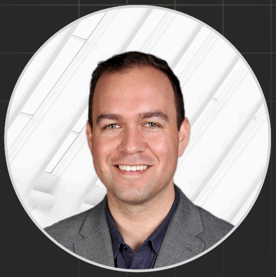
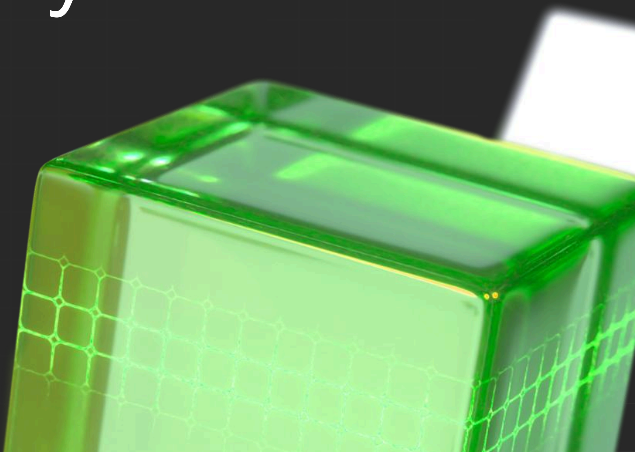
QOHASH



AI adoption moves at the speed of trust

Sovereign data security as a critical pillar of Canada's AI strategy

Insights from Jean Le Bouthillier,
CEO and Chairman of Qohash



Canada's adoption of AI will redefine its economic and strategic future. But while momentum builds, a critical weakness is being ignored: **foreign vendors dominate Canada's vital data security landscape.**

Safe and sovereign AI adoption in Canada depends on three pillars. ① **Sovereign AI models**, such as Cohere, are required for critical government, defence, and regulated uses. ② **Sovereign compute and power**, including initiatives like the TELUS AI Factory, are needed to operate AI at national scale. ③ **Sovereign data security** is required to protect sensitive data across the full AI lifecycle, including training, day-to-day use, and automated actions. Yet it is not treated as a core priority in Canada's AI strategy.

This paper outlines the key data security risks to national sovereignty and long-term control of Canada's digital assets, and explains **how these challenges can be addressed through Canadian data security innovation.**

