portfolio

BANKING on a *VIRTUAL PRIVATE* CLOUD

DEMYSTIFYING ***CLOUD SECURITY*** & ***EMBRACING INNOVATION*** IN BANKING

CONTENTS

ARE WE THERE YET?

From Cloud Adoption to Open Banking, the Industry Is Unmistakably Moving Forward

Are we there yet? It's one of those cliché questions that we ask on our way to somewhere other than here. It's a question we ask when we're young and naïve, when our limited experiences have provided us with a flawed sense of time, and we're simply left grasping at a clear but still imperfect idea of where we're going. It's funny, isn't it? It's a question we ask when we already know the answer, but we ask it, anyway. Like a child on a trip across the country, we're taking in the scenery and building new experiences that are actively transforming what we once imagined into what is now suddenly becoming real. *Are we there yet?* It's a question that implies anticipation and an underlying excitement, saying at the same time, I can't wait to be there. We look out the window at the passing trees, up at the wispy clouds. It's not a question that we ask at the start of our journey, but one we ask when we're already well on our way. A question we often ask more than once. *Are we there yet?* It says, *I know we're almost there. It's just a matter of time. So, how close are we?*

"As a collective whole, we're on our way to somewhere else, somewhere different, somewhere new."

In more ways than one, that's a perfect metaphor for the current banking industry in Canada. Whether it's the industry's recent accelerated adoption of cloud technologies,

the modernization and digital transformation initiatives that are essentially reshaping banks and their relationships with both consumers and technology, or even our industry's proposed shift to consumer-directed finance and its promise to redefine the cold and transactional nature of financial services by prioritizing financial experiences, we're unequivocally *in between things.*

We're on the move. We're going somewhere. As both individual elements and as a collective whole, we're on our way to somewhere else, somewhere different, somewhere new.

In terms of consumer-directed finance, that somewhere is a place we've seen in other parts of the world—we know it already exists and that it's possible—but it's a place we have yet to fully experience ourselves, and so we approach it with a careful balance of apprehension, optimism, and enthusiasm. In places like the United Kingdom, Europe, and Australia, financial industries have already adopted this new modern banking framework, one that's known outside of Canada as open banking. Driven by an unequal mix of legislative enablement and industry cooperation—and leveraging technologies like application programming interfaces (APIs) to facilitate integration between fintechs, third parties, and financial service providers—the open banking movement underscores the growing importance of consumer data rights, data ownership, and the belief that consumers should have the power to control their data.

"In more ways than one, that's a perfect metaphor for the current banking industry in Canada. (...) We're unequivocally *in between things*."

The increasing importance of consumer data rights is evident in the growing number of data and privacy regulations enacted in jurisdictions around the world, including the General Data Protection Regulation (GDPR) and the Second Payment Services Directive (PSD2) in both Europe and the UK, the Consumer Data Right (CDR) in Australia, and even the Consumer Privacy Protection Act that was initially proposed in Bill C-11 right here in Canada. Although that particular initiative may have fallen short, it's evidence that consumer data rights have become increasingly important and that there is a growing need for data privacy reform in Canada.

Are we there yet?

In addition to the shift toward open banking, the COVID-19 pandemic has changed the way banks operate, forcing entire workforces and business units to operate remotely, while also changing the way consumers bank both in Canada and around the world. It has forced targeted improvements in banking services, shifted focus from traditional strategic channels, and has unquestionably accelerated digital transformation in the industry. In many cases, it has compressed complex five-year technology plans into 12- to 18-month initiatives.

In some instances, those plans have even included what is considered to be a monumental shift to the cloud.

Although moving to the cloud is not a prerequisite for a financial institution's participation in open banking and consumer-directed finance, most banks

are finally considering a move to the cloud in order to leverage its many benefits and position themselves for the future. They have a clear but still imperfect picture of how the cloud can provide a more flexible technological foundation for the future of the industry—a place where real financial innovation is feasible, where banking infrastructure is scalable and adaptable, and where banks can respond to rising consumer expectations by bringing new products and new banking experiences to market quickly. The cloud offers banks a foundation for modernization, providing a cost-effective and modern infrastructure solution that can provide the responsiveness banks need to compete with cloud-native fintechs that can already move quickly to launch new and innovative banking experiences.

