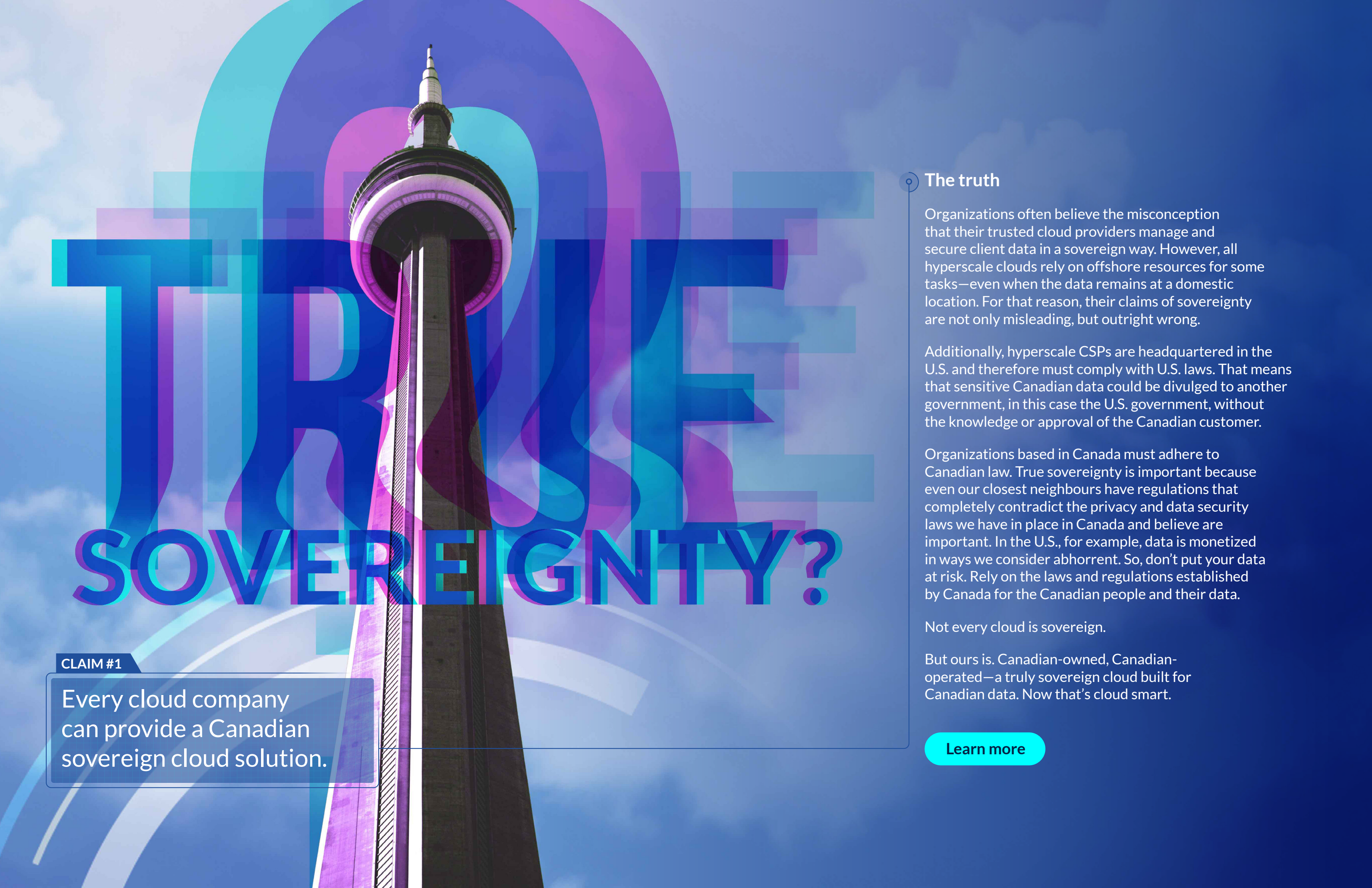




Debunking 7 common hyperscale cloud claims for the Canadian public sector

You want to be sure that your data sovereignty, traceability, and supply chain management are in full compliance with Canadian regulations and that you're getting a fair deal, right?

Then it's time for some cloud, **hard truths.**



TRUE SOVEREIGNTY?

CLAIM #1

Every cloud company can provide a Canadian sovereign cloud solution.

The truth

Organizations often believe the misconception that their trusted cloud providers manage and secure client data in a sovereign way. However, all hyperscale clouds rely on offshore resources for some tasks—even when the data remains at a domestic location. For that reason, their claims of sovereignty are not only misleading, but outright wrong.