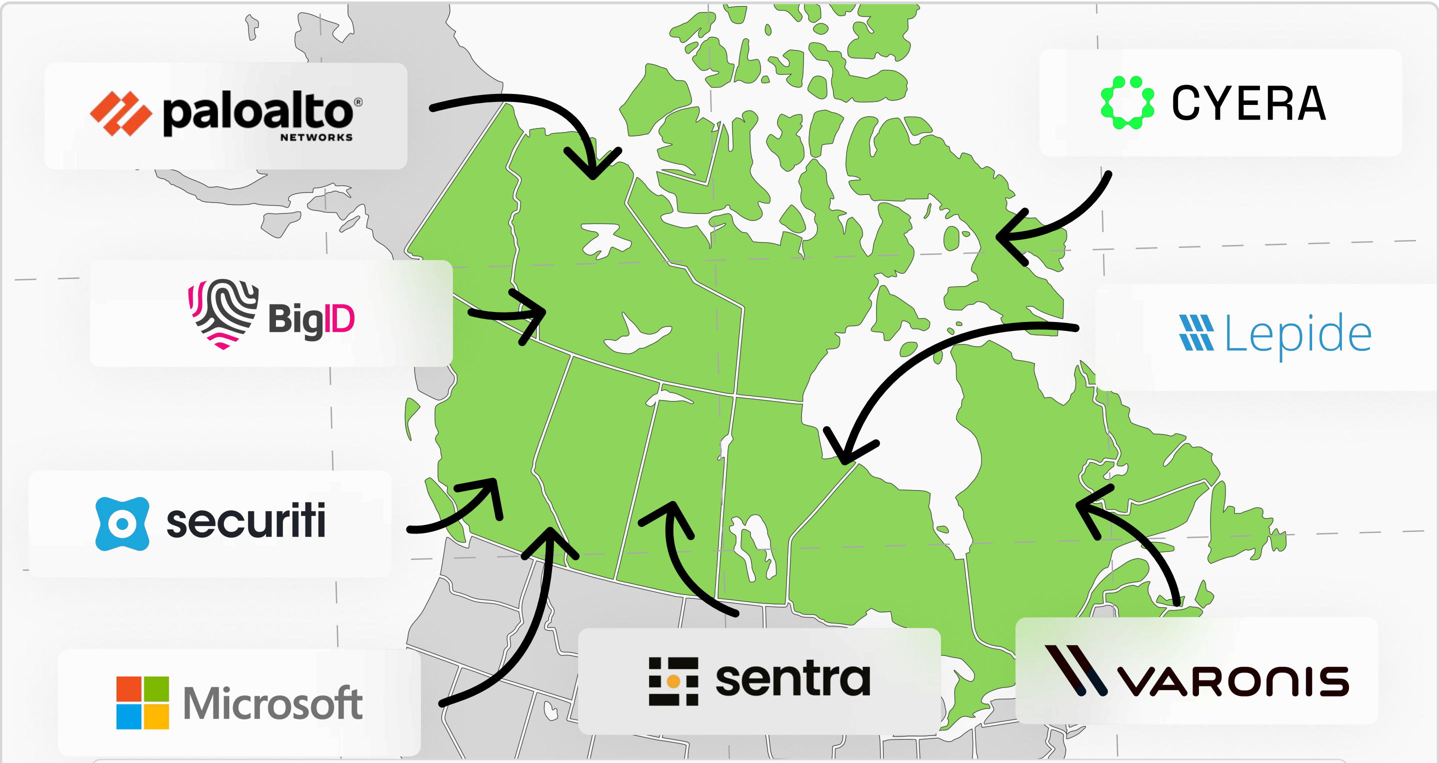
In this paper we cover:

- Foreign vendors dominating Canada's data security landscape
- Risks of relying on foreign, cloud-based data security vendors
- Qohash as Canada's next sovereign data security unicorn

Who controls Canada's data security?

Canada's enterprise data security market is overwhelmingly served by foreign vendors. Multiple Government of Canada publications recognize that over-reliance on external cloud and technology providers exposes sensitive Canadian data to foreign jurisdictions, foreign laws, and reduced national control.[1] [2] [3] However, these publications remain politically correct and do not convey the severity of what is truly happening on the ground:

- Most large Canadian enterprises and public institutions rely almost entirely on foreign data security solutions.
- The majority of data security solutions are cloud based, requiring sensitive data to be copied into third-party environments for analysis, increasing intelligence collection risk.
- Vendors headquartered in the United States and Israel completely dominate the market, controlling platforms, standards, capital, and distribution.



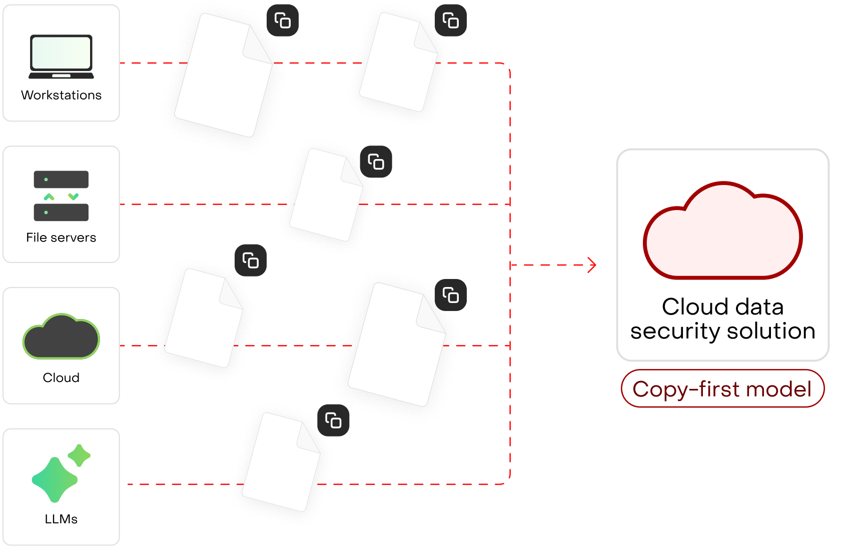
Jurisdiction follows control, not data center location. These risks are not theoretical. In 2025, Microsoft confirmed to European lawmakers that it cannot guarantee data sovereignty if faced with a lawful U.S. request, even when data is stored outside the United States.[4] [5] This obligation arises from the U.S. CLOUD Act, which allows U.S. authorities to compel access to data controlled by U.S.-based companies regardless of location.[6] The same legal framework applies to Canadian data held by U.S.-controlled platforms, meaning foreign jurisdiction can override Canadian control.

