AN F12.NET WHITEPAPER

Sovereign Cloud 101

HOW EMERGING CLOUD STRATEGIES SIMPLIFY COMPLIANCE, INCREASE CONTROL AND REDUCE JURISDICTIONAL EXPOSURE

CONTENTS

What is the sovereign cloud?

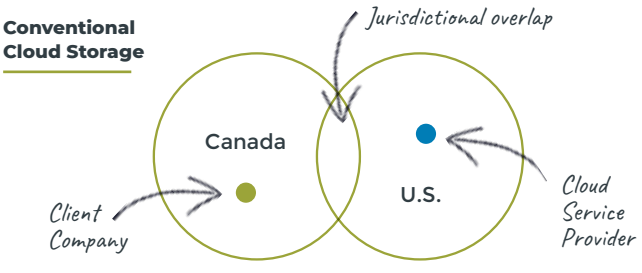
A sovereign cloud solution is just like a conventional cloud service, in the sense that it hosts services and stores your data on servers at a networked location that provides you with secure and resilient access from anywhere with a connection to the internet.

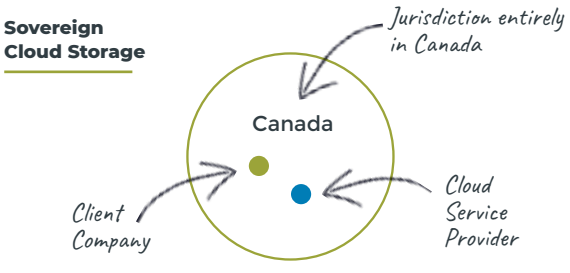
A sovereign cloud has one important difference, however: All aspects of the cloud service, from the physical location of the data to the legal incorporation of the company managing the services, are within the boundaries of a single nation-state. In the case of F12's sovereign-cloud solution, that nation-state is Canada–one of the most stable, least corrupt, and most secure countries in the world.

A Canadian sovereign cloud solution means that your data is protected by Canadian privacy and data protection laws, and is not accessible by foreign governments or any other external entities, such as the United States, China, or Russia, without due process of Canadian law.

To understand how a sovereign cloud is different from more traditional cloud services, think of your data as a filing cabinet full of sensitive documents. If you opt for a sovereign cloud strategy, that filing cabinet stays in Canada in a warehouse (a data centre full of servers, actually) managed by a Canadian storage provider, like F12. That way, it stays protected by Canadian privacy regulations.

In a traditional cloud arrangement, you likely would entrust that filing cabinet to a U.S.-based cloud provider–who may actually keep it in a warehouse in Canada. Trouble is, by keeping that filing cabinet under the care of a U.S. company, you're exposing your data to the jurisdiction of the US. Recent law has clarified that data residency no longer implies data sovereignty.





Why should I care about data sovereignty?

First, you should know that a sovereign cloud solution can be as secure, accessible, reliable, backed-up, and efficient as public-cloud solutions—while also providing you with the confidence that a foreign government cannot force access to the data stored inside.

That's because a sovereign cloud is a mechanism for storing data that is bound exclusively by the laws of a single national territory. For example, a cloud solution that is sovereign to Canada is structured so that it is bound exclusively by Canadian data privacy laws.

Because F12's sovereign cloud solution meets Canadian data residency and sovereignty requirements, the information it contains is not accessible to regulators or law enforcement from foreign territories without going through normal extradition channels.

At its heart, a sovereign cloud solution provides its users with confidence on four separate matters:

The data remains resident only within the chosen jurisdiction

- The data is subject only to the laws of its resident country
- The data centre services are managed by citizens of the resident country
- Other nations are not able to access that data

Why do I need a sovereign cloud solution?

As Canadian law evolves to reflect the state of the art in data security and digital privacy, the physical location of proprietary information will become an important consideration—one that, for certain classes of data, could be required by Canadian regulators to be stored on sovereign soil.

The Personal Information Protection and Electronic Documents Act (PIPEDA) already invests Canadian organizations with the responsibility of protecting the information they collect to operate. To be certain of data sovereignty compliance, privacy officers should consider employing a Canadian sovereign-cloud solution for their sensitive information.

Those in highly regulated industries, such as defense contractors and aerospace engineering, may need to certify that their sensitive data is managed exclusively within Canada by identifiable Canadian citizens. Sovereign Cloud services simplify such compliance.

Another important consideration is that U.S. law enforcement and regulators are able to access, by request, the information stored with American cloud providers. That is true regardless of where the data is actually stored. It also is true regardless of where the client—the nominal owner of the data in question—is legally incorporated.

That means U.S. providers of cloud storage, such as Microsoft Azure, Amazon Web Services, Google Cloud Platform, Oracle Cloud, and IBM Cloud, could be legally bound to provide data access to American authorities, such as the Federal Bureau of Investigation, the Securities and Exchange Commission, or the Internal Revenue Service. What's more, the authorities are able to access that data without even notifying the data owners.

