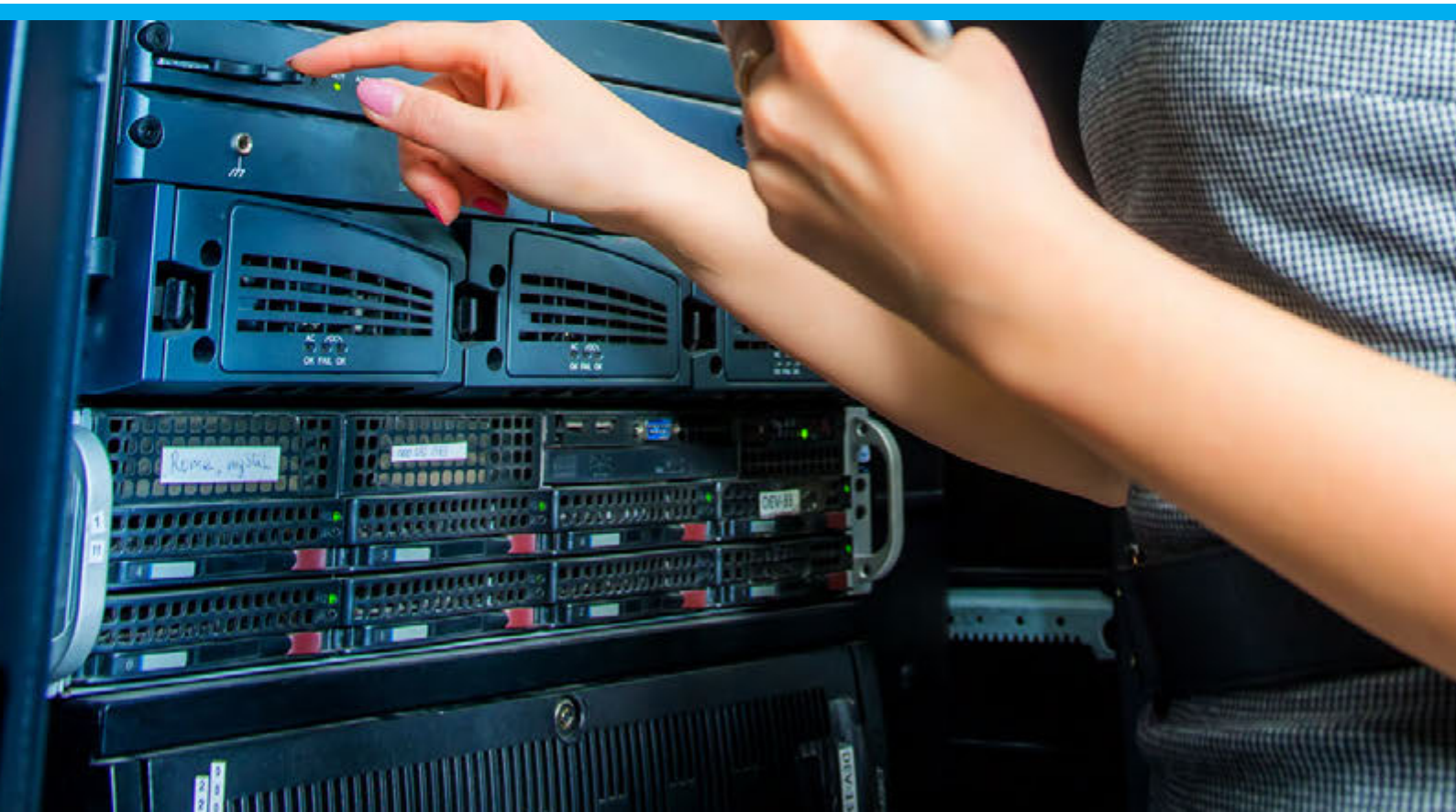
cogeco PEER 1

HYBRID IT

AT THE FOREFRONT OF ENTERPRISE



Contents

Introduction

Today, due to the rapid evolution of technology, it is notoriously difficult for any modern business to make well informed IT-based decisions with speed and agility.

This is especially true when you consider the ever-changing strategic vs. operational demands different people within an organization place on core assets, budget restrictions in place and market conditions that can be so volatile. It is a reality that has made choosing an appropriate IT infrastructure solution ever more challenging.

