Technology Brief

Data Sovereignty & Privacy Protection

Data Sovereignty: A Privacy Protection Pillar

ThinkOn and Intel are helping managed service providers, businesses, and government organizations protect data and comply with privacy regulations

ThinkOn

Introduction

Data has value today and retains that value for years in the future. It needs to be protected throughout its lifecycle, which can be a challenge since different countries have different rules governing data. That's why data sovereignty matters.

Data's Longevity Presents Protection Challenges

The value of data is continually increasing for businesses that are generating more and more data every second. At the same time, the lifecycle of data is being extended. Too often, companies aren't immediately aware that data has been stolen, and issues are compounded when that stolen data ends up in the hands of people outside of the local jurisdictional control and regulatory frameworks.

> "Storing data on servers in geographic locations across Canada provides redundancy and is effectively considered a global main state."
>
> **— Craig McLellan**
> ThinkOn Founder and CEO

The challenge is to ensure data is not only protected, but that it is handled in accordance with Canadian law and local privacy regulations, while remaining within the control of a business. Risks increase when that data is stored and accessed on server infrastructure beyond national borders or on infrastructure managed by foreign parties.

"As Canadians, we are very trusting people, but we can't predict what the next 10 years will bring," says ThinkOn Founder and CEO, Craig McLellan. "If we are storing data, both real data and metadata, for 10 years, or frankly forever, it is just too much risk to store that data where I don't have jurisdictional and regulatory control. Too often, we treat data with a short-term focus."

Solution: Canadian Data Sovereignty Matters

What does it take to help businesses adhere to privacy rules while safeguarding data? A multi-layered approach that includes data sovereignty is the key.

Managed service providers (MSPs) and IT leaders should discuss data sovereignty whether the company is a public sector-facing organization or not. The protection offered by sovereign cloud solutions is far-reaching and helps to give companies greater control over their data and how it is used.

"Every morning, I wake up with the exact same interests as every other Canadian; I want Canada to do well. A lot of businesses and a lot of public sector entities want to work with someone they will be able to 'control' or regulate without any ramifications of cross-border problems," McLellan says.

"Storing data on servers in geographic locations across Canada provides redundancy and is effectively considered a global main state. It gives us, as Canadians, a cloud option from a company that lives by the same laws and probably the same values that you have. It's a good place to start building a more secure and sovereign solution for data," he adds.

Cloud Simplicity without Security Compromise

Corporate boundaries are getting blurred in a world where people can work from anywhere. At the same time, the amount of data is increasing and the time that data has value is getting longer.

"There are two kinds of data – time-sensitive data that could have an immediate impact on our business and the data that has forever business implications – data that is completely comfortable sitting at rest today can end up in the hands of a bad actor in five years and be used against me," says McLellan.

MSPs and IT leaders can help businesses take a more strategic approach to their data and storage requirements, especially with the pervasiveness of cloud computing. This means understanding and helping to explain the risks associated with how and where data is stored.

> "There are two kinds of data – time-sensitive data that could have an immediate impact on our business and the data that has forever business implications."

According to ThinkOn, all data strategies should consider:

- **Who is in control?** Every country can define laws for how data is to be used and, in many countries, those laws are very broad. Without knowing the specifics about how countries will deal with other countries, "it is carte blanche. They can do what they want, and the thing is you don't know what they will do," says McLellan.
- **How is data being used?** Laws and rules defined by each country specify how data and metadata can be used – and it might not be the way you want it used, or it might run contrary to your corporate values, but you are not in control of it.
- **What rules apply?** Unfortunately, legislative frameworks for privacy and data protection haven't been fully tested in the courts and, when data is stored outside Canada, companies will have to navigate a foreign legal framework.

"Today is not the issue, but we don't know what it looks like in 2025. Bad actors are stealing data today, that they are looking to decrypt and use against us 10 years from now," says McLellan. "That's the double challenge of having this long tail of data retention, and that data is potentially accessible in a foreign country that does not adhere to the same values as Canada."