More broadly, when you store your data with a U.S.- or foreign-based provider of cloud storage, that data is bound by a set of laws that are different from the laws where you are legally incorporated. That fact has important privacy implications.

For example, information that belongs to Canadian corporations, which are stored with U.S.-based cloud providers, do not have the same privacy protections accorded to U.S.-based companies. They're not protected by the Fourth Amendment, which bars unreasonable government searches and seizures. Nor do they have the same privacy rights.

By choosing to store sensitive information with a U.S.-sovereign provider, or a provider from any foreign nation, you may complicate your jurisdictional exposure to foreign law enforcement, regulators, or other actors. And under Canadian privacy law, you could potentially be held liable for the consequences.

Ultimately, conventional cloud storage clients should operate under the assumption that their data, as well as the data of their customers, will be accessible to foreign authorities, should they wish to review it.

Think of the most sensitive information that your business operations require you to store. It may be the financial history of client corporations, proprietary business strategies or intellectual property on which your entire business model is based. Are you comfortable knowing that the information could be disclosed to foreign actors bound by the laws of a different nation?

What are the advantages of using a Sovereign Cloud approach?

Laws regarding personal and proprietary information are becoming more strict. Organizations are responsible for protecting the information they collect from Canadians, and regulators could hold your company to account, leaving you liable if that information is exposed or abused by a foreign nation, or anyone else. Consequently, many different types of businesses would benefit from storing at least some of their data on a sovereign cloud, including organizations from such sectors as:

- Defence contractors – Could have confidential national-security intelligence
- Technology startups –Business model based on proprietary intellectual property
- Financial firms – Sensitive client data, information that could affect client share prices
- Legal partnerships – Client data protected by legal privilege
- Health care – Client data related to medical histories
- Insurance firms – Private medical and other information
- Cross-border trade – Client data legal in host nation that contravenes rules in foreign jurisdictions
- Pension and hedge funds – Information that could affect public markets

Can't I just ask my U.S. cloud storage provider to host my data on a server located in Canada?

No, is the short answer. And listen, we get it. Many businesses haven't thought much about the details of their data. They know it is in the cloud. So long as that data is adequately backed up, and secure from bad actors, and the client can access it when they feel like, few organizations devote much consideration to where it is, or what is happening to it.

It's in the cloud. It's accessible 24/7 on a few milliseconds' notice. Who cares where it's really located?

Maybe that attitude used to make sense. But that all changed with a U.S. federal law called the 2018 Clarifying Lawful Overseas Use of Data Act. Better known as the CLOUD Act, the legislation allows American federal law enforcement to force the country's technology companies–including, you guessed it, Microsoft Azure, Amazon Web Services or

Google Cloud Platform—to provide access to data stored on their servers, on request, regardless of where the data is physically located.

For example, let's say that you have sensitive data stored on the cloud through a U.S. provider. You may not have any idea where your data is physically located on a server's hard disk. But let's say that server is situated in Canada. U.S. law enforcement is likely to be able to force access to it purely by virtue of the managing authority being an American corporation. You also may leave it exposed to surveillance by foreign intelligence organizations.

Best Practices for moving your corporate data to a Sovereign Cloud Ecosystem

Probably not. Recent emails are probably fine to leave on your existing public cloud solution, if you provide guidance to your employees to be cautious about the information they're sharing in electronic communications.

The best-in-class approach today is a multi-cloud solution, a combination that can include public clouds, private clouds, and sovereign clouds. The multi-cloud approach raises the question, what data belongs on a sovereign cloud? And what data is fine to leave on a public cloud? ("Public cloud" is a term that describes web-accessible data storage solutions, such as Amazon Web Services, Microsoft Azure and others. Despite the possibly misleading name, the stored data is secure, and not accessible by members of the general public.)

At F12 we advise our clients to carry out an enterprise risk management process that assesses the implications, should each data category become public, or exposed to foreign authorities. Sometimes, this process would result in enterprise resource planning (ERP) data or other financial records being hosted on a sovereign cloud. Organizations should consider storing sensitive client information in a sovereign cloud if their clients are concerned about data sovereignty or wish to limit their jurisdictional or regulatory exposure.

Case Studies

Sovereign Cloud Use Case #1

OPPORTUNITY

A Canadian law firm specializes in litigating trade disputes, sometimes against American government organizations. The law firm's discovery process often collects depositions that disclose sensitive information. In addition, the law firm hopes to build a business representing foreign nation-states before international trade tribunals—and the foreign governments have strict requirements for data residency from their legal representations.

SOLUTION

Switching from Rackspace to F12's Canadian Sovereign Cloud solution kept the law firm's data secure from compelled discovery by foreign states.

