dimension data

accelerate your ambition

Hybrid Cloud Best Practice Guide

Mastering the 6 Critical Success Factors of Hybrid Cloud

Mastering the 6 critical success factors of hybrid cloud

For every established enterprise, and every born-in-the cloud company too, hybrid cloud is a reality today.

For every established enterprise, and every born-in-the cloud company too, hybrid cloud is a reality today. SaaS applications, private clouds, and cloud hyperscale providers are all essential parts of any business's IT ecosystem in the digital age.

An effective hybrid cloud operating environment can move as quickly as your business needs to – and slow down just as quickly when required. You can expect it to deliver the business outcomes you're looking for, like increased speed of execution, flexibility to adapt, and the ability to seize new business opportunities.

But there are a number of things you have to get right if hybrid cloud is to deliver the outcomes you require…

We believe the 6 critical success factors of hybrid cloud are:

Strategy

Focusing first on the business outcome you are trying to achieve, deciding on the right workload placement strategy, and architecting a solution that will satisfy governance and compliance requirements

Security

Building on a strong foundation of consistent security policies, behaviour, visibility and management across your cloud environments; securing your data and applications against a dynamic cyber threat landscape in real time; and ensuring you can respond rapidly and effectively to security incidents

Management

Having the ability to manage all your clouds centrally; choosing platforms that offer the right mix of enterprise-grade public, private, and hosted services; finding help with refactoring, migrating, and managing workloads; getting access to the skills you need, and keeping up to date with emerging technologies

Networking

Navigating the complexity of networking across clouds, data centres, the WAN, and the access layer

Consumption models

Choosing a commercial model that is aligned to your business profile

Business continuity

Ensuring effective cloud backup, business continuity, and disaster recovery

In this Best Practice Guide, we'll show you how to master these, so that you can get the most out of your hybrid cloud investment and accelerate your digital business.

This Guide is about hybrid cloud, which is the combination of multiple private and public clouds. In most mature organisations hybrid cloud will form part of a wider hybrid IT environment, which includes physical infrastructure as well as clouds.

Strategy

Workload placement strategy

First, focus on the business outcome you are trying to achieve and design a technology solution that will deliver it. Consider every layer from the business process, through the application, the platform, and the infrastructure. Then you'll be in a position to decide which is the best place to put your workload.

You may be an established enterprise looking to move applications in the cloud. You may have already moved the easy workloads and now you're looking into whether it's worth moving more complex workloads. On the other hand, you may be a born in the cloud company, or already embracing new models, and your next move is to leverage containerised applications.

Either way, workload placement is a careful balancing act between cost and performance, compliance and security. We recommend asking yourself these simple questions:

- **Why** am I considering moving it – what are the benefits I'm chasing, their scale versus the risks and complexities, and how sensitive is the ROI model?
- **What** am I moving – the app or part of the app, the data or part of the data, the processing, the storage, etc?
- **Where** am I thinking of putting it – the geographical location, the type of venue, the possible provider(s); and where are these located in relation to the users?
- **When** will I move each component, what are the priorities, and what's the correct order?
- **How** am I going to carry out the migration process – will I need the help of a separate migration agency, or can my cloud provider do it for me?

Governance, risk, and compliance

Once you have a strategy to deliver the business outcome you desire, you need to consider how you will ensure proper governance and compliance.

At the planning stage, you should consider all the rules and regulations you'll need to comply with – your own corporate policies, industry rules, and data privacy laws – and devise a solution that satisfies them all. Any transformation plan should also consider the business risk of exposing strategic applications or intellectual property.

You'll need to evaluate the risk vs reward of the proposed hybrid cloud deployment to see if the effort is worth the return. Ask yourself if the advantages on offer outweigh the risk of change – especially if the workload is working alright where it is.

Take into account how the proposed change could affect your risk. Cloud is no longer the security risk it used to be – many public clouds are actually more secure now than some companies' in-house data centres (see section 2).

Hybrid clouds require a different approach to disaster recovery (see section 6), but they can also be part of the solution.

Our workload placement consulting service can help you address these issues and find the most appropriate solution.

Ability to exploit cloud

Once you've decided on the ideal strategy for workload placement, with due regard to cost, performance, governance, risk, and compliance, you'll need to assess your ability to execute it.