Different solutions come with different benefits, levels of service, and of course, price tags. But with so many IT solutions and reputable providers in the market, how can you be sure which one is right for your business?

This is where hybrid IT is redefining the technology landscape for modern day businesses across the globe.

As a game-changing solution, hybrid IT enables any business to leverage a range of third-party IT resources with minimum disruption to operational workflow or strategic vision, while fully maximizing return on investment.

The mix-and-match nature of hybrid IT solutions allow organizations to define and implement the right mix of technologies for them. Specifically deploying what they need, where they need it, to meet the requirements of stakeholders, partners, customers and their marketplace at large.

Chapter 1 – What is Hybrid IT?

As the name suggests, hybrid IT is a combination of at least two different technologies to achieve a seamless, robust IT solution. It essentially blurs the lines between managed hosting, managed services, cloud, colocation and on-premise facilities - by allowing multiple solutions and technologies to be used simultaneously and harmoniously.

Every company's unique needs can be satisfied with a hybrid IT setup that implements the best elements of each selected solution. It ultimately provides a business with highly effective, fit-for-purpose IT infrastructure and applications, on demand.

With hybrid IT, the days of a one-size-fits-all approach to infrastructure are gone. As businesses become more diverse, no two environments are alike. Considering business size, structure, location and budget, IT requirements can be delivered to exact specification and preference.

That's why more and more companies are looking at hybrid IT to effectively give them the best elements of their chosen worlds:

a) The flexibility, scalability and economies of scale that come with managed hosting, cloud services and colocation.
b) The ongoing maintenance, support and peak performance associated with fully-managed infrastructure, applications and network solutions.
c) The peace of mind afforded by comprehensive, state-of-the-art security and recovery solutions.
d) The control, familiarity and intimacy that come with on-premise IT solutions which remain ever optimized.

Chapter 2 – Infrastructure Options

When it comes to hybrid IT, achieving the right technology mix for unique business needs, challenges and processes is critical. There really is no such thing as an off-the-shelf solution.

The right solution will ultimately depend on the company's goals and the needs of each business user. Therefore, a successful implementation requires significant input and buy-in from the key stakeholders in the IT department. Essentially, a hybrid IT solution will require changes in roles, processes and business management that internal IT personnel have traditionally resisted.

For this reason business leaders sometimes pursue a strategy that utilizes external IT services, without the involvement of key IT stakeholders. This creates an unnecessarily difficult situation as both internal and external teams need to work together to effectively backwards engineer cohesion between the platforms.

The easiest way to understand hybrid IT - and get all key stakeholder buy-in - is to look at the various infrastructure components you have vs. need, and analyze the merits of each. This will allow for a more informed appreciation of how hybrid IT is able to utilize the very best aspects of outsourced infrastructure solutions and services, and marry them with on-premise solutions in a way that complements the organization's forward-thinking business strategy.

Cloud Hosting

Cloud hosting has emerged as one of the most popular infrastructure solutions for businesses today because of its highly customizable, highly flexible and highly scalable nature. Add to this the fact that no capital expenditure is required - and that billing is routinely done on a per-usage basis - and it's easy to understand why so many businesses are turning to the cloud as an infrastructure solution of choice.

Moreover, cloud environments are unique in that they utilize virtual servers that are underpinned by an extensive farm of physical servers. Said virtual servers are provided with as many or as few resources as they need depending on demand, and this allows any business operations to scale at will.

Cloud environments also benefit from unrivalled availability due to the way they are configured. Virtual servers can be added to the pool dynamically, ensuring that applications and services are always available.

Managed Hosting

Similar to cloud hosting in that an organization inevitably doesn't own the infrastructure hardware it utilizes, managed hosting is a popular choice for modern enterprises as it requires zero capital expenditure, is expertly supported and highly customizable.

The main benefit of the hardware remaining the property of the IT provider means that the business gets to take advantage of best-in-class configurations on the latest infrastructure, all the time and without having to make large capital expenditures.

It also enables an enterprise's internal IT resources to focus more on core business activities instead of spending inordinate amounts of time on infrastructure management and other routine tasks associated with server management.

Moreover, the performance-oriented nature of managed hosting solutions means they are ideal for businesses with heavy resource demands that require unrivalled reliability, security and uptime.

