macquarie
DATA CENTRES

The new normal for data infrastructure.

Authored by Macquarie Data Centres

macquariedatacentres.com

Executive Summary.

The events of the past five years have radically shaped the way we live and work. From wild weather events, to geopolitical tensions, a once-in-a-century global pandemic and the accompanying move to online.

These macro-economic forces have created challenging conditions for many enterprises. Traditional business models are being pushed aside and how a company responds will determine its future – adapt and survive or resist and fold.

Many organisations have used this period to reassess their physical footprint, as well as their financial and operational models, in a bid to emerge leaner and more efficient in a post-pandemic world.

The massive demand for cloud-based services as a result of COVID-19 – and the ongoing shift from CAPEX to OPEX – is generating more data and driving demand for localised storage offerings.

This whitepaper will assess how these changes have helped herald a new era for data infrastructure.

In this new period, we expect to see more companies move their on-prem data centres to outsourcing providers or choose colocation in order to achieve greater security, stability, and reliability.

Equally, enterprises will become more strategic about where they run particular workloads. For some this will involve moving applications away from the public cloud and repatriating their own hardware. While for others it involves adopting a hybrid IT model in a bid to quell rising security, cost, compliance and performance concerns (IDC).

The paper will address the future of data centres and colocation; and how businesses can scale with confidence, while readying for the impact of key trends like AI, IoT and Edge computing on their IT infrastructure.

Global economic slowdown.

The world's economic foundation was already shaky at the turn of 2020, before the COVID-19 pandemic took hold. Lingering pressures like Brexit, tightening local credit restrictions, and economic slowdown in China, impacted the GDP of most global superpowers.

Despite these forces, the overall enterprise infrastructure industry in Australia and New Zealand was expected to grow three per cent in 2020 (IDC).

But when COVID-19 hit – upending ICT supply chains and generating widespread market apprehension – IDC adjusted its 2020 forecast, instead projecting a decline of 3 per cent. With transformational IT projects pushed back and enterprise budgets slashed, the COVID-19 crisis looked as though it might be too much for the, otherwise resilient, sector.

However, in the same way that extreme pressure forms diamonds, so too have data centres risen from the charcoal like a Baker's globe mallow.

With social distancing protocol forcing everyday workflows into the digital realm – upping our reliance on internet connectivity – a new, worldwide appreciation for data centres has emerged.

The 'invisible infrastructure' that is responsible for helping businesses create remote work environments; streaming and online entertainment providers manage unprecedented demand, and that which supports the push to digitisation within hospitals, utilities and governments, was quickly considered an essential service. Not only to help keep society's lights on and telecommunications running, but to facilitate social cohesion as we stayed apart to save lives.

If they weren't already, this experience has also encouraged many governments to start considering data centres as mission-critical infrastructure – alongside power and water utilities – due to their integral role in keeping economies, hospitals and societies in working order.

In recognition of the sector's growth and it's resilience throughout the pandemic, IBISWorld recently more than doubled its revenue forecast for the 2020 data storage services industry, from 6.1 to 12.7 per cent.

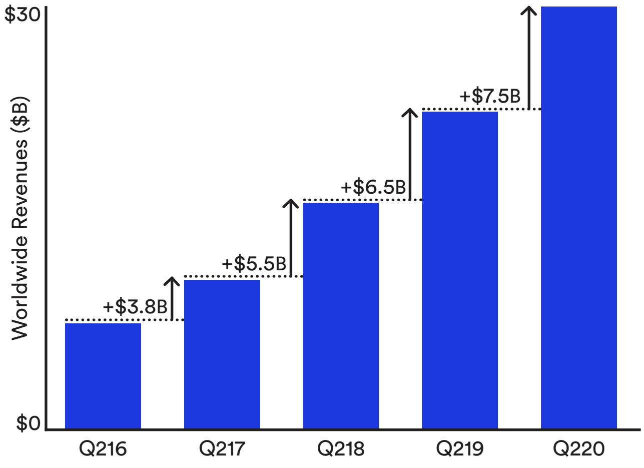
Assessing cloud workflows.

For many organisations across this period, the cloud has provided a panacea, helping them spin up new workloads and provide remote storage options in a matter of hours or days; to support people confined to home environments.