Key execution considerations will be:

- If your workloads are going to be moved, they may need refactoring
- If you're thinking of using containers, you should probably start in the cloud
- Think about whether your providers' management platforms give you the control and visibility you need
- You may have the skills you need in house, or you may need to tap into them by partnering
- You'll also need to look at whether your network will be able to cope.

Our cloud consulting services can help you address these issues and plan your next steps.

Hybrid cloud architecture

Once you've evaluated your ability to exploit cloud, you'll need to architect the appropriate solution. For many use cases this will involve a combination of on-premise and hosted private cloud, as well as public cloud – sometimes several of each operating together.

You should concentrate on service integration, ensuring that you will have the ability to integrate multiple clouds by using open APIs. Integration at the API level, and use of open standards, will protect you from becoming locked into any one provider's way of doing things and give you the flexibility you need to achieve your desired outcomes.

In reality, your hybrid cloud architecture cannot be separated from your wider hybrid IT environment, as the cloud components will need to interact with physical infrastructure, both on premise and hosted, as well as SaaS services.

Our architecture consulting services help you navigate these complexities, and design a solution that will satisfy all your requirements today, avoid locking you into one provider, and give you the flexibility to adapt as your business evolves.

Security

Key considerations

Effective security calls for an end-to-end holistic approach that combines threat intelligence, protection, detection, and response combined with administrative, technical, and physical controls.

First, you need visibility across the whole of your physical and virtual estate, because you can't secure what you can't see. You also need to be able to segment your network to limit threats at every level, from macro domain to individual containers.

You need defined security policies that address access control, regulatory compliance, and data security classification levels. You also need a security policy framework that is managed centrally. It should enable rapid deployment and consistent policy implementation across diverse cloud environments and be consistent with your on-premise security practices. Security controls should be deployable in your cloud environment as quickly as compute or storage resources.

Monitoring and defending against today's complex cybersecurity threat landscape is essential and must be carried out across your IT landscape no matter where your data or applications reside. You need the ability to predict, diagnose, and prevent threats to your applications, data – and virtual and physical infrastructure.

For cloud environments, you need to establish a software-defined security perimeter that can mirror the anti-virus, intrusion prevention and detection systems, firewalls and identity access management that would be deployed in an on-premise data centre environment.

You also must be ready and able to respond in the event of a security incident and contain any intrusions quickly to minimise business risk and prevent business disruption.

Our suggested hybrid cloud security methodology

- **01.** Understand your risk profile by discovering all your digital assets – on an on-going basis – regardless of location
- **02.** Validate your security posture from the asset discovery, leveraging advisory and technical services with penetration testing to define current gaps and prevent future security gaps
- **03.** Choose the right cloud environment and cloud provider based on your security needs. Ensure that you can compartmentalise service elements, both physical and logical, on a trust basis at macro, micro, and nano levels where needed
- **04.** Develop or review your security policies and implement them consistently across your cloud and on-premise environment
- **05.** Implement a well-managed, monitored and maintained software-defined security perimeter for your cloud environments, leveraging virtualised technologies that embed advanced firewall, intrusion detection, identity and access management.
- **06.** Simplify your security management and enable more automation to enforce your security standards using a leading security policy management platform that can be integrated with your hybrid cloud orchestration engine
- **07.** Be prepared with a plan to respond rapidly if there is an intrusion. If you do not have the skilled resources in house, turn to a managed security provider that has proven capabilities to support you when you need them.

Management

Platform-independent management

The aim of hybrid cloud is to be able to use whatever clouds suit your workloads, and to achieve that you need a platform-independent management capability (or a partner with one). This capability will take the form of a service management platform which abstracts away provider-specific complexities to effectively de-couple workloads from the underlying infrastructure.

Dimension Data's Managed Services Platform does this through a service layer containing a library of abstracted common services which all workloads require, such as identity management. These are accessed via open APIs to allow the workloads to function on any physical infrastructure or cloud platform, or a combination of both. We use them to automate multi-cloud orchestration processes, and deploy reference architectures automatically across whatever is the most appropriate venue(s) for the workload.

Access to such a capability is essential to realising the value of hybrid cloud, avoiding provider lock-in, and integrating hybrid cloud with physical components in a wider hybrid IT architecture.

Reference architectures

To make the most of the flexibility which hybrid cloud offers, workloads need to be based on reference architectures so that they can easily be deployed on any platform.