Colocation

Unlike cloud and managed hosting solutions, colocation requires an organization to make a capital investment in hardware, which is then placed and configured in one of the colocation provider's professional data center facilities.

Power, cooling, physical security and network connectivity are all provisioned by the colocation provider, while the primary responsibility for monitoring and managing the infrastructure sits firmly with the organization.

However, while the business is responsible for infrastructure management and support, many colocation providers today offer remote hands services for extra flexibility. These services - sometimes referred to as 'smart hands and eyes' - allow an organization to call upon the colocation providers highly-trained staff to carry out basic tasks and troubleshooting. Such services eliminate travel costs and can maximize uptime by resolving issues before they become service impacting.

So, rather than leasing hardware and/or services, the organization simply pays for the physical space its hardware occupies on an ongoing basis. This enables it to leverage a state-of-the-art data center at a fraction of the cost of building its own.

Managed Services

Just because an organization chooses to keep all - or some - of its IT infrastructure on-premise, doesn't mean it can't benefit from meticulously-managed server solutions provided by third parties.

Such thorough service offerings see a team of external experts working closely with an organization's own internal IT personnel, to ensure that every aspect of their server estate is performing as it should be. This frees up more time for internal resources to focus on core business activities, and ensures maximum uptime for enterprise applications.

From configuration to maintenance and troubleshooting, managed server solutions can help businesses realize significant operational savings. The best part of all is that businesses can pick and choose which managed solutions they want to leverage, allowing them to remain totally flexible while still benefitting from infrastructure that is managed for peak performance.

Here are some of the elements a managed server solution might include:

- **Hypervisor Management –** Designed to help with the monitoring and management of VMware and Microsoft Hyper-V to ensure virtual environments remain up and running.
- **Operating System Management –** Designed to keep Windows and Linux operating systems running at peak performance and reduce the likelihood of system crashes.
- **Application Management –** Monitors core business applications to ensure high availability and peak performance to keep the lifeline of a company working.
- **Database Management –** Delivers support, analytics and insights to keep business databases fine-tuned, real-time and performing at their peak.
- **Network Management –** Designed to monitor and support critical network elements such as switches, routers and firewalls, for consistent operational performance.
- **SAN Management –** Round-the-clock monitoring, maintenance and support to keep storage elements operating as they were designed to, and with minimal downtime.

Enter Hybrid IT

It is clear that cloud hosting, managed hosting and colocation offer numerous tangible benefits for your business today. But when you consider how they can all be configured to work in unison with existing on-premise IT solutions, the real potential is realized.

Add to this additional fully-managed infrastructure, application and network solutions, as well as comprehensive,

state-of-the-art security and recovery solutions, and you get a formidable IT mix that offers exponential flexibility, scalability and speed.

By implementing a truly hybrid IT solution, your businesses can realize all the benefits of cloud hosting, managed hosting, colocation and on-premise solutions, without having to worry about the drawbacks of legacy IT infrastructure. For this reason, hybrid IT is fast becoming the solution of choice for businesses across the globe, and is leveling the playing field for businesses large and small across many industries.

The right hybrid IT solution will ultimately allow your business to see four key benefits:

- **Cost-efficiency**
- **Flexibility**
- **Scalability**
- **Security**

Chapter 3 – Security

Despite the increasing popularity of next-generation IT infrastructure solutions - and proven benefits of deploying them - many organizations are still hesitant when it comes to adoption.

For example, some 70% of respondents to a Unisys survey on deploying cloud solutions cited security as their primary concern. Yet these reservations are often spawned from confusion or myth, which is why clarity is always needed to appease uneasy stakeholders.

Executive management buy-in can normally be achieved by addressing security concerns individually, and by demonstrating that perceived barriers are not insurmountable. This peace of mind in any third-party security provision is paramount to the short, medium and long term viability of a hybrid IT infrastructure.

The bottom line is that security concerns vary a great deal across industries, and these should be dealt with as a primary part of due diligence. There are also many resilience and compliance issues applicable to businesses across different sectors, and these too should be addressed with the third-party hosting provider before implementation.

Privileged User Access

Hosting data and services externally means they will be administered by a third party, i.e. the hosting provider and its employees. However, this does not mean that a business shouldn't demand reassurances when it comes to privileged user access.

