threat data with intelligence partners.	Where are the resolvers? What is logged and retained? What data is shared? How are false positives, remote clients and SIEM integrations handled?
Staff training	**Cybersecurity Awareness Training**	Provides bilingual courses, phishing simulations, reports, risk assessments and optional email analysis.	CIRA sells the service. A third-party supplier provides the platform, hosting and Tier 3 support. Data is processed and stored in Canada and Europe.	Who is the supplier? Where is each data type processed? How are submitted email, AI features, deletion and export handled?

Function	Service	Documented capability	Canadian-control factors	Questions for CIRA
Authoritative DNS	**CIRA Anycast DNS**	Provides secondary authoritative DNS through Canadian and international nodes, with DNSSEC, TSIG, IPv6, APIs and DDoS protection.	CIRA controls the service, and the network includes infrastructure outside Canada.	Where are the management plane and logs? How are zone transfers, DNSSEC, DDoS capacity, failover tests and SLA exclusions handled?
Registry DNS	**CIRA TLD Anycast**	Provides global authoritative DNS for top-level-domain operators.	CIRA operates the service through global infrastructure.	Is the buyer a registry or TLD operator, which is the service's intended market?
Portal	**CIRA Hub**	Displays product information, trends, alerts, threats and action items.	Public documents say the portal is still being developed.	Which products work in the portal today? Does it provide correlation, role-based access, audit logs, APIs and exports?

The product pages describe the intended functions. Buyers still need to confirm architecture, contract terms and performance in their own environment.

How Canadian control differs by service

The Government of Canada assesses digital sovereignty through control of infrastructure, data, intellectual property, law, operations, technical capacity, workforce and suppliers. Its framework recognizes that Canada will continue to depend on an interconnected global internet.[17]

Dimension	Cyber Stack position	Assessment
Canadian governance	CIRA is a Canadian member-based not-for-profit that operates .CA and reinvests revenue in its Canadian internet mission.	CIRA's Canadian ownership reduces foreign-parent exposure. Buyers should still identify every licensor, partner and supplier.
Data location	XDR and MDR carry clear Canada-residency statements. Awareness training uses Canada and Europe. Anycast DNS is globally distributed.	Location depends on the service. Buyers should obtain a data map covering backups, support access, telemetry, submitted emails and management metadata.
Operational control	CIRA operates Canadian infrastructure and support; MDR uses Canadian analysts and initially partnered with Calian's Canadian SOC.	CIRA documents Canadian operations for its core services. Contracts should name everyone who can access data, authorize containment, change detections or provide after-hours support.
Technology and supply chain	XDR is presented as open and modular; awareness training relies on a third-party platform; integrations introduce additional providers.	CIRA describes XDR as open and modular. Buyers should request software-component, licensor and subprocessor lists for every service.
Assurance	CIRA achieved ISO/IEC 27001:2022 recertification covering managed services supporting the Registry, DNS services and XDR, including related infrastructure and development assets.	The certificate covers the published scope. Buyers should confirm coverage for each purchased component, the MDR partner and the awareness platform.
Continuity and exit	Products are modular and XDR is described as open. Standard terms use three-year periods unless an order form says otherwise; XDR export help may require paid professional services and 90 days' notice.	Exit terms depend on the contract. Buyers should agree on export formats, transition help, deletion evidence and renewal dates before deployment.

Overall assessment

CIRA documents Canadian governance and Canadian-hosted XDR and MDR. Its DNS services operate at established scale. Awareness training uses processing in Canada and Europe, while Anycast uses infrastructure outside Canada. Buyers should describe sovereignty service by service.

CIRA states that sovereignty requires the ability to act independently within a globally connected internet.[13]

Documented strengths

1. The DNS services operate at scale

CIRA operates .CA and reports millions of DNS Firewall users and more than 145 billion average Anycast queries per day.[5][6][13]

2. MDR provides 24/7 monitoring in Canada

Some Canadian organizations cannot staff a 24/7 security operations centre and require telemetry to remain under Canadian jurisdiction. XDR provides locally hosted detection and orchestration. MDR adds continuous monitoring and coordinated response by Canadian personnel.[3][4]

Standard XDR support covers Monday to Friday from 08:00 to 20:00 EST, with urgent after-hours support for priority 1 and 2 service issues. MDR provides the 24/7 threat monitoring layer.[10]

3. Customers can buy one service at a time

CIRA sells the services separately. A customer can add one product and keep its other controls.[1]

4. CIRA targets organizations with small security teams

CIRA targets the MUSH sector - municipalities, universities, schools and hospitals - and underserved small and medium-sized organizations. These buyers often have small security teams and need bilingual service, local support and controls they can operate.[14][15]

5. Cybersecurity revenue funds CIRA's Canadian internet work

CIRA reinvests cybersecurity revenue in its Canadian internet mission. Buyers seeking a Canadian vendor may value that ownership model. Product effectiveness requires separate evidence.[2][16]

Where Cyber Stack fits in a broader security architecture

Cyber Stack supplies several controls within a broader defence-in-depth program.