Additionally, hyperscale CSPs are headquartered in the U.S. and therefore must comply with U.S. laws. That means that sensitive Canadian data could be divulged to another government, in this case the U.S. government, without the knowledge or approval of the Canadian customer.

Organizations based in Canada must adhere to Canadian law. True sovereignty is important because even our closest neighbours have regulations that completely contradict the privacy and data security laws we have in place in Canada and believe are important. In the U.S., for example, data is monetized in ways we consider abhorrent. So, don't put your data at risk. Rely on the laws and regulations established by Canada for the Canadian people and their data.

Not every cloud is sovereign.

But ours is. Canadian-owned, Canadian-operated—a truly sovereign cloud built for Canadian data. Now that's cloud smart.

[Learn more](#)

CLAIM #2

If my data is in a data centre in Canada, it's sovereign.

RESIDENCY

The truth

There's a BIG difference between data sovereignty and data residency. Data sovereignty refers to both the ownership and operational supply chain location of the data. Data residency, on the other hand, refers only to the geographical location of the data. If a Canadian company operates a data centre in the U.S., the assets within that facility are subject to U.S. jurisdictional rules and are not sovereign. On the flip side, data might be deployed on assets in Canada (residency) that are owned by a foreign entity and/or are operated by non-residents that lack security clearance. These vendors often attempt to obfuscate a non-sovereign service by positioning residency as equivalent to sovereignty.

If non-resident individuals manage the infrastructure, they're not required to comply with your country's privacy policies. While compliance may be a requirement of employment, employees are governed by the laws and policies of their country of residence, and those laws might not penalize employees for compromising data. For example, threat actors are known to take advantage of low labor cost markets that lack anti-bribery laws, in order to bribe employees for access to your data and even export a copy of that data to a third party. When discovered, the individual

might be relieved of their duties for breaking the provider's policies, but they wouldn't be legally accountable for their actions. And if the bribe they were paid was significant enough, the loss of their employment would be irrelevant.

The Government of Canada warns: "Regardless of where the cloud resources are physically located, when data is stored in a cloud environment, the stored data may be subject to the laws of other countries." Hyperscale CSPs, with global deployment, "could be required to comply with a warrant, court order or subpoena request from a foreign law enforcement agency seeking to obtain [Canadian] data." Even if a CSP operates in Canada (as the hyperscale providers do), they are headquartered elsewhere and therefore subject to the laws of another country.

ThinkOn is a Canadian-owned and Canadian-operated company, so we have a vested interest in protecting Canadian data. [Working with a truly Canadian company like ThinkOn](#) ensures that data sovereignty, traceability, and supply chain management are in full compliance with Canadian regulations.

[Learn more](#)

CLAIM #3

Forget cloud first or cloud smart, it should be cloud everything.

The truth

Nope. Not everything should be in the cloud—ours or anyone else's. The push for cloud first was like chasing a shiny object. Many workloads were rushed to the cloud only to find the costs weren't predictable, or the application didn't work as hoped. When you rush, especially with complex government workloads, they can become compromised. That's why cloud smart is the way to go.

There is a lot of non-cloud or private cloud infrastructure inside the government that can support applications—and it should absolutely stay there to support those applications. There's no need to move an existing application and risk compromising it just for the sake of saying that it's cloud first. With cloud smart, you have time to analyze the application and decide whether it really makes sense to move it to the cloud. For some workloads, the cloud makes perfect sense, especially when the data is seasonal or schedule-oriented, such as election or census data.

But for other recurring, business-critical workloads, the cloud may not be the best solution.

The cloud isn't a magical data catch-all. It's someone else's server, configured in a way that makes it more flexible to consume. When it comes to your workloads, the key to knowing whether to cloud—or not to cloud—is knowing your consumption and the best place to direct it.