Companies should be asking their hosting partner to be transparent about their privileged users, and are well within their rights to ask providers to supply detailed information about the hiring and on-going oversight of administrators. This should also encompass access controls and procedures to address employee turnover.

Regulatory Compliance

Some IT partners make compliance easy for organizations by offering colocation and managed hosting solutions that fully comply with stringent compliance requirements such as the Payment Card Industry (PCI) Data Security Standard (DSS).

Their facilities are regularly audited by independent third-parties to ensure continued compliance, giving organizations one less thing to worry about.

Data Segregation

In some cloud configurations, mass customer data resides on the same storage devices. This obviously poses concerns for businesses, and encryption is just one method by which company data should be protected.

This is why data segregation has to be demonstrated by the hosting provider, and its encryption schemes designed - and subsequently tested - by encryption specialists. Encryption accidents can render data totally inaccessible, and even basic levels of encryption can have an impact on availability.

This is why many organizations choose to go down the managed hosting or colocation route.

Backup & Recovery

Because every business is unique, the backup and recovery solutions implemented for one organization won't necessarily be fit-for-purpose for another. That's why many companies today choose to partner with third-party providers that can implement dedicated and robust backup and recovery solutions.

Forward-thinking organizations don't want to be lumbered with a backup and recovery solution that is expensive and inflexible. They need the freedom to be able to build and scale backup and recovery procedures to match their business needs, both at the present time and in the future.

Network Perimeter & Remote Access

A corporate network is really only as secure as the perimeter defenses that are in place to protect it. For this reason, many organizations choose to implement an array of perimeter security solutions and partner with third-party providers to get them implemented.

Managed firewalls - whether they are dedicated or shared - provide a solid first line of defense, and are designed to protect an organization's valuable infrastructure assets. Having them managed by a third-party provider removes a lot of the stress and hassle for the organization.

Likewise, dedicated remote access and VPN services are designed to facilitate seamless connectivity for business users, while keeping unwanted intruders out. Organizations should look for highly secure, flexible and cost-effective IPSEC network solutions which can adapt to their needs going forward.

DDoS Protection

Despite being one of the oldest threats on the IT security landscape, DDoS attacks still represent a huge risk for businesses today. The fact they are growing in magnitude and evolving all the time, means that businesses often cannot keep track of them.

Mitigating such threats in-house is usually prohibited by budget, resources and time constraints. It's not surprising therefore that bespoke DDoS shields provided by third-parties - which safeguard applications and platforms from these increasingly powerful attacks - make a lot of sense for modern enterprise.

Application Security

Even with a managed firewall protecting an organization's perimeter, there are still plenty more application security solutions that can be implemented behind it.

Web application firewalls (WAFs), for example, sit just behind the main perimeter security and monitor traffic, looking for unexpected behavior and data patterns. They serve to protect the actual applications themselves from malicious threats, minimizing downtime.

Log-monitoring tools, which detect potential security issues in real-time, allow organizations to investigate and address any anomalies before they become service impacting. Log-monitoring tools can also help satisfy compliance requirements.

User Security

No matter how much an organization spends on business user training in terms of security, threats will always remain. That's why managed web content filtering and managed anti-virus/anti-spam solutions exist.

With managed web content filtering, any potentially unsafe URLs and unwanted data are blocked at the network gateway level. This allows a business to better protect its users from undesirable content and inappropriate websites.

Managed anti-virus/anti-spam solutions provide an extra layer of defense against email threats, filtering messages to remove viruses, worms and Trojans. This vastly reduces the chances of a user being duped by a convincing email, and compromising the entire network as a result.

Customer Security

Trust is massively important when it comes to eCommerce, which is why enterprises with a large online presence utilize SSL certificates from a trusted Certificate Authority such as Symantec. They help to confirm to the organization's website visitors that they are indeed dealing with a legitimate business, and that it's safe to share their information.

Regulatory compliance like SSL certificates can also be the difference between an enterprise's customers trusting their online offering and not.

Chapter 4 – Mission Critical

Hybrid IT presents many exciting opportunities for business environments across the globe. However, many organizations have concerns when it comes to hosting mission critical services and applications anywhere outside their own data center(s), or having a third-party IT services provider administering them on a fully-managed basis.