Sovereign Cloud Use Case #2

OPPORTUNITY

A Canadian company that is developing self-driving trucking technology has spent years building a large database of driving interactions that artificial intelligence algorithms must analyze to improve the on-road behaviour of its autonomous vehicles. The company's largest competitor is a Chinese firm, and the CTO worries that a public cloud solution could inadvertently store data in a server farm on the Chinese mainland, providing access to bad actors intent on corporate espionage.

SOLUTION

Relocating sensitive intellectual property from AWS to F12's Sovereign Cloud added protection against industrial espionage from any nation.

Sovereign Cloud Use Case #3

OPPORTUNITY

The United States bars its citizens from visiting Cuba, as well as doing business with Cuban companies. It also makes things difficult for foreign companies that aim to do business both with the U.S. and Cuba. So when a Calgary oil and gas executive saw an opportunity to provide ongoing services to a Havana refinery, he wanted to be sure that the new deal wouldn't endanger his existing relationships with Houston and Dallas.

His first step was to incorporate a new business entity, solely to trade with Cuba, then operate that at arm's length from his existing venture. What else, he wondered, could he do to ensure that his equipment could be sold both to Havana and Houston?

SOLUTION

Moving the ERP systems from Microsoft Azure to F12's Canadian Sovereign Cloud provided the oil and gas executive with confidence that he minimized risk to both his business lines.

Client Testimonial

One F12 client that has adopted our cloud sovereignty service is VantageOne, a credit union in the interior of British Columbia with approximately 1,400 commercial clients among their account holders. Glenn Benischek is VantageOne's CEO and president. He says the decision to pursue a sovereign cloud strategy came down to risk management.

Like any financial services firm, the credit union has been entrusted by its members with confidential data, such as their names, occupations, credit scores, and financial histories—and much more. "The data we hold on our member base is significant," Benischek says. "Making sure that data is housed in a nation that follows the same laws that we are governed by—that's important to us."

After all, Benischek says, many nations have altered the regulations that govern data privacy, and those changes can have troubling consequences for companies that are based in other jurisdictions. Heads of governments can change, political parties can exchange power and global events can create major swings in regulatory philosophies, which can in turn affect disclosure regulations.

It was one of these legislative changes that first prompted VantageOne to pursue its data sovereignty strategy more than 20 years ago. The World Trade Center disaster had just happened, and two months later the Bush administration passed the PATRIOT Act. While the legislation was intended to fight global terrorism, it also radically rewrote disclosure regulations and provided U.S. law enforcement with access to far more financial information than they had previously.

"That made us think about where our data is stored globally," Benischek recalls. "And what changes could happen in laws that would give government entities the right to have access to that information. That's where it came into focus for us—that we'd like to have our data stored in our sovereign country."

Cloud sovereignty also helps VantageOne stay in compliance with the spirit of Canadian banking regulations. "We're in a highly regulated industry—the financial sector," notes Bensichek. Canadian regulators ask questions around many different aspects of the credit union business, including data integrity, data governance, data storage, and geographic exposure. For example, Benischek says, they'll ask, "What systems are you using? Where's the data stored? Have you done a risk assessment on your data suppliers?"

In each case, VantageOne's cloud sovereignty strategy assures the credit union's numerous different stakeholders that the credit union is being thoughtful about how it manages its data, and its overall approach to risk management. "Reduce a risk—that's what it does," says the credit union CEO. "The idea is to ensure that our data is as protected as possible."

The Wrap Up

As data privacy regulations evolve, regulators are holding organizations accountable to secure their client data. Traditional cloud storage solutions can expose sensitive information to foreign actors. F12's sovereign cloud strategy provides you with the reassurance that your data stays physically located on Canadian soil, and protected by Canadian privacy regulations.

Seeking to learn more about how cloud sovereignty solutions can help your company? Contact F12 to discuss options.

Background on the CLOUD Act

The need for cloud sovereignty dates back a decade, to 2013, when law enforcement in New York was conducting a drug trafficking investigation. The police wanted access to certain emails managed by Microsoft. The problem, at least for law enforcement, was that the emails were located at Microsoft's enormous data centre in Dublin, Ireland. And Microsoft declined to allow the police to access them, because, they said, the U.S. police had no jurisdiction over those servers. A U.S. magistrate issued a warrant requiring the Seattle company to produce them anyway. Microsoft appealed, and the case went all the way to the U.S. Supreme Court. But before the justices could deliver their decision, the U.S. Congress passed the CLOUD Act in 2018, rendering the original legal dispute moot. The CLOUD Act enabled U.S. law enforcement and regulators to access information stored by U.S.-based organizations, regardless of where that data is physically located.

F12.net™

sales@f12.net 1-886-F12-8782 f12.net

ALBERTA • Calgary | Edmonton | Red Deer
BRITISH COLUMBIA • Courtenay | Nelson | Vancouver | Vernon | Victoria
ONTARIO • Toronto | Vaughan | Waterloo