The cloud isn't exactly new, though. So, with its potential to lay the foundation for a financial institution's digital transformation and modernization, why haven't our largest banks embraced the cloud until now?

Prior to the pandemic, the Canadian banking industry was a place where technological change seemingly happened in slow, carefully calculated increments. Although there were some rare exceptions, innovation was arguably scarce. Where technology promised speed, innovation, and change, banks favoured safety, security, and stability at all costs. Striking a balance that embraced innovation wasn't necessary to achieve high revenue targets and healthy growth. With limited competition in the market, it was easy for banks to simply ask, *Why fix what isn't broken?*

Until now, it was easy to postpone investment in new technology for another quarter, another year, another time.

With a significant increase in fintech innovation, a better understanding of the value of personalized financial experiences, and rising consumer expectations pressuring banks to change—along with both the increased importance of data rights and the proposed adoption of open banking collectively pushing the industry forward—it's safe to say the leaders of our biggest banks today understand the value of investment in cloud technology in order to meet both the demands and the requirements of the future.

"In a post-pandemic world, one thing is now clear: Banks need the cloud. The challenge is how to get there safely and securely. . "

In a post-pandemic world, one thing is now clear: Banks need the cloud.

The challenge is how to get there safely and securely. While some banks are well on their way, others are still grappling with the complexities of cloud migration.

For one, migrating a bank onto the cloud is hard. It's complicated. It's expensive. It requires resources and planning and time. On top of that, moving systems that were never designed for the cloud onto a cloud environment

is a unique challenge in itself that introduces risk—not only risk to systems but also potential regulatory and compliance risk. Banks have strict requirements for how and where they store their data. When it comes to the cloud, any lack of clarity from regulators makes the transition that much more complicated.

The biggest obstacle, though, may be the most obvious one: Some leaders have a deeply rooted concern for cloud security in public cloud infrastructure. How do we keep data and systems safe on the public cloud? How can we trust a banking infrastructure that we can't see and touch? What methods and technologies will ensure that our data and systems remain secure?

Unlike a simple road trip across the country, it's fair to admit that our journey is much more complex. We're expected to go several places all at once and to be moving quickly and safely to our destinations, down different paths that aren't always clear. Still, we're moving forward. We're well on our way, but we're still somewhere in between. Without a doubt, removing a roadblock here and there or getting directions may help us arrive at our destination sooner.

"The biggest obstacle, though, may be the most obvious one: Some leaders have a deeply rooted concern for cloud security in public cloud infrastructure."

If we can address the most prominent concerns about cloud security for banks, maybe we can move one step closer to our destination—adopting technology that provides banks with a safe and secure foundation for consumer-directed finance and a platform to embrace innovation.

Are we there yet?

Not quite. Hang in there, though. We'll be there soon.

WHEN IT COMES TO BANKS & THE CLOUD, THERE'S A LOT AT STAKE

Canadian banks are leaders in cybersecurity. They work closely with other financial institutions, law enforcement officers, government officials, and industry regulators in an ongoing effort to monitor, detect, and prevent cybersecurity threats and cybercrime in the financial system. While they're occasionally criticized for their reluctance to adopt new technologies—relying on monolithic legacy systems and mainframes, falling behind on digital transformation efforts, and failing to meet the rising expectations of digital-natives and tech-savvy consumers—that's in no part due to a complete lack of investment in technology.

In fact, Canadian banks are known to invest heavily in their pre-existing systems in order to protect their technological infrastructures, consumer data, and the financial system itself from cybersecurity threats.