Reference architectures that will operate effectively on any infrastructure are not easy to develop. They need to be thoroughly tested to make sure they scale, are resilient, and function on every kind of cloud or physical infrastructure you might want to use. Companies often don't have the resources or inclination to build reference architectures themselves, and rely on providers like Dimension Data who have already made the investment.

We've developed world-class reference architectures in the productivity and collaboration space: for Microsoft (Skype for Business Enterprise Voice, Exchange, SharePoint) and Cisco Hosted Unified Communications. We also have them for Backup-as-a-Service, and our own Managed Cloud Platform. These reference architectures are designed by experts, validated by vendors, tested to breaking point, and proven in real life deployments.

Provider selection

One option is to build a hybrid cloud platform yourself. This is time consuming and costly, and burdens you with operational responsibility which to some extent defeats the object of hybrid cloud. For these reasons, DIY private cloud will probably only make sense where highly customised processes require the platform to be totally dedicated, owned and operated by the organisation itself on its own premises.

With all due regard to supplier diversity, it makes sense for most enterprises, for both operational and commercial reasons, to choose as their main cloud provider one who can offer private and public cloud from one platform, as well as integrate with the enterprise's private on-premise and hosted deployments, and any third party hyperscale providers they use.

The Dimension Data Managed Cloud Platform is a good example. It offers Enterprise Private Cloud and public cloud models of its own, as well as managed hosting services, and integrates easily with third-party public clouds, the clients' own on-premise private clouds, and third-party hosted private clouds.

Other considerations in the choice of providers will be the suitability of their platform for the application and workload, its performance, security, cost, location in relation to users, the amount of professional services and human support available, and analytical/reporting capability for charge-back and compliance purposes.

Migration

Cloud encourages a mindset of self-service, which might be entirely appropriate for developers to create the innovation you need. However, as you move into production, and you need stronger governance and security, you may require more support.

Tools alone won't provide the sort of support an enterprise needs. Very few companies have all the requisite skills in house, so they either use a third-party migration agency, or if Dimension Data is your service provider, we'll provide a full professional migration service, which extends to hybrid cloud scenarios that combine our own cloud platform with AWS or Microsoft Azure.

Your migration partner should plan the migration in every detail, and get the new environment ready to within an inch of production. Then at midnight, stop production, shut down the existing database and application servers, capture the last pieces of production data, and migrate the data to the new environment. Then they should spin up the application with real data in the new environment for the first time, and run all the necessary user acceptance tests. It's critical to monitor every aspect of performance – disc, memory, CPU, back-up, security, traffic – to see if they are performing within expected parameters, especially as users return, and at month end.

Automation and customisation

In order to manage workloads automatically across hybrid cloud environments you need to be able to de-couple the workload from the underlying infrastructure. To do this you need a management capability that uses abstraction to create a library of the

Management

common micro-services that all workloads require. These services can then be accessed by automation runbooks to deploy reference architectures automatically across any hybrid cloud, or wider hybrid IT environment.

Automation is a necessary, but not sufficient, prerequisite for success in hybrid cloud. Any complex enterprise will also require the ability to customise the processes it's automating. At Dimension Data, we give clients not just abstracted services and automation runbooks, but also access to them via open APIs so that they can customise them, or we can customise them of their behalf.

Although hybrid cloud is a highly automated world, there is always a place for people. Most enterprises will also need access to skilled professional support personnel who are available at the times and locations, over the channels and speaking the languages, they require.

But before you can automate, you need visibility.

Visibility

As you adopt more hybrid cloud, visibility becomes more of an issue. You need to be able to see everything you've got, both private and public resources, on-premise and hosted – and preferably your non-cloud resources as well – ideally, all in one place.

Visibility isn't an end in itself – you don't want to be looking at a portal all day. The data the portal collects gives you the ability to automate business policies around events. Having a portal gives you the option to intervene when you're troubleshooting, and analyse trends to spot opportunities for automation.

Again, getting this 20/20 vision of hybrid cloud isn't easy if you have to use a separate provider's portal for each resource.

Our award-winning business portal, Manage Centre, gives you the centralised visibility you need. It's an immediate, graphical view of your different technologies – all in one place:

- colour coding shows you instantly where to focus
- interactive charts, diagrams, and maps make important things clear at a glance
- you can drill down to analyse the data and understand trends
- and see the impact that your technology is having on your business processes.