When protecting data means exposing it

Most data security solutions used in Canada are not only foreign, they are also built on an outdated and dangerous copy-first model of data centralization. This model dates back to the early days of enterprise security, when Splunk was founded in 2003 and security meant collecting data into a central system for analysis. As cloud adoption accelerated in the late 2000s and early 2010s, platforms such as ELK extended this approach, making centralized data collection the default architecture for security, including data security.

Today, the majority of data security solutions work by copying sensitive files to the cloud to analyze them. Files from employee laptops, file servers, shared drives, and services like OneDrive are duplicated and sent to a third-party application for scanning. Contracts may promise limited use and deletion after processing, but the fact remains that the data has left the organization. Control is lost the moment the data is copied. Even when the cloud runs in Canada, the vendor controls the software, access, and processing. This creates a large intelligence collection risk that grows as AI expands access to sensitive data at scale.

⚠ The centralized, copy-first data security model



When cloud-based data security tools are hosted in Canada but operated by foreign companies, sensitive data remains exposed to legal and strategic obligations outside Canadian control.

Worst case: sensitive Canadian data is exposed to foreign legal access or intelligence collection.

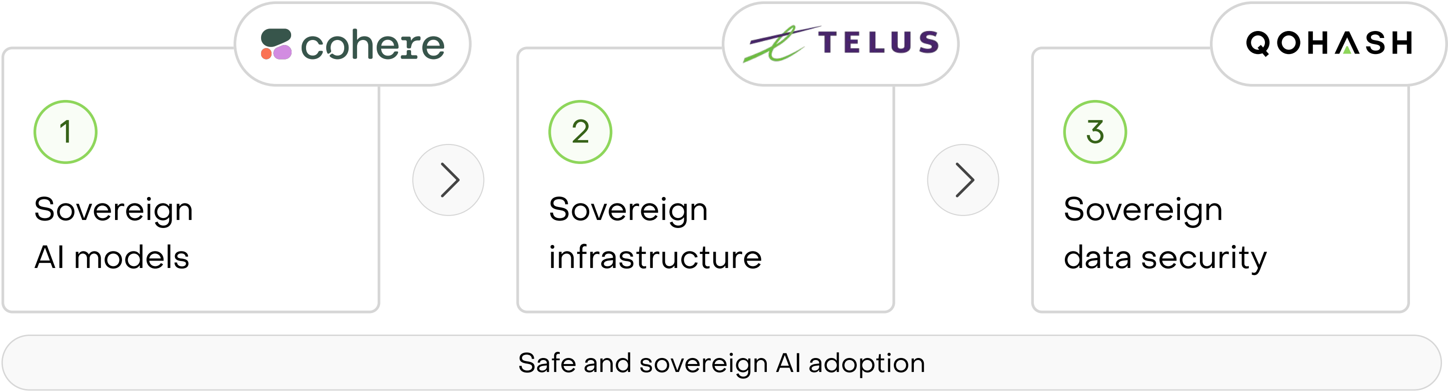
Main issues with cloud-based, copy-first data security