According to the Canadian Banker's Association, "Over the past decade (2009 – 2019), banks have spent $100 billion on technology, which includes technology dedicated to security measures." While that all-encompassing figure includes investment in all forms of technology, any investment in banking systems and infrastructure requires significant investment in cybersecurity efforts to ensure that those systems remain secure. That includes investment in everything from security enforcement controls to intrusion detection and prevention systems, as well as threat management solutions and the cybersecurity professionals themselves that actively maintain a bank's comprehensive security strategy.

"There is a major difference between a lack of investment in technology and a lack of innovation in technology,."

There is a major difference between a lack of investment in technology and a lack of innovation in technology, and it's the lack of meaningful technological innovation that is largely attributed to the common misconception that financial institutions have failed to invest in technology as a whole and, as a result, have fallen behind in our expectations on delivering better personalized digital banking experiences.

That misconception could soon change, but there's still a long journey ahead.

If financial institutions want to secure and build trust with the next generation of consumers and prove that traditional banks can deliver the personalized banking experiences that these consumers expect, they need to innovate. Things need to change. That doesn't mean banks shouldn't continue to protect their investments in core systems and technology; it simply means that they will need to invest in new ways of leveraging that technology. It's about modernization. Banks need the ability to move quickly to create innovative digital financial experiences that deliver value that is both educational and enhances the lives of consumers. In order to shift from providing traditional product-driven experiences to providing digital consumer-driven experiences, they need innovation, and innovation requires an infrastructure that is conducive to change.

There are major shifts happening in the financial services industry today. We're seeing a convergence and fusion of the tech and banking industries that have blurred the lines of banking. Partnerships between fintechs and banks have changed the way financial services are being delivered. More and more banks are turning to artificial intelligence, machine learning, and automation technology to provide new and efficient data-driven experiences, and application programming interfaces (APIs) are driving a paradigm shift in the industry. APIs are now connecting the industry in entirely new ways, leading to new integrated banking experiences and driving the emergence of financial ecosystems. Among the expectation to adopt new technologies that have the potential to drive innovation and change, banks are also expected to maintain the safety and security of their current infrastructure, while also continuously meeting rigorous compliance and regulatory requirements.

It's a challenging balancing act to manage.

While ongoing investment in technology is key to keeping systems safe and secure, investing in technology that drives innovation—what we'll call *investing in innovation*—has now become essential to long-term survival.

Banking leaders are aware that the industry is shifting in major ways and that transformational changes are required to meet the demands of the digital consumer. They must leverage new forms of technology and shift their businesses and cultures to embrace and promote innovation. While cloud solutions can provide that flexible, adaptable, and scalable foundation for the digital transformation and modernization banks require, banks must first confront the risks of migration and their often flawed, preconceived notions of cloud security.

Without question, the on-premises systems and infrastructures Canadian banks have built are incredibly secure, and the level of security our financial institutions have maintained over decades of operations have contributed to the level of trust we have in our banks and our financial system. That's important to acknowledge because when it comes to moving banking systems, workloads, business processes, applications, and consumer data onto the cloud, there's certainly a lot at stake.

IS THE PUBLIC CLOUD SAFE FOR BANKS?

It's often the first and most pressing question that banking leaders and their teams must face: Is the public cloud safe for mission-critical banking systems? In order to leverage all the benefits of a flexible cloud banking infrastructure and embrace a technological foundation that promotes innovation, banks must first be willing to move those reliable, trusted, and secure on-premises systems onto the cloud. Not only is that an incredibly complex undertaking that requires investment, specialized skills and expertise, migration planning, and additional resources, but it means banks must also be willing to trust a third-party cloud service provider with things like data storage, data privacy, resiliency, and—that's right—cloud security.

That's a lot to ask.

"While trust is important, it won't keep your data, applications, workloads, and systems secure."

With the banking industry's strict regulatory and compliance requirements—along with important considerations regarding data residency and data sovereignty—moving banking systems and applications that store and process the sensitive financial data of thousands of customers requires careful consideration.