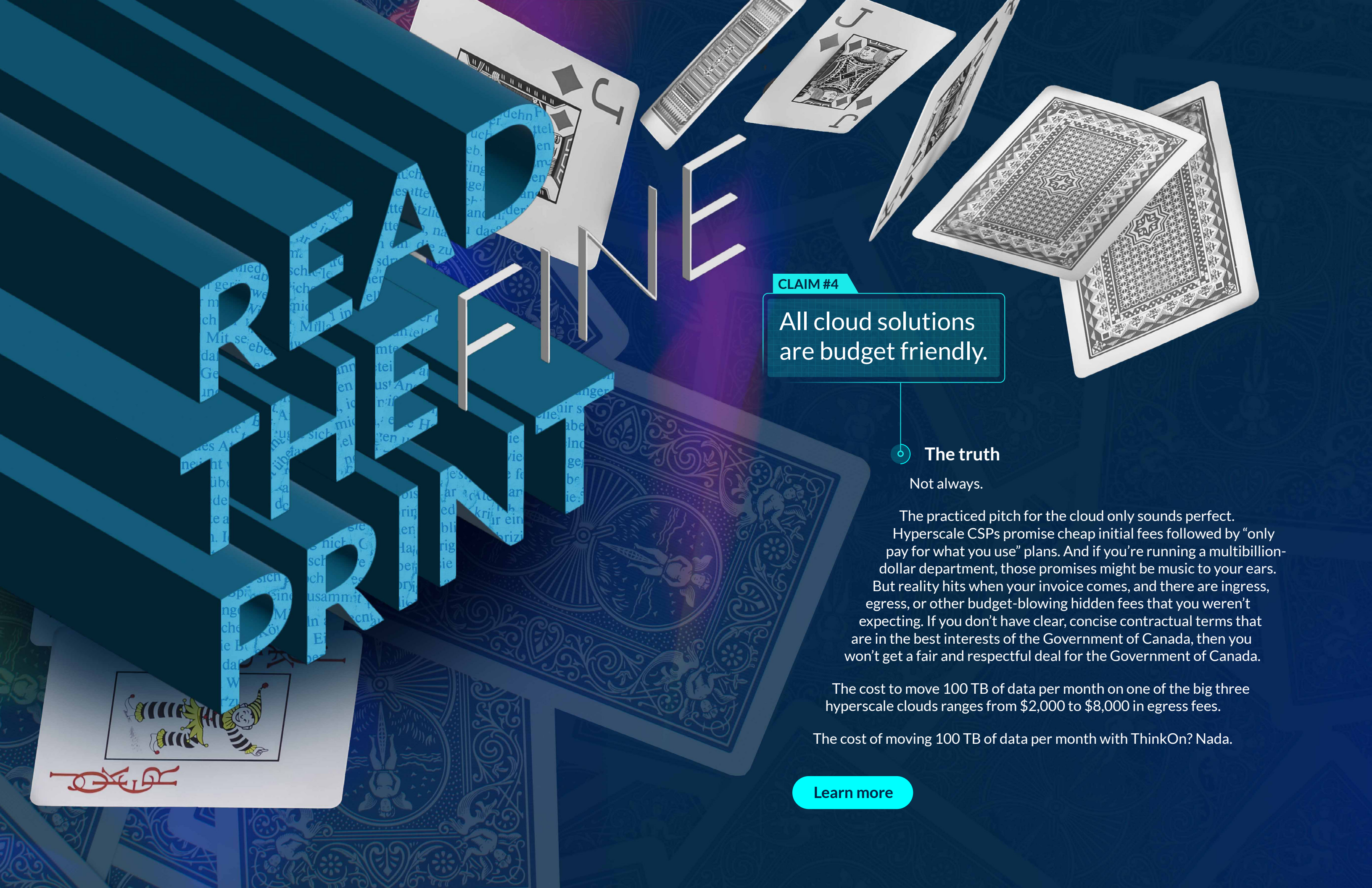
To understand your consumption and link it back to your costs, you need to have clear, transparent contractual relationships with your suppliers. This way, you don't get locked-in with a piece of technology unique to the cloud provider that you use, and you don't find yourself in a situation where you don't understand the contractual cost opportunities or obligations that you're committing to.

You need to have clear, concise contractual terms that respect the Government of Canada. We understand the [public sector and public sector workloads](#). Our expert Thinkers can help you evaluate your workloads and decide whether your application is cloud smart. We keep IT transformation simple and invoicing transparent.

[Learn more](#)

A FOOT IN

BOTH
WORLDS



CLAIM #4

All cloud solutions
are budget friendly.

The truth

Not always.

The practiced pitch for the cloud only sounds perfect. Hyperscale CSPs promise cheap initial fees followed by “only pay for what you use” plans. And if you’re running a multibillion-dollar department, those promises might be music to your ears. But reality hits when your invoice comes, and there are ingress, egress, or other budget-blowing hidden fees that you weren’t expecting. If you don’t have clear, concise contractual terms that are in the best interests of the Government of Canada, then you won’t get a fair and respectful deal for the Government of Canada.

The cost to move 100 TB of data per month on one of the big three hyperscale clouds ranges from \$2,000 to \$8,000 in egress fees.

The cost of moving 100 TB of data per month with ThinkOn? Nada.

Learn more





Welcome to the HOTEL CALIFORNIA

ONCE YOU'RE IN, IT'S HARD TO LEAVE

The truth

It's like Hotel California. Checking in is easy. But, once you're in, it's hard to leave.