Security need	Cyber Stack contribution	Controls still commonly required
Detection, investigation and response	XDR; optional 24/7 MDR	Incident-response plans, legal and privacy workflows, forensics retainers, crisis communications, cyber insurance coordination and tested recovery decisions.
Endpoint and telemetry visibility	XDR agents and integrations	Secure configuration, patch and vulnerability management, application control, mobile-device management and specialized EDR features where required.
Identity monitoring	XDR ingestion and correlation	Identity governance, MFA, conditional access, privileged-access management, lifecycle controls and phishing-resistant authentication.
DNS-layer prevention	DNS Firewall	Network segmentation, firewalls, secure web gateways or SASE/ZTNA where appropriate, and application-layer protections.
Public DNS resilience	Anycast DNS	Primary-DNS governance, registrar security, registry lock, domain monitoring, DNS change control and recovery testing.
Human risk	Awareness training and phishing simulations	Role-based procedures, executive exercises, secure business processes, payment verification and a culture that rewards reporting.
Data protection	Indirect visibility through XDR	Encryption and key management, data classification, DLP, immutable backups, disaster recovery and retention governance.
Cloud, application and product security	Telemetry and selected integrations	Cloud-security posture, workload protection, application security testing, software-supply-chain controls, secrets management and secure development.

CIRA's strategic plan targets organizations that find large enterprise portfolios expensive and difficult to operate.[14]

Evidence available today

Claims supported by public records

- CIRA operates .CA under Canadian governance.[16]
- CIRA reports 4,050,984 active DNS Firewall users, 413 Firewall customers and more than 145 billion average Anycast queries per day.[13]
- ISO/IEC 27001:2022 recertification covers the Registry, DNS services and XDR-related managed services and assets.[12]
- Awareness training had 497 customers and 318,000 employees protected at the end of FY26, according to CIRA.[13]
- CIRA has published a Yukon University XDR case study describing Microsoft 365 log integration, correlation across email, firewall and Azure AD data, and customized dashboards.[18]

Claims with limited public evidence

- XDR launched in May 2025 and MDR launched in February 2026. Both have a shorter operating record than the DNS services.[3][4]
- CIRA's FY26 report says XDR missed the original adoption forecast and that CIRA revised its approach. Buyers should ask how many organizations now use XDR and request references from customers with a similar environment.[13]

- CIRA's FY27 plan lists continued development of CIRA Hub.[15]
- CIRA remains the main source of public evidence. Independent tests, comparisons and MDR outcome data are limited.

Verify performance and compliance claims

CIRA publishes metrics for threat feeds, detection speed, phishing-click reduction and MDR containment. Buyers should ask how each metric was defined, measured and tested in a comparable environment.[4][5][7]

XDR and MDR may help collect evidence and meet residency or monitoring requirements. Customers remain accountable for compliance, configuration and lawful data handling.

Public information still needed

CIRA should publish these details for each service and include them in contracts.

1. **Service-level sovereignty facts.** Identify corporate jurisdiction, data locations, support locations, subprocessors, backup regions, remote-access paths and legal-control boundaries.
2. **Supported integrations.** Publish validated data sources, supported operating systems, identity and cloud connectors, response actions, licensing dependencies and current Hub coverage.
3. **Service-level results.** Report paid customer counts, monitored assets, alert-validation performance, response times, false-positive reduction and customer retention without combining them with free Canadian Shield users.
4. **Exit terms.** Specify standard export formats, transition timing, deletion evidence, rule and dashboard portability, and the cost of professional assistance.
5. **Assurance coverage.** Clarify which components, partners and subprocessors sit inside ISO certification, penetration testing, business-continuity exercises and incident-notification commitments.

Questions to ask before purchase

Ask CIRA or its reseller to answer these questions in writing.

Architecture and coverage

- Which products and current versions are included in the proposed scope?
- Which endpoint, identity, network, email, cloud and SaaS data sources are natively supported?
- What telemetry is collected, at what volume, and how are ingestion, storage and retention charged?
- Which detections, dashboards, integrations and playbooks are included versus professional services?
- Which security controls remain the customer's responsibility?

Sovereignty and privacy

- Where is each data class stored, processed, backed up, administered and viewed?
- Which legal entities, licensors, hosting providers, MDR partners and subprocessors can access it?
- Can foreign-based personnel provide support or receive telemetry under any circumstance?
- What data is shared for collective defence or threat intelligence, and how is it de-identified?
- For awareness training, what remains in Canada, what is processed in Europe, and what changes when optional email-analysis or AI features are enabled?