- Sensitive data must be copied to third-party cloud platforms
- Every copy increases exposure and attack surface
- Security is applied after data has already moved, reducing control at the source
- Costs increase as more data is scanned and stored

Safe and sovereign AI adoption

Safe and sovereign AI adoption in Canada depends on three foundational pillars. ① **Sovereign AI models**, such as Cohere, are required for critical government, defence, and regulated use cases. ② **Sovereign compute and power** are required to operate AI at national scale, including initiatives such as the TELUS AI Factory. ③ **Sovereign data security** is required to protect sensitive data before, during, and after AI use.

Qohash directly addresses the third pillar of data security, which has been historically neglected and underinvested in Canada. Our core mission is to dramatically strengthen Canada's sovereign data security posture so the country can safely adopt AI without relying on foreign solutions or exposing sensitive data to intelligence collection risks. This mission also extends to supporting allied nations facing the same challenge. We are also building deep cybersecurity and software engineering expertise in Canada.



The name Qohash reflects this national ambition. Q represents Quebec and O represents Ontario, where the company was originally conceived. Qohash was designed as a pan-Canadian company spanning from Quebec City as the easternmost bound to the greater Toronto area. Today, our ambition and footprint extend across Canada, including major innovation hubs such as Vancouver, Calgary, and Halifax, all of which play an essential role in Canada's rise as a tier one cybersecurity solution provider.

QOHASH
Quebec
QOHASH
Ontario
QOHASH
Data hashing

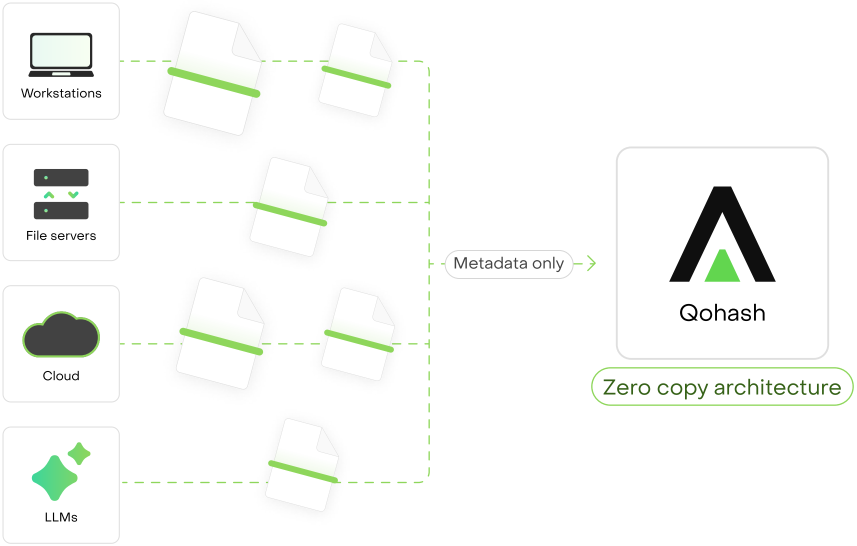
In summary, Qohash is being built as a core national asset. Our objective is to develop leading data security technology in Canada to meet our own needs, Canadian solutions for Canadian problems, and to export this technology globally to support safe and sovereign AI adoption worldwide.

Qohash, the pioneer of zero copy data security

When we founded Qohash with the objective of solving Canadian data security problems with Canadian solutions, **we asked a simple question: why send sensitive data away just to analyze it?** Instead of copying and centralizing data, we designed the data security model of the future based on three clear realities:

- Computing power continues to increase predictably. Moore's Law remains a reliable trend, enabling more processing where data is created.[7]
- Data volumes continue to grow exponentially. Global data creation is doubling roughly every two years, making centralized security unsustainable.[8]
- Intelligence is moving to the edge. GenAI and advanced analytics are increasingly embedded directly in devices, servers, and local systems, requiring security to operate at the source rather than in centralized clouds.[9]

The zero copy data security platform



Trusted by top companies in:

- Financial services
- Energy
- Public sector
- Manufacturing
- Technology & R&D

Zero copy eliminates data movement by securing data at the source—the only scalable approach for petabytes of unstructured data.