While this is a reservation that is not without grounds, businesses are utilizing external infrastructure solutions and value-add services more and more for mission critical needs. In so doing they - along with their service provider - recognize and address any associated risks before migration. Mitigating issues and streamlining deployment so that their mission critical services and applications don't miss a beat.

Risk Assessment & Management

When moving any assets to external environments, or allowing them to be managed in-house by an external third-party, it is imperative that organizations conduct a thorough risk assessment and subsequent risk management plan. It is unfair to assume that the external environment or third-party provider will automatically create greater levels of risk, which is another reason why an in-depth risk assessment cannot be bypassed.

A risk assessment should ideally include the following steps:

- **Define the risks…** It is necessary to compile a definition of risks for every asset, based on its business criticality.
- **Assess the status…** Assess the current status of each risk prior to migration. This information will allow each risk to be accepted, mitigated, transferred or avoided.
- **Analyze the risk profile of each asset…** With the risk assessment complete, the risk profile of each asset can be analyzed.

This process will allow a business to make a comparison in terms of risk between its current state and its 'desired' hybrid IT solution.

With a suitable risk assessment in place - and due diligence conducted - migration of mission critical applications and services can begin. This should be a seamless task that involves the organization's internal IT department and the third-party IT services provider, the latter offering their full migration expertise.

Security best practices like secure tunnels and VPNs are a must when migrating any assets to an external hosting environment.

Protecting Your Data

Of equal importance is the protection of assets once they are in the hybrid IT solution. For example, controlling access to critical applications and the threat of data breaches are always prominent concerns for a business.

For example, many individuals see the cloud as a large target for data thieves, and are dubious about transferring any confidential information to it. Yet most cloud infrastructures are ultra-secure, provided these best practices are followed by the hosting provider:

- Customer segregation at the network level.
- Multi-tenant technology to ensure customer segregation at the storage level.
- No infrastructure overlaps between customers.
- Stringent network security capabilities to prevent malicious attacks.
- Ensuring only authorized users can access cloud-hosted systems.

With appropriate operational, physical and network security, a cloud solution can boast an environment that is as good, if not better, than an on-site data center. Furthermore, the value-added security services offered by many IT providers are also available to mitigate the risks to on-premise infrastructure posed by today's increasingly sophisticated digital threats.

Ensuring Business Continuity

The 24/7 provisioning of business critical applications is of crucial importance to modern day enterprise. The impact downtime has on an organization's productivity, profitability and reputation can be enormous.

Every business needs to understand what protocols are in place to ensure high availability, and what business critical service level agreements are being adhered to. Ultimately, it depends on the mix of infrastructure solutions in an organization's hybrid IT setup as to who is responsible for ensuring the availability of services on an on-going basis.

Organizations and IT providers alike must have stringent procedures in place for incident management, problem management and, where applicable, change management. Any downtime will need to be thoroughly investigated, and measures implemented to prevent future recurrences.

Businesses need complete reassurance when it comes to high availability, and IT providers can improve a company's disaster recovery program by implementing nightly replication to enhance data integrity.

In addition, bespoke backup and recovery solutions, as provided by third-party IT services providers, can boost an organization's continuity plans and resilience.

For example, some backup and security solutions facilitate the migration of data, services and operating environments to infrastructure that is housed off-site. This allows primary site recovery and restoration after a disaster.

Furthermore, some IT services providers offer fully-managed recovery of an organization's servers, enabling them to operate normally in their own environments until such time as the business is ready to restore operations to their primary data center/infrastructure solution.

The ability to carry out on-demand restorations of data improves the overall effectiveness and efficiency of a company's restore capabilities, and the IT partner can often provide full online or physical assistance where required. This mitigates data loss, enabling any enterprise to get back up and running as soon as possible, with minimum business interruption.

Chapter 5 – Long-Term Maintenance

Maintenance is an inevitable part of any technology configuration, and hybrid IT solutions are no different. The on-going availability of a hybrid configuration - and prevention of system downtime - depends on regularly scheduled, routine maintenance.

These maintenance activities should be accompanied by appropriate documentation and checklists to ensure they are undertaken in a meticulous and uniform way.

With a hybrid IT environment, both in-house IT personnel and the external third-party service provider could be responsible for maintenance. This presents opportunities and threats to the system's integrity, and to both organizations.

Why is Long-Term Maintenance Important?