Beyond hybrid cloud, it actually shows you everything covered under a contract with us – all your technologies (data centre, cloud, networking, security, applications, etc) – and you can view it on your laptop, tablet, or mobile device.

Skills

In a recent survey, we conducted of global enterprises, 35% said that lack of skills was one of the main concerns they had around adopting more hybrid cloud.

There are many different types of skills required for successful hybrid cloud programme: skills in strategy, architecting, migration, management, security, networking, containerisation and so on.

Talent with these skills is increasingly hard to attract and retain, and a faster path is to use a service provider who already has them.

The same survey revealed the most common strategy for accessing these scarce skills is to tap into them on an as-needed basis through a partner, with 62% of hybrid cloud spend being on managed services.

Using a managed cloud service provider frees you from mundane activities and allows you to apply your in-house skills where they will add more value to your business, such as in defining business policies or accelerating innovation through DevOps.

Management continuum

In the light of all these management issues, the final question about management to ask yourself is where you want to be on the management continuum, i.e. how much do you want to manage hybrid cloud yourself, versus how much do you want it provided as a managed service.

The answer will depend on where on the management continuum you feel you create business value, and the degree of standardisation vs customisation involved. It also depends on what resources you need, who's using them, and what skills you have in-house.

You may want the ability for developers to spin up development environments on public cloud resources themselves on a self-service basis. But you may want a higher degree of management support from your service provider for a production environment on the private portion of your hybrid cloud. Here you might want support at just the infrastructure level, or you may need it to be managed at the platform, application, or business process level.

Networking

Cloud networking

An often-overlooked area of complexity in hybrid cloud is cloud networking. Each cloud provider has their own preferred way for you to connect to them. It's important to understand their networking product set so you can control where your traffic enters the cloud provider's network, as this can affect application performance. The drawback is that learning their toolset takes time, and you have to keep up with it as it evolves.

The other side to this is that in a hybrid cloud environment some of your workloads will be on your own private cloud, and you don't want to have to connect to these elements in a totally different way.

The advantage of working with an independent networking specialist like Dimension Data is that we can allow you to connect to all parts of your environment in a consistent way. This means we can give you an end to end view of application performance across all parts of the network making it easier to troubleshoot any bottlenecks.

We do this through the service layer of our cloud management capability. It uses an abstracted library of microservices accessed via open APIs to orchestrate networking resources across on-premise private clouds, third-party public clouds like AWS or Microsoft Azure, and our own Managed Cloud Platform, so providing a unified way of managing networks across your hybrid cloud environment.

Data centre networks

Many companies will keep some of their workloads in private clouds in their own data centres for compliance reasons. From the end user's point of view, applications hosted in your own data centre have to offer the same quality of experience as workloads hosted in the cloud.

To keep up with the performance levels set by the hyperscalers, you need to invest in speed, scalability, and capacity in your data centre network, especially for the East-West traffic staying within the data centre. This means getting bigger pipes, faster switches, and software-defining the data centre network.

A software-defined data centre network is necessary to automate how the network provisions itself up or down in real time, in tandem with compute and storage elements of your cloud services. This applies not just to connectivity and bandwidth, but other networking services such as IP addressing, and optimisation services.

Upgrading technology is part of it, but you also need to evolve management processes and skill sets. In the hybrid world, you have to treat the network as a system and program it through an SDN controller, accessed via an API. Most companies aren't ready to do this themselves, but we've upskilled our data centre networking people, and implemented SDN in all our data centres, so if you host your private cloud in our data centre we can handle this for you.

Hybrid WAN

As companies adopt more hybrid cloud, WAN performance becomes more of an issue.

Most companies' existing WANs were architected pre-cloud on an assumption that traffic needed to be routed to and from an application running in their private data centre. As workloads are moved to the cloud, data traffic patterns change, and WANs need to be rearchitected to avoid performance degradation.

Companies who continue to rely on the existing Internet breakout at their data centre, might easily find themselves inadvertently routing traffic for thousands of extra miles to where their application is physically located within their cloud provider's environment, causing performance and cost issues.

A potential alternative is to break out to the Internet closer to the branch, but this opens up a new attack surface, and the resulting security and data governance issues will need to be addressed carefully.