When it comes to the cloud, security and compliance becomes a shared responsibility. While trust is important, it won't keep your

data, applications, workloads, and systems secure. So, when considering whether a cloud service provider is safe, it's often best to simply focus on the underlying cloud security technologies, systems, tools, and methods that will be used in a securing a financial institution's cloud-based infrastructure.

When you understand how cloud security technologies, systems, tools, and methods work together collectively to prevent cyber threats like data leaks, data loss, unauthorized access, malicious behaviour, service disruptions, malware, and theft, you can begin to establish confidence in cloud security on a tactical level. That approach will allow you to build confidence in the underlying cloud security technologies and practices. If you can establish confidence in the underlying technologies and practices that keeps banking infrastructure safe on the cloud, then you'll have a solid foundation for building trust in a cloud service provider.

Surprisingly, establishing that trust with a public cloud service provider might not be as hard as you think.

Many banks will find that the technologies, tools, and methods that are used to secure banking systems and data on the cloud today are often the same kinds of technologies, tools, and methods used to keep their current banking systems safe and secure.

What's the difference? One significant difference is that cloud service providers are always using the latest cloud security techniques and technologies, and they're consistently investing billions of dollars each year to ensure that their cloud computing platforms are always meeting the highest standards of privacy and security. Their core business is essentially to keep systems and data secure. On any given day, cloud service providers are thwarting over a million attempts to compromise their systems, and they're collecting data and information from those attempted attacks to continuously build intelligence around new, existing, and potential threats. They're even leveraging the intelligence gained from those attempts and applying it to protect other customers on the cloud.

Like how the human body learns how to fight off viruses through exposure, cloud service providers learn from attempts to compromise their systems to build and strengthen what is essentially an immune system of cybersecurity.

By moving their systems onto the cloud, banks are no longer forced to simply rely on their own internal cybersecurity tools and practices. On the cloud, they can leverage a cloud service provider's ongoing investment in security and take advantage of the sophisticated intelligence and cloud security solutions that are created and maintained by world-class cloud security experts.

Technologies and tools used to secure banking systems and data on the cloud can include advanced security enforcement controls, like next-generation firewalls (NGFWs); obfuscation technologies, like encryption and cloud-based tokenization; secure authorization protocols, like OAuth 2.0; intrusion prevention systems (IPS) and intrusion detection systems (IDS), like real-time threat-detection monitoring and alerting solutions; and secure communication protocols with data encryption, like HTTPS with Transport Layer Security (TLS) and PC over IP (PCoIP).

Until recently cloud security was often cited as a primary concern and one of the few reasons many financial institutions would not move to the cloud. Things have changed. Over the last few years, banking leaders have come to realize that the cloud is an opportunity for banks to

improve security. In fact, it's now commonly cited as one reason to make the move.

Now, while cloud security is primarily focused on the technologies, tools, and methods used to keep cloud-based infrastructures secure, one of the biggest threats to cloud security has nothing to do with vulnerabilities in technology at all—it has to do with human vulnerabilities. According to a 2019 report by Kaspersky Labs, "Incidents in public cloud infrastructure are more likely to happen because of a customer's employees rather than actions carried out by cloud providers." The Kaspersky Labs report found that, "around 90% […] of corporate data breaches in the cloud happen due to social engineering techniques targeting customers' employees, not because of problems caused by the cloud provider."

Social engineering and other manipulative tactics that target human vulnerability can create weaknesses in any organization's security. The important thing to note is that it's not a challenge that's unique to cloud-based infrastructures. It's simply a cyber threat all organizations face today, whether their systems and data are on the cloud or not. So, while the cloud can provide world-class cybersecurity for banks, it's still important to understand that cybersecurity extends beyond tools and technology. While next-generation firewalls can be effective, it's just as important to create human firewalls to keep an institution's data secure.

The three primary cloud services providers currently offering cloud computing, storage, hosting, and disaster recovery services to the financial services industry today are Google Cloud, Microsoft Azure, and Amazon Web Services (AWS). When it comes to establishing trust, they're some of the most trusted technology brands in the world.