Built on a Secure Foundation

VMware named ThinkOn to its Sovereign Cloud Initiative, which helps customers engage with trusted national cloud service providers to meet geo-specific requirements around data sovereignty and jurisdictional control; access and integrity; security and compliance; independence; and mobility, analytics, and innovation.

"Providing high levels of security are 'table stakes' for any data centre and sovereign data solution," says McLellan. ThinkOn standardizes on Intel® Xeon® Scalable processors, including 3rd Gen Intel Xeon Scalable processors.

"We have been exclusively Intel on the compute side since the beginning of time," says McLellan. "That's table stakes for us. We feel Intel-based hardware is an important foundation for us because it gives us flexibility and security."

The 3rd Gen Intel Xeon Scalable platform is optimized for cloud environments. It offers a balanced architecture with built-in acceleration and advanced security capabilities that support most in-demand workloads and a range of XaaS solutions.

Intel® Xeon® Scalable Processors Have Built-in Security

The security features of the latest generation of Intel Xeon Scalable processors include:

- Intel® Software Guard Extensions (Intel® SGX) provides fine-grain data and privacy protection via application isolation in memory, independent of the OS or hardware configuration.
- Intel® Crypto Acceleration brings built-in Vector AES-NI, Vector CLMUL, Intel® Secure Hash Algorithm Extensions, VPMADD52 instructions, and RSA/DH encryption protocols.
- Intel® Trusted Execution Technology (Intel® TXT) helps attest that the BIOS, OS, and hypervisor haven't been tampered with.
- Technology that provides platform-based hardware acceleration for cryptography and data compression.
- Intel® Total Memory Encryption for full physical memory encryption support to enhance data and VM protection.
- Intel® Platform Firmware Resilience (Intel® PFR) uses an Intel® FPGA to protect, detect, and correct, providing NIST SP800-193 compliant firmware resiliency. Now, platform firmware can be validated before execution, while runtime monitoring and filtering help protect against manipulation. In case of a compromise, Intel PFR provides automated recovery in minutes.

In a world where businesses are working globally, data security and protection challenges are heightened.

High-Performance Data and Storage

ThinkOn has also tapped Intel to help manage storage for its customers' growing volumes of data with Intel® Optane™ technology.

"Memory is becoming a very important part of our business and our customers' business. They want to consolidate data into fewer databases, so Intel Optane technology gives us the ability to offer very large, high-performing databases," says McLellan.

Intel Optane technology establishes new tiers in the memory and storage hierarchy, providing persistent memory, volatile memory, and persistent storage in multiple form factors. Intel Optane SSDs and 3D NAND SSDs extend storage performance and capacity, consolidate storage resources, and boost VM density.

The solution helps increase capacity and performance in a data-centric world.

Intel® Optane™ Technology

Optimize, store, and move larger, more complicated data sets with Intel Optane technology. This innovation helps to bridge critical gaps in the storage and memory hierarchy to deliver persistent memory, large memory pools, fast caching, and fast storage.

Intel combines the Intel® Xeon® Scalable processor platform with flexible Intel Optane products – like Intel Optane persistent memory and Intel Optane SSDs – to deliver solutions that increase overall performance.

Security and Privacy Protection in a Hybrid World

Canada has similar views to Europe's General Data Protection Regulation (GDPR) for privacy protection and monetization of data. New regulations in Canada are promising to further heighten privacy protection for consumers and businesses.

"Companies and people want control over their data and its derivative works, which is supportable, defensible, and even more importantly, legally respected when you are dealing under the umbrella of a sovereign nation. You start to question your legal protections and ability to protect your data when it's in another country," explains McLellan, adding, "jurisdictional control has not yet been tested in the courts."

In a world where businesses are working globally, data security and protection challenges are heightened. McLellan notes that the minute a laptop containing data crosses a border, the laws of that region now apply.