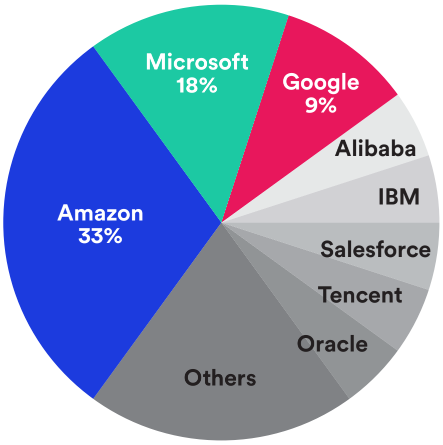
New Synergy Research shows that spending on cloud infrastructure services rose dramatically across the first half of 2020, surpassing US$30 billion between April and July. Investment during the three-month timeframe increased more than US$7.5 billion, compared to the same period in 2019, continuing a trend of "ever-larger increments" in cloud spending.

Quarterly cloud infrastructure service revenues – including IaaS, PaaS and hosted private cloud services – accounted for roughly US$30.5 billion during the quarter, with trailing twelve-month revenues reaching US$111 billion.

Cloud Infrastructure Services Market
IaaS, PaaS, Hosted Private Cloud



Source: Synergy Research Group



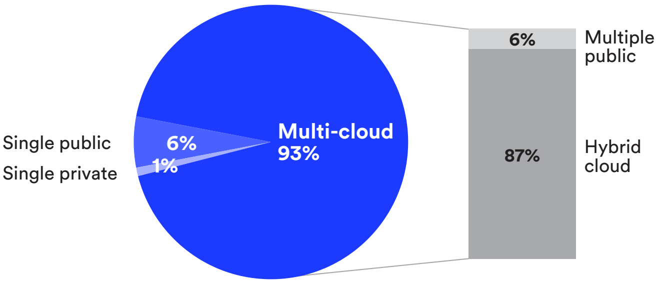
Market Share Q2 2020

While vendors like AWS, Azure and Google dominated across this period, global giants like Alibaba Cloud also saw huge growth. So much so, Alibaba has announced plans to invest over US$28 billion in the construction of data centres and cloud infrastructure over the next three years.

That is not to say, though, that data storage and infrastructure spending has been unconstrained. Whilst enterprises grapple with reduced – or altogether blighted – revenue streams, ICT and wider enterprise dollars are more precious than ever before. This has paved a path for more conscious data infrastructure spending and prompted many to reassess their existing set-up.

Enterprises that were first to cloud are now leading a shift away from public cloud, to various hybrid infrastructures or multi-cloud environments. Other organisations are accelerating migration from their own on-prem data centres to colocated spaces. In doing this many are relying on their colocation provider to help them overcome challenges brought on by the pandemic; including reduced headcount, difficulties accessing their own data centre facilities, and delays in hardware supply chains – all of which have the potential to dramatically impact business continuity if not expertly managed.

Enterprise Cloud Strategy
% of enterprise respondents



N=554

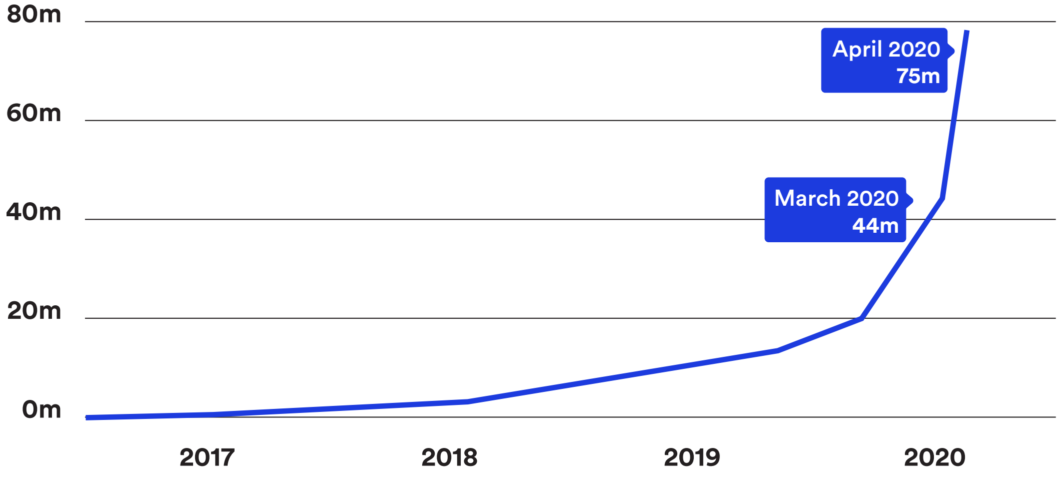
Source: Flexera 2020 State of the Cloud Report

The impact of remote and hybrid working models.