So, what happens when the government decides—at the budget level—to no longer fund a particular program? Instead of being able to repatriate your data or turn it off, you can't easily extricate yourself and your data is stuck. There's no concept of those exit terms in most cloud agreements because ultimately, public cloud contracts are designed to retain customers and not make it easy to leave.

CLAIM #5

You can come and go from the cloud as you please and with ease.

One way they trap you is through charges. They're called egress fees, and they can be incredibly punitive. And the irony? The longer you're a consumer or the larger the consumer you are, the more data you have—and the more you have to pay to remove it.

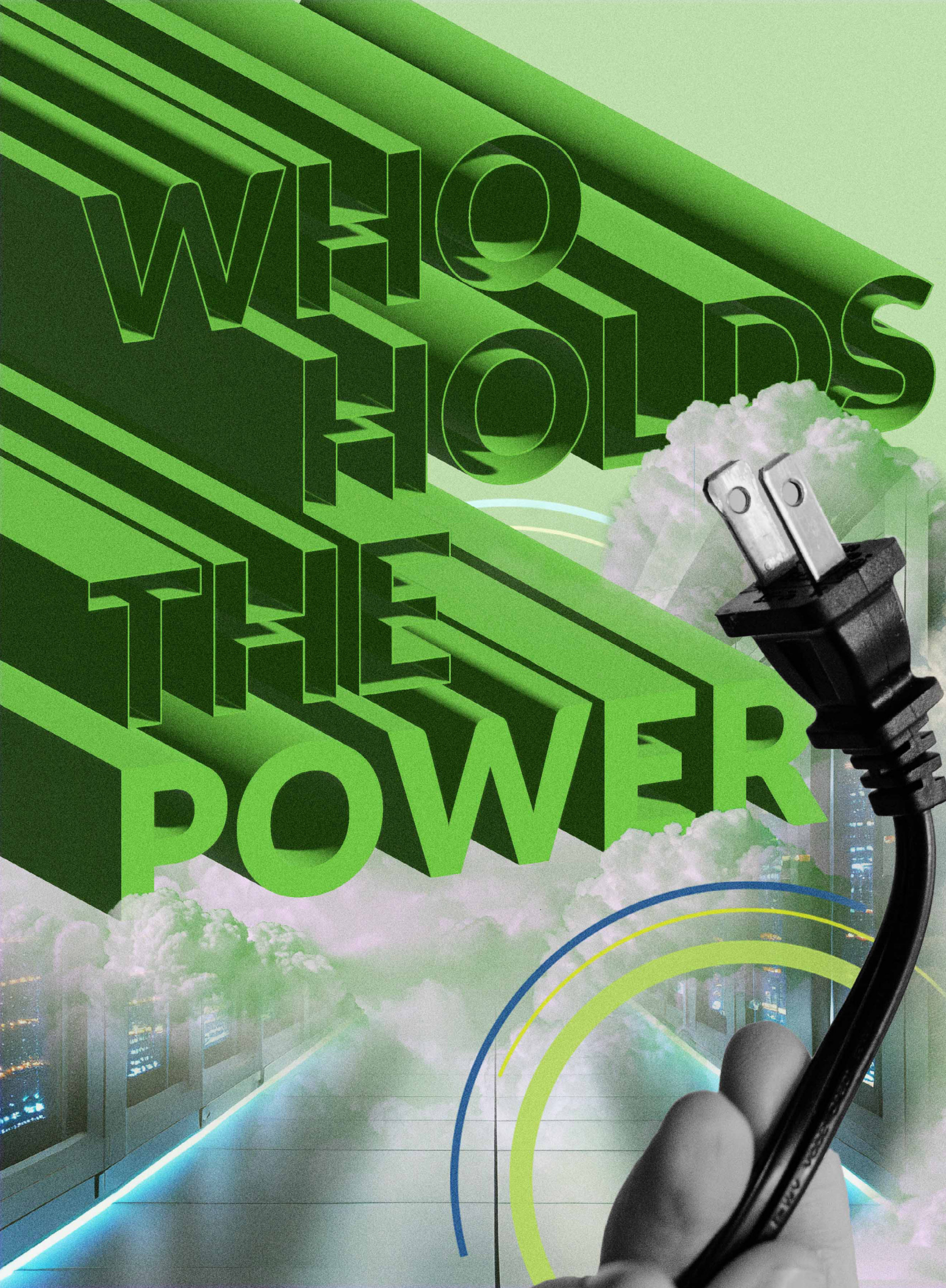
Another way you can get stuck in the cloud is due to workload repatriation challenges. Say you deploy a workload in a hyperscale cloud. Then, for any variety of reasons that are completely outside of your control (the budget has changed, or your allocation for this application has been reduced, or you no longer have a need for it) you want to repatriate it back onto Shared Services

infrastructure or perhaps end of life the application. The catch? If you're using features of the hyper-cloud that you can't move back in-house, then you can't repatriate the workload.