Operations and incident response

- What is monitored 24/7: customer threats, service availability, or both?
- What are the contractual targets for acknowledgement, investigation, escalation and containment?
- Which containment actions may analysts take automatically, which require approval, and how is authorization recorded?
- Who preserves evidence, coordinates forensics and supports regulatory or legal notifications?
- How are detection quality, false positives and missed incidents reviewed?

Contracts and exit

- What is the exact scope of ISO 27001 and any other independent assurance relevant to the purchased services?
- May the customer review penetration-test summaries, business-continuity results and material incident history?

- What are the initial term, renewal period, non-renewal deadline, annual uplift and service-credit limitations?
- How are data, rules, cases, dashboards and evidence exported, and what transition assistance is included?
- What is deleted at termination, on what schedule, and what proof of deletion is available?

Test the service before purchase

Run a limited deployment and decide in advance what result would justify a purchase. Test connectors, alerts, analyst workflow, containment approvals, bilingual support, performance, data export and failover. Use one tabletop incident to test handoffs among CIRA, its MDR partner, the customer's security team, legal counsel and executives.

Conclusion

Cyber Stack gives Canadian public-interest and mid-market organizations a domestic XDR and MDR option, established DNS services and bilingual support.

CIRA's Canadian governance, DNS operations and Canadian-hosted XDR and MDR are the clearest parts of its sovereignty claim. Awareness-training data is processed in Canada and Europe, and Anycast uses infrastructure outside Canada. Several services also depend on third parties. Buyers should document those dependencies for each product.

Buyers seeking Canadian control should include CIRA's ownership in their review. They should also require service-level data flows, supplier lists, customer counts and independent results.

Scope and limits

This report reviews CIRA product pages, policies, contracts, plans and reports published through 3 September 2026, along with the Government of Canada's digital-sovereignty framework. It had no access to private architecture, customer contracts, demonstrations, penetration-test results, paid analyst research or independent laboratory testing.

This is not a competitor ranking, legal opinion, compliance certification or purchase recommendation. Buyers should verify current products, partners, terms and data locations.

Sources

1. CIRA, CIRA introduces Cyber Stack: a Canadian cybersecurity suite, 1 October 2025. Evidence for: launch date and initial portfolio scope.
2. CIRA, CIRA Cyber Stack, accessed 3 September 2026. Evidence for: portfolio positioning and CIRA Hub.
3. CIRA, CIRA XDR, accessed 3 September 2026; CIRA, CIRA XDR launch, 1 May 2025. Evidence for: XDR functions, Canadian hosting and launch date.
4. CIRA, CIRA MDR, accessed 3 September 2026; CIRA, CIRA MDR launch, 18 February 2026. Evidence for: 24/7 monitoring, Canadian personnel and MDR launch date.
5. CIRA, CIRA DNS Firewall, accessed 3 September 2026. Evidence for: DNS filtering features and product claims.
6. CIRA, CIRA Anycast DNS, accessed 3 September 2026. Evidence for: Anycast features and global infrastructure.
7. CIRA, Cybersecurity Awareness Training, accessed 3 September 2026. Evidence for: training, phishing simulations and product claims.
8. CIRA, Cybersecurity Awareness Training Terms of Service, updated 12 June 2026. Evidence for: third-party delivery and processing in Canada and Europe.
9. CIRA, Privacy Policy for the CIRA DNS Firewall Service, accessed 3 September 2026. Evidence for: DNS logging, retention and threat-data sharing.
10. CIRA, CIRA XDR Terms and Conditions and SLA, accessed 3 September 2026. Evidence for: support hours, integrations and export terms.
11. CIRA, Master Subscription Agreement, accessed 3 September 2026. Evidence for: standard subscription and renewal terms.
12. CIRA, CIRA achieves ISO 27001 recertification, 23 June 2026. Evidence for: certification scope.
13. CIRA, Fiscal Year 26 Annual Report to Members, 2026. Evidence for: service scale, customer counts and XDR adoption.
14. CIRA, FY26-28 Strategic Plan, 2025. Evidence for: target market and product strategy.
15. CIRA, FY27 Corporate Plan, 2026. Evidence for: CIRA Hub development and current priorities.
16. CIRA, About CIRA, accessed 3 September 2026. Evidence for: ownership, governance and .CA operations.
17. Government of Canada, Digital Sovereignty: A Framework to improve digital readiness, 12 November 2025. Assessment framework.
18. CIRA, Transforming cybersecurity at Yukon University with CIRA XDR, accessed 3 September 2026. Evidence for: published deployment example.

Junior Williams Systems and Enterprise Architecture | Cyber and AI Risk trustcyber.ca | Book an intro call