So, is the cloud safe for banks? Absolutely, the cloud can be safe for banks! With the right security enforcement tools, controls, expertise, and intrusive detection and prevention systems in place, the cloud can provide a trusted technological foundation for a safe and highly secure infrastructure for even the largest banks.

HOW BANKS STAY SAFE & SECURE ON A VIRTUAL PRIVATE CLOUD

From identifying software containerization technologies to building out an effective cloud migration team, there are numerous decisions that banks need to make before they can begin moving banking systems, applications, and data onto the cloud. Every financial institution is different with different systems, different workloads, and different business processes, so banking leaders and their teams will have to establish early on how much of the public cloud they are able or willing to adopt. That decision often comes down to a complex balance of risk tolerance and identifying what systems can effectively be containerized and moved to the cloud. Once those decisions are made, there are generally four cloud deployment models banks can consider: private cloud, public cloud, hybrid cloud, and virtual private cloud.

Some banks may opt for a combination of public and private cloud, known as hybrid cloud, to either mitigate concerns with cloud concentration or simply to maintain control of particularly sensitive systems or data they're unwilling to move. For banks that are committed to building an effective cloud-based infrastructure, a virtual private cloud will provide a platform that will allow financial institutions to take full advantage of the cost, performance, flexibility,

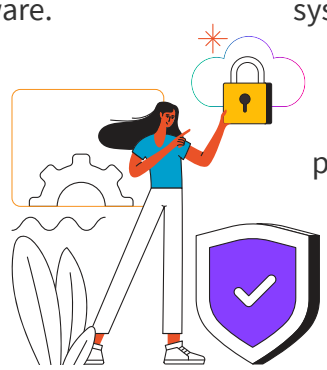
"A virtual private cloud will provide a platform that will allow financial institutions to take full advantage of the cost, performance, flexibility, scalability, and security benefits that the public cloud has to offer."

scalability, and security benefits that the public cloud has to offer. This secure cloud computing technology is a solution that's primarily reserved for organizations that process highly sensitive data and have unique security and compliance requirements. It's currently available and used by governments, businesses, banks, and financial institutions.

What is essentially a private cloud hosted on the public cloud, a virtual private cloud (VPC) combines the scalability and flexibility benefits of the public cloud with the ability to isolate sensitive data and systems on a private cloud network. Financial institutions that use virtual private clouds leverage an arguably more secure, single-tenant architecture on the multi-tenant public cloud and have access to isolated computing resources that are reserved exclusively for them.

Virtual private clouds are created on the public cloud using a combination of technologies that include a subnet, a virtual local area network (VLAN), and a virtual private network (VPN). These three technologies work together to effectively isolate a small piece of the public cloud for private use.

Cloud service providers divide part of the public cloud for private use by leveraging a private IP subnet—or a range of private IP addresses that are reserved and not available through the public internet—and a virtual local area network (VLAN). Much like how a local area network connects hosts on the same network using a physical switch and hardware, a VLAN allows administrators to separate or segment virtual networks logically on the same physical hardware. Using private IP subnets and VLANs, network administrators can also implement and configure different security controls over different virtual networks. Finally, in order to access the virtual private cloud, a virtual private network (VPN) is used, providing users with secure, authenticated, and encrypted remote access to the isolated resources within the virtual private cloud.



While the combination of **a subnet, a VLAN, and a VPN** provide the necessary isolation to create a virtual private cloud on the public cloud, there are some key technologies that will also help ensure financial institutions are bringing next-level security features to their virtual private cloud.

Next-generation firewalls (NGFWs) are one of the most important tools used to protect systems and applications on the cloud. They provide advanced network visibility capabilities and enhanced control for a cloud-based banking infrastructure. Effectively replacing traditional firewalls and unified threat management solutions, NGFWs leverage integrated intrusion prevention systems and are able to identify and enable applications regardless of port, protocol, evasive tactics, or SSL encryption. NGFWs also provide more control over applications and deeper inspection capabilities, making them a critical component in any bank's cloud security strategy.