At the outset of the COVID-19 pandemic, when stage four lockdown measures were first introduced, 91 per cent of APAC businesses were thrust into a remote working model, practically overnight. Today, many have resumed office-based operations, but thousands are still expected to work from home for at least half of the week, for the remainder of 2020.

This remote working model has significantly increased our reliance on internet connectivity. The usage of online collaboration tools such as Zoom, WebEx and Microsoft Teams has surged, with Teams increasing its active daily users from 20 million to 75 million between November 2019 and April 2020.

Microsoft Teams User Growth Since 2017



Source: DataCentre Dynamics / Microsoft

While the average consumer is now more aware of network bandwidth and various unified collaboration (UC) tools than ever before, the real challenge lies in the data infrastructure that supports them. On-prem data centres are rarely geared to provide the right level of digital support for widespread work from home arrangements – where data and applications are distributed among disparate systems and various endpoint devices. In this multi-cloud, post-pandemic era, the on-prem data centre has become vast and complex, designed to drive the best user experience, rather than private, secure and compliant mechanisms it was likely intended to provide.

Some organisations have sacrificed security protocols in order to support such rapid remote work transitions. Attackers have also taken advantage of the initial overload of COVID-related news to prey on people that are otherwise preoccupied or have relaxed their guard while working from home.

Microsoft's intelligence unit shows that in the months leading to May 2020, every country in the world saw at least one COVID-19 themed attack. As we continue to work and learn remotely, the ability to manage who participates in meetings, and who has access to meeting information has never been more critical.

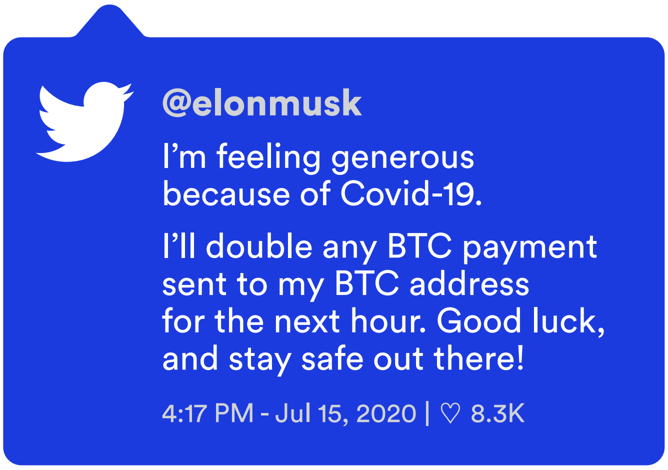
For IT teams, it's also vital to ensure that access to applications are managed with multi-factor authentication and personal data is safeguarded with enterprise-grade encryption.

Twitter's bitcoin data breach nightmare is a cautionary tale of what can happen when trusted privileged access falls prey to insider attacks and the consequence of weak data security practices. The major hack involved a bitcoin scam that targeted dozens of high-profile accounts including Barack Obama, Michael Bloomberg, Apple and more. The attackers targeted employees who had access to its internal systems in what it believed to be a coordinated social engineering attack.

The breach highlights the importance of strengthening security controls to ensure only the right people have access to sensitive data. This is especially key if you lose chain of custody to third parties or in a world of remote work where you're unable to see individual movements across a network without robust security monitoring tools.

At a time where security, cost and compliance concerns are heightened, these occurrences are expected to drive more companies towards colocated data centre facilities.

High profile accounts involved in a recent Twitter data breach.

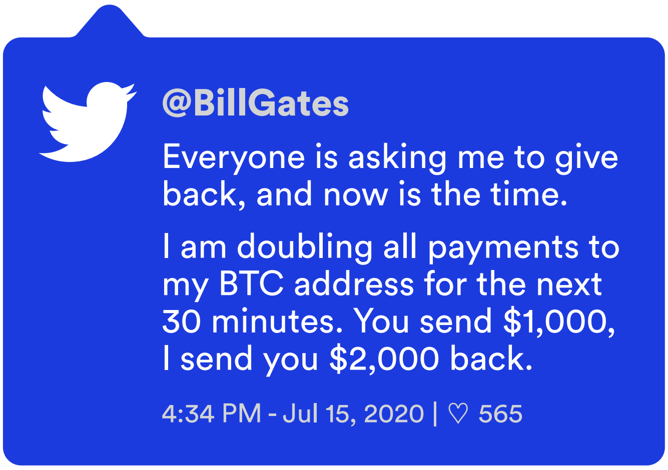


@elonmusk

I'm feeling generous because of Covid-19.