- ✓ Rapid in-place data scanning
- Native instant remediation
- Full inventory of unstructured data
- Costs decoupled from data growth

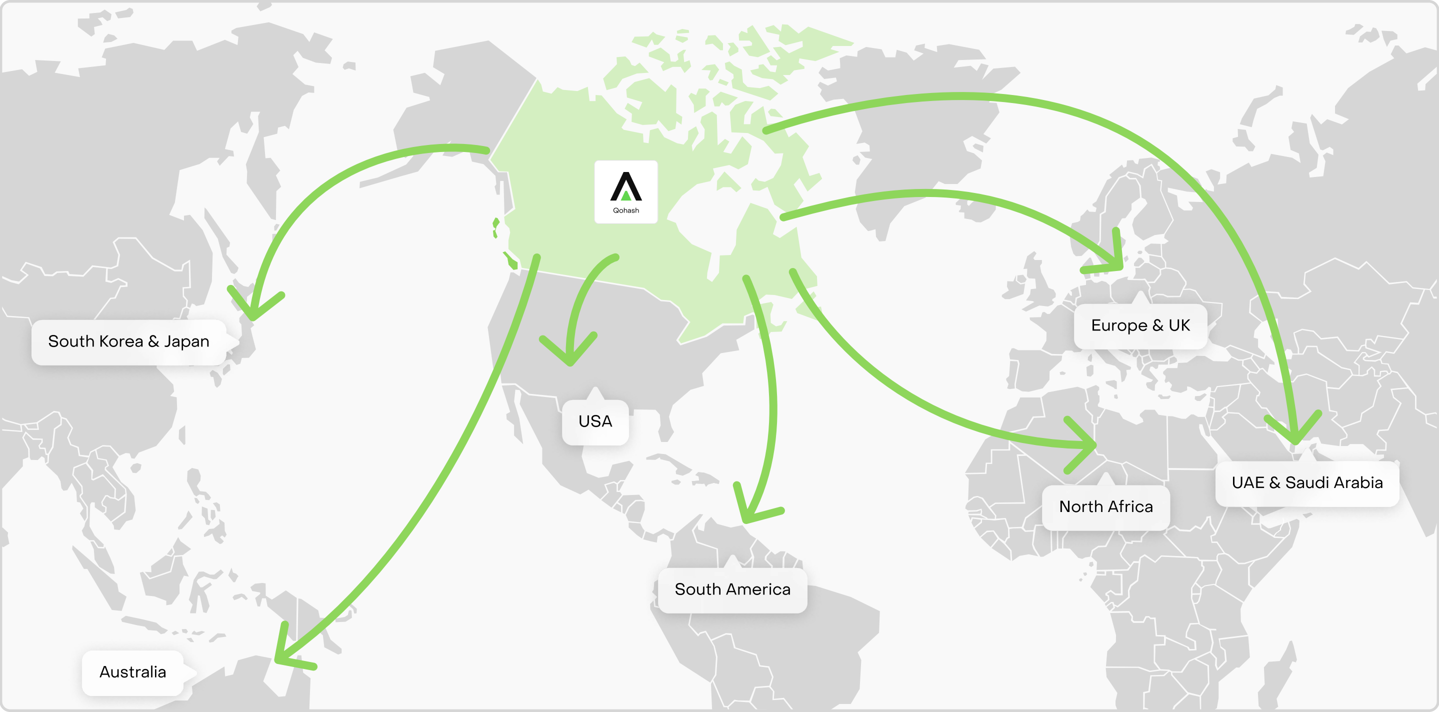
Trusted data security, built in Canada, deployed globally