Comprehensive cloud security and compliance management technologies, like Palo Alto Prisma, can help banks predict, prevent, detect, and automatically respond to security and compliance risks by continuously validating Payment Card Industry Data Security Standard (PCI DSS) and Service Organization Control 2 (SOC2) compliance.

Intrusion prevention systems (IPS) and intrusion detection systems (IDS) can provide financial institutions with real-time threat-detection monitoring and alerting solutions.

Obfuscation technologies and cloud encryption are critical tools for protecting sensitive data on the cloud. Leveraging cloud encryption for both data in transit and data at rest allows financial institutions to secure important information by transforming sensitive financial data from plaintext into indistinguishable cyphertext before it is transferred between cloud-based applications or stored on the cloud. The practice provides an extra level of security over sensitive data.

Authentication and authorization mechanisms are another important tool for banks moving to the cloud in preparation for consumer-directed finance. Financial institutions can leverage OAuth 2.0 tokens to authorize and provide third-parties secure access to web applications and resources without sharing passwords. The technology can help financial institutions provide secure access to partners for API-based integration and open banking by providing a secure framework for authorization.

Secure communication and cryptographic protocols like HTTPS with Transport Layer Security (TLS) will help ensure that any encrypted data in transit also travels securely, providing an encrypted connection between authenticated users, applications, and servers. PCoIP, on the other hand, can securely deliver visual applications or workspaces from the cloud to specific endpoints, transferring only the encrypted image information in the form of pixels. By transferring the display of a virtual desktop pixels, PCoIP ensures that important business data doesn't leave the cloud. These cryptographic technologies and secure communication protocols can help prevent data breaches and unauthorized access to sensitive financial data stored or travelling between applications on the cloud.

Finally, introducing **vulnerability scanning and penetration testing** into the DevOps continuous integration and continuous delivery (CI/CD) pipeline will ensure that security is designed into the development process itself to ensure systems and software on the cloud are consistently tested for weaknesses and security flaws.

While this isn't an exhaustive list of the technologies and tools that are available to financial institutions, it covers many of the key underlying cloud security technologies that work to keep financial institutions safe on the cloud. Understanding how a virtual private cloud is isolated on the public cloud and further exploring how these key technologies keep banks secure should help demystify cloud security and streamline the journey to the cloud.

As with any journey, this is about removing roadblocks, understanding where we are, and focusing on the road ahead.

Again, every financial institution is different, and while each journey to the cloud will look different, every bank will use similar cloud security technologies, systems, protocols, and enforcement controls to ensure their banking systems, applications, and data remain secure.

So, are we there yet?

We're getting closer. In fact, you can almost see it now.

portfolio+

ABOUT PORTFOLIO+

Portfolio+ Inc. connects financial institutions with customers and partners using innovative technologies. Its core banking software solutions and open banking technology are used by financial institutions in Canada and the UK. With its powerful +Open Banking Platform and fully documented RESTful APIs, Portfolio+ has the power to connect banks, credit unions, and financial institutions with the evolving ecosystem of financial services technology that is putting everyday customers in control of their financial data.