Whether it's due to prohibitive costs or application restrictions, you find yourself locked into the vendor—able to check in, but never leave.

With ThinkOn, you're free to come and go (even though we know you'll want to stay!). And, with transparent pricing and no egress or other hidden fees, we don't hold your data for ransom.

[Learn more](#)



CLAIM #6

The hyperscale cloud representative you're dealing with has the power to negotiate a contract with you.

The truth

Far too often, organizations find themselves negotiating with representatives who do not have the power to settle on terms.

It's important to understand that foreign-owned cloud operators keep tight control over contractual commitments. So, when the public sector in Canada negotiates with people who present themselves as cloud vendor representatives, they are often talking to people that don't have the ability to execute contracts or negotiate terms—stakeholders that aren't really dealing in the day-to-day—and the whole deal ends up having to go back and forth across the border.

At ThinkOn, our team is empowered to talk terms.

[Meet the team](#)

CLAIM #7

All clouds are created equally.

We deliver reliable, affordable, high-security solutions that help you balance tight budgets and mitigate skilled IT talent shortages. We're the only CSP capable of offering sovereign cloud to the Government of Canada. Our services are built on a model that puts simplicity first, with no-surprise billing, no fees (ingress, egress or otherwise), and no vendor lock-in. We are a trusted partner who understands public sector needs and the critical nature of data supply chain protection for Canada's future.

We aren't a hyperscale CSP, and we're proud of it. Learn about what makes us stand out from the crowd.

[Learn more](#)

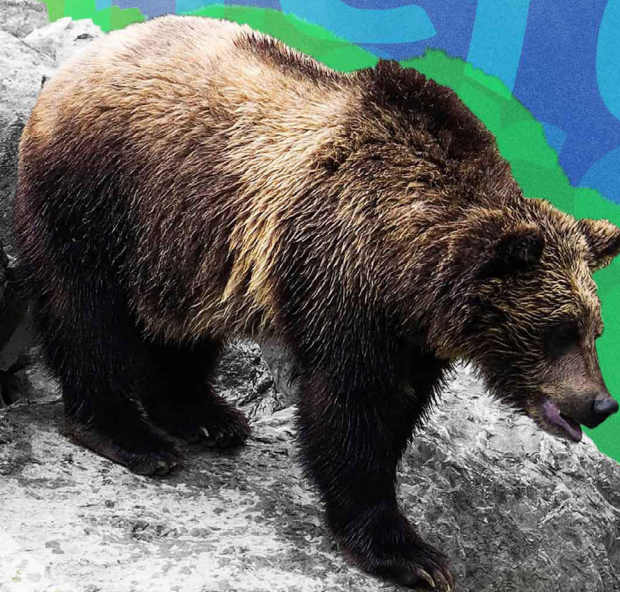
The truth

Over 90% of public sector workloads are built on VMware hypervisor technology. This means that ThinkOn's cloud infrastructure, also built on VMware [technology](#), allows for seamless migration of existing investments, as well as application modernization options for existing legacy IT environments. Our goal? [Simple, straightforward migrations.](#)

VMware recognizes ThinkOn as a [Canadian VMware Sovereign Cloud partner](#). The VMware Sovereign Cloud initiative helps customers engage with trusted national CSPs to meet geo-specific requirements around data sovereignty and jurisdictional control.

The ThinkOn

Difference



A woman with long brown hair, seen from behind, holds a large Canadian flag. She is standing in front of a dark, misty mountain range. In the top left corner, there are large, vibrant red maple leaves. On the right side of the image, the tall, stone clock tower of the Parliament Hill in Ottawa is visible, topped with a Canadian flag. The overall scene is atmospheric and patriotic.

A Canadian

Triple Threat

ThinkOn is where government and public sector data thrives.

We are the only Canadian supplier with the contractual capability to sell cloud-based data management services to support both Federal Government Sensitive (PBMM) workloads as well as workloads from all levels of municipal, federal, and Indigenous government public sector entities in Canada—from healthcare and education to defense and policing.

Canadian data needs a made-in-Canada solution. That's why you need ThinkOn. We're Canadian owned and operated, headquartered in Canada, with data managed by Canadians for Canadians.

That's a lot of Canada...the perfect amount for your Canadian data. Think true north for your data—with ThinkOn.

Reach out. Let's talk.