I'll double any BTC payment sent to my BTC address for the next hour. Good luck, and stay safe out there!

4:17 PM - Jul 15, 2020 | ♡ 8.3K



@BillGates

Everyone is asking me to give back, and now is the time.

I am doubling all payments to my BTC address for the next 30 minutes. You send $1,000, I send you $2,000 back.

4:34 PM - Jul 15, 2020 | ♡ 565

Geopolitical tensions shape new data legislation.

Amid the challenges of COVID-19, underlying friction with China has also resurfaced. The Australia-China relationship has been beset with geopolitical tensions since the 1980s; and China's relationship with the USA, since the 1940s.

Although these tensions have been abated by strong bilateral interests, more recent tensions have heralded an ongoing trade war between China and various nations, including the USA. They have also been a catalyst for various law changes which have, in turn, impacted the data flows and the broader data centre environment.

One recent source of tension – which has profound implications for data centres globally – is a new piece of Chinese cryptography legislation, enacted in December 2019. Under this law, Chinese authorities are granted full, unrestricted access to any data transmitted or stored within China. The Cybersecurity Multi-Level Protection Scheme (MLPS 2.0), as it is known, prohibits VPNs, private and encrypted messages, and anonymous online accounts. It effectively makes all data – from either Chinese servers or transmitted through Chinese networks – visible to the government.

Alongside the MLPS 2.0 is another new piece of encryption legislation which specifies that the development, sale and use of cryptographic systems, "must not harm the state security and public interests." It also makes cryptographic systems which are not "examined and authenticated" punishable by law.

Additionally, if a company's data centre uses a Chinese-owned software service, authorities now have the right to seize all data stored and managed by that service – including sensitive financial information. As a result of these laws, a number of high-profile organisations have begun relocating their data from Chinese-owned or Chinese-based facilities – often at a significant financial cost to the enterprise.

For example, Australia's Defence Department recently announced that it will spend $2 million terminating its relationship with a Sydney data centre and moving its private files into a government-owned hub. This was after a Chinese consortium purchased half of the centre's parent company. It is expected that many other companies will follow suit, either through shared circumstances, or as a precautionary measure.

Compounding these security concerns, a company's physical proximity to its data centre is becoming increasingly important to businesses that wish to emerge leaner and more efficient in a post-pandemic world. Closer proximity to a data centre can improve the performance of IT infrastructure, or facilitate direct cloud on-ramps, whereas replication and latency issues often emerge when transmitting large volumes of data over distance.

Cloud repatriation for critical workloads.

In assessing IT infrastructure performance, many enterprises have realised that while the public cloud might offer better agility for some, offloading critical computing resources also causes unexpected challenges. Regulatory, compliance and privacy issues can surface when a company migrates to public cloud, particularly with firms that view and treat it as another form of data centre.

According to IDC, 85 per cent of IT managers are now repatriating some workloads from public cloud environments, bringing them back into their data centres or edge environments, with much stronger understandings of cloud functionality, cost, architecture, technical and compliance requirements.

Decision makers should also consider latency, availability and control within this mix. Often, moving an application or workload from the cloud makes good business sense when critical operational benchmarks are not being met. This might mean inconsistent application performance, high network latency due to congestion, unforeseen costs, or concerns about data security.

Dropbox was one of the first big companies to make this call. In announcing its intention to go public in 2018, the world got to peek into Dropbox's financial reports and see how much the company's decision to optimise its IT infrastructure had truly saved it. By shifting a significant volume of its data and storage away from public cloud, to a multi-cloud environment with custom colocation facilities, it reduced its operating expenses (OPEX) by an eye-watering US$75 million.

Future data demands driving colocation.

Not only are businesses wisening to the benefits of hybrid IT environments to meet data demands; macro trends like the growth of AI, Edge and IoT are also fuelling demand for faster, more power-efficient computing hardware. These data-hungry technologies are placing on-prem data centres under increasing strain, paving the way for colocation services.

Over the coming decade, a proliferation of data-driven tools – like AI and interconnected devices – are expected to permeate mainstream enterprise practice. These technologies will deliver between $9.5 trillion and $15.4 trillion in economic value, annually.

Machine learning in particular – which use large data sets and algorithms to make complex business decisions – is expected to make a big footprint. Their rise is inevitable. Given the economic pressures of COVID-19, companies can no longer afford to make decisions based on intuition.