"When people are working anywhere, there are two key things to consider – does the 'anywhere' still adhere to the same jurisdictional oversight and are we comfortable with the employee working the same way in that region," he says, noting when you have employees with operational responsibilities working remotely, you are expanding the attack surface of the company.

In 2021, the average cost of a data breach in Canada was $5.35 million[1] per incident (up from $4.24 million in 2020) and the cost of a breach was $1 million more on average[1] when remote work was a factor.

"The rules that govern data change depending on where that data resides," says McLellan. "Reporting data breaches in Canada is mandatory. Companies that fail to report a breach could be fined up to $100,000.[2]"

VDI – A Solution to the Problem

"Virtual desktop infrastructure (VDI) was a solution looking for a problem for many years and I think it has finally found it. The work-from-anywhere future requires a more secure way to control and protect data access," says McLellan. "Anyone coming into a VDI session is considered an untrusted guest until they are authenticated with multifactor authentication."

Rather than running everything locally on an employee's PC, which can put data at risk, VDI runs on a centrally controlled, secure, and sovereign server infrastructure to provide security improvements. If an endpoint device is stolen, there's no sensitive data in its local storage.

"We are going to start using VDI technology exclusively for remote employees. I would say in two years we'll see 90 percent VDI utilization because inside the VDI environment I can apply much higher levels of control," predicts McLellan. Adding VDI makes deploying zero-trust agents across thousands of devices much more viable.

ThinkOn's model for governments and MSPs who want to offer customers secure solutions requires every administrator to enter a secure VDI session so they can guarantee no data ever passes to the laptop accessing the session. "I see this air-gap mentality becoming more and more relevant as we grow as a nation of data users because the threats are continuing to get more sophisticated," he says.

Homomorphic Computing is Coming

With an eye towards constantly pushing the possibilities for computing and security, ThinkOn is currently building what McLellan describes as "the world's first, fully homomorphic encrypted data repository."

McLellan explains that fully homomorphic encryption isn't hackable quantum computing, and is an ultra-secure repository. It will allow companies to make queries against the stored data for machine learning and AI training applications without ever decrypting the datasets.

"Imagine a future when customers can store their data for the long term, but we are indexing it and putting that data into a full homomorphic computing environment so it's searchable without being disclosable. This is the other edge of innovation," says McLellan.

ThinkOn is building its homomorphic computing environment on the Intel® Xeon® Platinum 8380 processor with Intel Crypto Acceleration, built-in AI acceleration, and Intel SGX, as well as next-generation Intel® Optane™ SSD P5800X. This environment will leverage the Intel® Homomorphic Encryption Toolkit and Intel® Homomorphic Encryption Acceleration Library (HEXL), designed to offer Intel® AVX-512-optimized environments with commonly used lattice-based homomorphic encryption libraries.

"We are using Intel technologies for this project because we think Intel has a better strategy around the math needed for fully homomorphic encryption," McLellan says.

Learn More

You may also find the following resources useful:

- Intel Xeon Scalable Processors
- Intel Homomorphic Encryption Toolkit
- Intel Optane SSD
- ThinkOn Joins VMware Sovereign Cloud Initiative
- Secure and Sovereign Canadian Cloud

About ThinkOn

ThinkOn Inc is an industry leader in Canadian cloud security standards. The company solves complex data problems with its portfolio of turnkey cloud Infrastructure-as-a-Service (IaaS) solutions. ThinkOn was recently named the first VMware Sovereign Cloud Initiative partner in Canada, and its channel-only distribution model empowers over 150 value-add resellers and MSPs worldwide.

Solution Provided By:

[1] "Average cost of a data breach still rising, says IBM study," IT World Canada, July 28, 2021.

[2] "Data Breaches In Canada: Reporting Obligations, Class Actions And Breach Management," Gowling, June 2017.