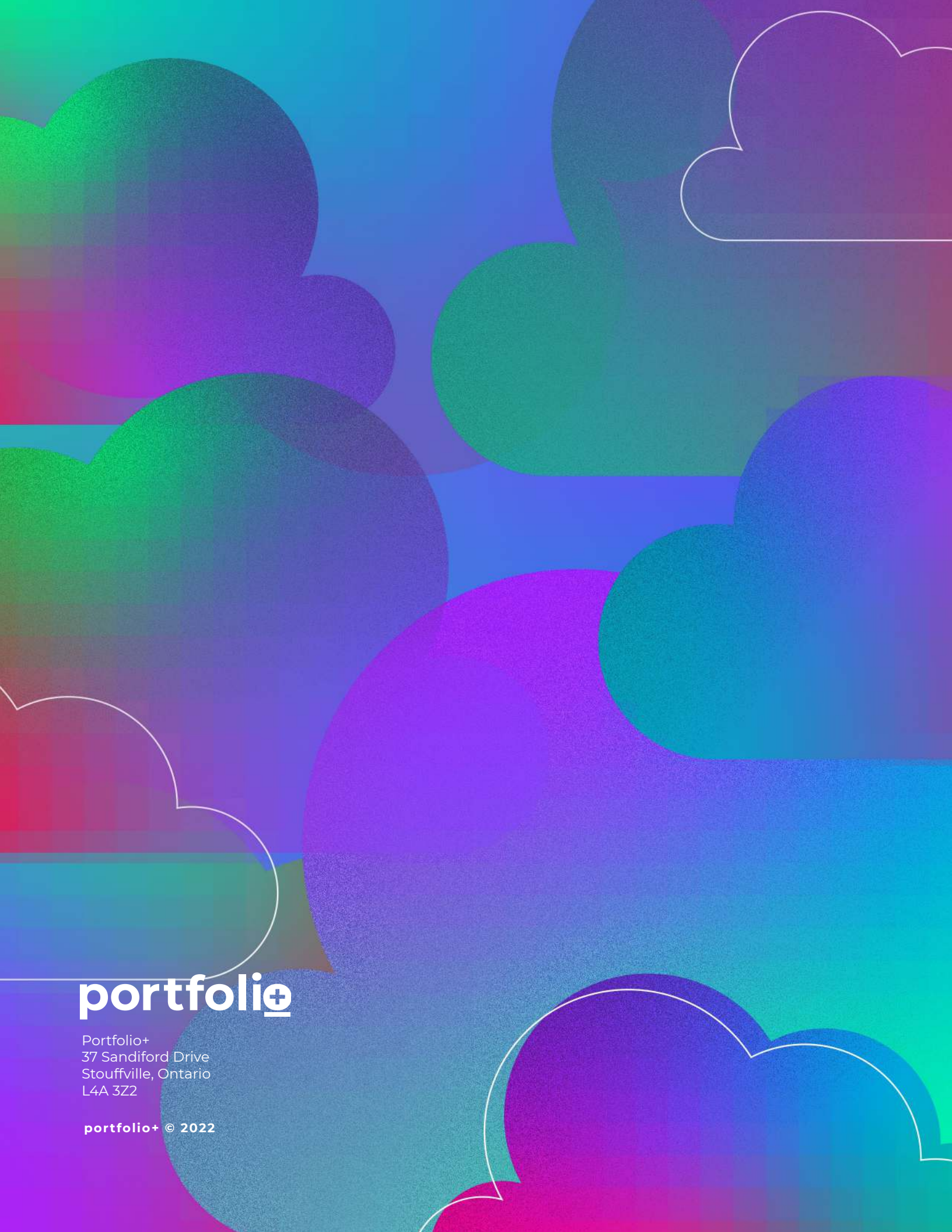
Located in the Greater Toronto Area (GTA), Portfolio+ is used by 5 of the 7* largest financial institutions in Canada and is a part of Volaris Group Inc.

For more information, visit portfolioplus.com.

*Based on TSE market capitalization figures retrieved in September 2020.

SOURCES

1. https://www.canada.ca/en/department-finance/programs/consultations/2021/final-report-advisory-committee-open-banking.html (Retrieved January 7, 2022)
2. https://www.finextra.com/blogposting/20273/what-is-stopping-banks-from-transitioning-to-the-cloud (Retrieved February 8, 2022)
3. https://www.kaspersky.com/about/press-releases/2019_head-in-the-clouds-humans-cause-nine-out-of-ten-data-breaches-in-the-cloud (Retrieved November 15, 2021)
4. https://www.cloudflare.com/en-ca/learning/ssl/transport-layer-security-tls/ (Retrieved February 18, 2022)
5. https://www.tokenex.com/blog/what-is-cloud-security (Retrieved February 18, 2022)



portfolio+

Portfolio+
37 Sandiford Drive
Stouffville, Ontario
L4A 3Z2