Maintenance is essential to ensuring that any computer system operates to the best of its ability, as close as possible to 100% of the time. This fact is even more prevalent when it comes to servers that are running enterprise applications and storing sensitive information.

A server crash will inevitably lead to significant issues; business downtime, loss of revenue, loss of reputation, compromised data integrity and employee productivity issues, to name but a few. This is why preventative maintenance is such an important part of any IT department's on-going strategy.

Well-maintained servers afford greater reliability and performance compared to hardware configurations that are cluttered and insecure. Furthermore, long-term maintenance inevitably extends the life of a business asset and keeps it functioning more efficiently.

Application of updates and manufacturer patches to close security loopholes and improve resilience are standard maintenance routines. Failure to apply release updates may lead to a future issue should the business seek advice from the hardware or software manufacturer. Often, a prerequisite for troubleshooting any issues with a provider is to have a fully patched server. Failure to do so will usually be met with advice to apply relevant patches prior to any further changes being made.

What Does Maintenance Incorporate?

Applying manufacturer patches/updates ensures that a business is always running the latest version of a manufacturer's software, and that it is protected from potential threats that might have been exploited had the relevant patch not been applied.

In addition, bespoke backup and recovery solutions, as provided by third-party IT services providers, can boost an organization's continuity plans and resilience.

For example, some backup and security solutions facilitate the migration of data, services and operating environments to infrastructure that is housed off-site. This allows primary site recovery and restoration after a disaster.

Furthermore, some IT services providers offer fully-managed recovery of an organization's servers, enabling them to operate normally in their own environments until such time as the business is ready to restore operations to their primary data center/infrastructure solution.

The ability to carry out on-demand restorations of data improves the overall effectiveness and efficiency of a company's restore capabilities, and the IT partner can often provide full online or physical assistance where required. This mitigates data loss, enabling any enterprise to get back up and running as soon as possible, with minimum business interruption.

Maintenance Responsibility

Whose responsibility it is to undertake routine maintenance activities depends completely on an organization's implemented solution. In a hybrid IT infrastructure, maintenance of cloud servers and managed hosting servers is inevitably the responsibility of third-party providers.

With colocation, it's the primary responsibility of the organization and its own IT personnel to manage and maintain infrastructure components. Although many colocation providers do offer remote hands services, which enable small changes and fixes to be conducted by their own staff rather than organization staff.

Maintenance of an internally hosted, on-premise server lies squarely with the business and its respective IT personnel. If this component is used in conjunction with an externally hosted service, the third party host may provide maintenance and support to ensure smooth operation.

The Bottom Line...

Hybrid IT solutions incorporate a range of hosting technologies, managed IT services and on-premise infrastructure. They allow today's enterprise to be totally flexible in their approach to IT infrastructure, by implementing a range of solutions that match their business needs, goals and vision.

The flexibility of hybrid IT allows every organization to evolve with speed and agility, while complementing growth plans at all times.

Oftentimes, expensive capital expenditures do not afford such flexibility and hamstring a business at the times when it needs to be most dynamic. With the right hybrid IT solution, the opportunities for your organization are endless.

About Cogeco Peer 1

Cogeco Peer 1 is a wholly-owned subsidiary of Cogeco Communications Inc. (TSX:CCA) and is a global provider of essential business-to-business products and services, such as colocation, network connectivity, managed hosting, cloud services and managed IT services, that allow customers across Canada, Mexico, the United States and Western Europe to focus on their core business. With 17 data centers, extensive FastFiber Network ™ and more than 50 points-of-presence in North America and Europe combined, Cogeco Peer 1 is a trusted partner to businesses small, medium and large, providing the ability to access, move, manage and store mission-critical data worldwide, backed by superior customer support.

To learn more about how we can enable Hybrid IT for your organization, please visit www.cogecopeer1.com

Ready to learn more?

Streamline your IT with Cogeco Peer 1.
Visit www.cogecopeer1.com

CA
413 Horner Ave,
Etobicoke,
ON M8W 4W3
1.866.579.9690

US
250 E Grayson St,
San Antonio,
TX 78215, United States
1.888.978.7251

UK
30 Town Quay,
Southampton
SO14 2AQ, United Kingdom
0800 840 7490

FR
GreenSide, Bât 2
400 avenue Roumanille
06410 Biot, France
0805 210 280

cogeco PEER 1