Canada has a unique opportunity to lead globally in data security at a moment when trust, sovereignty, and control have become defining issues of the AI era. As AI adoption accelerates across governments, critical infrastructure, defence, and the private sector, countries around the world are confronting the same challenge: **how to secure sensitive data at scale without surrendering control to foreign platforms.**

Qohash's vision is to establish trusted data security as a Canadian-built capability that can be deployed globally. Built on first principles and designed for large enterprises, our zero copy data security approach responds directly to the realities shaping AI adoption worldwide: explosive data growth, increasing intelligence at the edge, and rising concerns over sovereignty and jurisdictional exposure. This model allows organizations to secure data where it lives, rather than exporting it to centralized platforms beyond their control.

Governments and enterprises across Europe, NATO countries, MENA, and Asia-Pacific face similar regulatory, security, and trust challenges as AI becomes embedded in daily operations. **Canada is well positioned to offer a credible, values-aligned alternative built on transparency, trust, and sovereign control.**

This is not only a commercial opportunity, but a strategic one. Exporting Canadian data security capability strengthens Canada's influence in the global AI ecosystem while reinforcing domestic resilience.



A Canadian path to global leadership in data security

Through our work with large enterprises and critical infrastructure organizations, we've seen firsthand what it takes to secure sensitive data in the AI era.

Over the next 36 months, Qohash has a focused growth plan that will deliver multiple strategic outcomes for Canada:

1 **Scale global availability from a Canadian base**
Expand Qohash beyond Canada, the United States, and Europe into NATO, MENA, ASEAN, and other allied markets seeking alternatives.

2 **Advance a world-leading zero copy data security platform**
Continue investing in platform development to solidify leadership in zero copy data security as the standard for safe and sovereign AI adoption.

3 **Build a dual-use national capability**
Strengthen a core data security technology that can be readily used for both commercial and defence AI adoption and security use cases.

4 **Create high-value Canadian jobs and expertise**
Grow headcount in engineering, AI, cybersecurity, and go-to-market functions, building durable, high-paying technology jobs and deep domestic expertise.

5 **Anchor data security as national security**
Ensure the technology, operations, and control of this capability remain in Canada, under sovereign governance and trusted oversight.

Qohash is the pioneer of zero copy data security, the only model designed to secure petabytes of unstructured data in large enterprises. AI-native by design, Qohash is leading the shift to autonomous data security, continuously identifying and enforcing data risk controls at machine speed without moving or copying data.

Visit our website www.qohash.com | visit our trust center trust.qohash.com

AICPA SOC 2 TYPE 2 · AICPA SOC 3 · ISO 27001 · ISO 27701 · ISO 42001

References

1. Government of Canada. Government of Canada white paper: data sovereignty and public cloud. Treasury Board of Canada Secretariat. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html

2. Government of Canada. Digital sovereignty in cloud environments https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html

3. Public Safety Canada. Canada's National Cyber Security Strategy: Securing Canada's Digital Future. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

4. The Register. Microsoft admits it cannot guarantee EU data sovereignty under U.S. law, 2025. https://www.theregister.com/2025/07/25/microsoft_admits_it_cannot_guarantee

5. Heise Online. Not sovereign: Microsoft cannot guarantee EU data stays in Europe, 2025. https://www.heise.de/en/news/Not-sovereign-Microsoft-cannot-guarantee-the-security-of-EU-data-10494789.html

6. United States Congress. Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018. https://en.wikipedia.org/wiki/CLOUD_Act

7. Wikipedia. Moore's law. https://en.wikipedia.org/wiki/Moore%27s_law

8. Exploding Topics. Amount of data created per day (2025). https://explodingtopics.com/blog/data-generated-per-day

9. Wevolver. The 2025 Edge AI technology report: The future of edge AI. https://www.wevolver.com/article/2025-edge-ai-technology-report/the-future-of-edge-ai