As a result of these forces, IDC predicts that the world will generate 40 zebibytes (40 trillion gigabytes) of data in 2020 and 175 zebibytes in 2025. Moreover, Gartner predicts that by 2022, 70 per cent of this data will be created at the Edge, up from 40 per cent in 2020.

These heavier data sets will be harder and more expensive to move around, placing existing networks under increasing strain. By localising data traffic, analytics and management, however, enterprises can more effectively control their data and scale their digital business. To this end, data centres will be pivotal; as will larger and faster networks - and “data thinning” from distributed compute capacity. More enterprises will also choose to colocate with one or more data centre providers, to bring compute power closer to where the user resides.

Resilience in a changing world.

Research shows that 70 per cent of companies that currently rely solely on on-prem data centres have plans to migrate some data into a colocation facility at some point in the future. As such, Statistica predicts that revenue from the wholesale and retail data centre colocation market will rise to US$54 billion by 2023, up from US$38 billion in 2018.

Colocated data centres offer the data infrastructure to help firms navigate the post-pandemic world. They already relieve a number of COVID-19 related pain-points: reliability, security and cost-efficiency.

In terms of reliability, features like multiple power sources and internet connections, Tier III certification and back-up generation help them stay online in the event of a disaster. In August 2020, this latter feature proved useful when a heat-related power shortage caused a state of emergency in California and data centres were asked to turn on their generators to help relieve the load.

Tier III data centres are designed to ensure services continue to operate no matter what is happening outside the premise. They are highly secure and offer concurrently maintainable facilities. If replacement parts are required for any reason, the service level agreements a colocation provider has in place typically ensure parts are flown overnight to where they are required.

Border closures and deep cleans in manufacturing plants, as a result of COVID-19, have impacted this process for some providers. For Macquarie Data Centres it’s meant enacting pandemic-ready Business Continuity Plans; whereby spare parts inventory for all critical plant equipment is stored securely within Australia, and service level agreements (SLAs) are refreshed with our critical infrastructure providers – ready to go if faced with this or any other challenge.

On the security front both physical and cybersecurity have become mainstays as enterprises consider the future of their data infrastructure. On-prem storage might suffice when everyone is working from physical offices. But with the changes heralded by this next normal, does the enterprise require a more flexible and scalable solution?

Operating and running mission-critical infrastructure in-house can create weighty overheads, with power management, on-site staffing resources, cooling and security all impacting the bottom line.

Security options available:

- ✓ Business continuity plans
- ✓ Supply chain resilience
- ✓ Physical security guards protecting the data centre sites
- ✓ Multi-factor authentication measures
- ✓ CCTV and alarms
- ✓ Logical security controls

Colocating with a data centre provider can reduce this burden. Whether that's through the range of security options available, including the provider's business continuity plans and supply chain resilience; the physical security guards protecting the data centre sites, multifactor authentication measures, CCTV and alarms, or the logical security controls the enterprise selects for their own racks. Requirements might vary, but what doesn't change is the importance of knowing how the data centre provider is working to keep each enterprise's data safe.

In terms of cost-efficiency, colocated facilities provide a lower cost per Mbit, with renters able to piggyback off the provider's efficiency of scale. Carrier neutral facilities, or facilities located in fibre and network-dense locations, can also provide pricing flexibility.

Additionally, colocated data centres are based on a CAPEX model, with fixed charges. This can work out more favourably than cost-for-performance (OPEX) models, like that offered by public cloud service providers. As discussed earlier in this paper, public cloud often creates sticker shock for companies when it comes to storage and bandwidth costs. By contrast, a colocated facility enables firms to fill up their rack(s), or entire halls, with vast amounts of storage for a modest monthly flat rate.

Conclusion.

The tumultuous start to 2020 has created significant uncertainty for enterprises, worldwide. With revised revenue forecasts and a continuously moving deadline for resuming business-as-usual operations, the path ahead has not always been clear. Despite this uncertainty, strong themes have emerged, which help refocus enterprises priorities in a post-pandemic world.

Now, more than ever before, companies must strive to achieve security, reliability and cost-efficiency with equal weight, when managing their data. The good news is that the technologies that can help businesses maintain these outcomes simultaneously already exist.

With better data-driven expertise, enterprises can make smarter decisions, planning for the future of data infrastructure and investing in the facilities that are right for them.

In today's world, doing so is a matter of survival.

Want to learn more about the new normal for data infrastructure? Let's talk. We'd love to start the conversation at one of our Intellicentres, so you can experience them for yourself.

Macquarie Data Centres
1800 004 943
macquariedatacentres.com

Sep/2020