The hybrid WANs used for hybrid cloud use multiple carriage types, i.e. carriers and the Internet, so some companies ask their carriers to design them, but they need to be wary of the carrier's vested interests. In order to get a true optimum balance between VPN and the Internet it's best to use an impartial managed network service provider who is carrier neutral.

Getting your hybrid WAN right is critical to making hybrid cloud work, because if you don't, not only could you see your potential savings ebb away, but you could even end up with worse application performance.

Wireless access

One of the common types of workload deployed across hybrid cloud is unified communications and productivity. In modern workplaces, these applications are commonly accessed via wi-fi networks, and feature high volumes of voice and video traffic.

As a consequence of this trend, many companies are finding it necessary to invest in upgrading their wi-fi access points and access layer network infrastructure in order to deliver a satisfactory user experience.

According to our Network Barometer Report 2016, 33% of enterprises have access points supporting wireless protocol 802.11n and upwards, and the prevalence of 10Gb capable access switches has risen by 18% in the last year.

But increasing bandwidth is not enough. The wi-fi network also needs to be smart enough to prioritise voice and video traffic over, say, email, in order to deliver appropriate quality of service for these time-sensitive applications.

Do not simply assume the network will be able to cope. Assess current capability, forecast future requirements, analyse the gap, and implement upgrades to both wi-fi access points and the access layer network. This way you can ensure your hybrid cloud strategy is not foiled by inadequate capacity at the access level.

Consumption models

Consumption-based pricing

In general, cloud has given the enterprise market an appetite for consumption based pricing. Companies are attracted to the opportunity of avoiding capital expenditure and matching costs more closely to fluctuating business volumes.

Consumption-based pricing is now a realistic option for enterprise grade public cloud. For example, our multi-tenanted public cloud platform is priced per resource per hour. Clients pay per gigabyte per hour for memory, per hour per virtual CPU, and per gigabyte per hour for storage (of different types, depending on the technology being used).

Hybrid consumption models

Consumption-based pricing isn't important to all organisations. Many in the public sector operate entirely on capital budgets; others have stable business volumes and want predictable costs to match.

Enterprises are also less intent on variable costs when it comes to private cloud. They want flexibility, but they want it in a dedicated environment, so accept a commercial model which combines fixed and variable elements.

For our Enterprise Private Cloud, we charge a baseline six-monthly fee, and then on top of that there is a flexible pricing structure, in which clients can balance fixed and variable costs according to their predicted usage profile.

Some clients who know their usage will fluctuate, and want their costs to align with usage, opt for low monthly charges, and a larger proportion of usage-based charges. Others who can't make such certain predictions about their variable usage, prefer higher monthly fees and a smaller consumption-based component.

Don't forget to turn the lights out

One of the surprising things about consumption-based pricing is how some clients don't turn off usage-based resources when they're not using them. This seems to be a matter of psychology more than anything. Just because you have the option to turn the lights out when you leave a room, it doesn't mean you will. Many clients like to come back to a 'lit room', and don't mind paying to keep the lights on while they're out.

But if you want to make sure hybrid cloud gives you the cost savings you were hoping for, you need to implement management processes to switch off usage-based resources when you're not using them.

Business continuity and disaster recovery

Risk assessment and resiliency strategy

Business resilience and backup planning begins at the strategy stage. Before designing your hybrid cloud environment, you need to conduct a business impact and risk analysis to identify critical processes and systems that may be susceptible to unplanned outages, and examine vulnerabilities that could contribute to a disaster.

Then when you are architecting your solution, you need to ensure that it is resilient and recoverable, and aligns with your business policies and budgets. You need to make sure everything critical is protected fully, but that you don't over-engineer and over-pay for resilience where it's not needed.

Cloud backup

Once operational, you need to make sure that your hybrid cloud environment is backed up in compliance with corporate policy and industry regulation. You need a system that will back up all your servers regardless of their location.

For example, we back up our clients' workloads whether they're on our cloud, someone else's cloud, on physical equipment on the clients' premises, or in a hosting facility.

Enterprises should look for a backup service that includes de-duplication for faster backup, reduced storage requirements, and greater cost savings.

Encryption on the wire and at rest will ensure data security and compliance at all times. These services are available without any capital outlay, priced per server, per gigabyte, or on a daily basis.

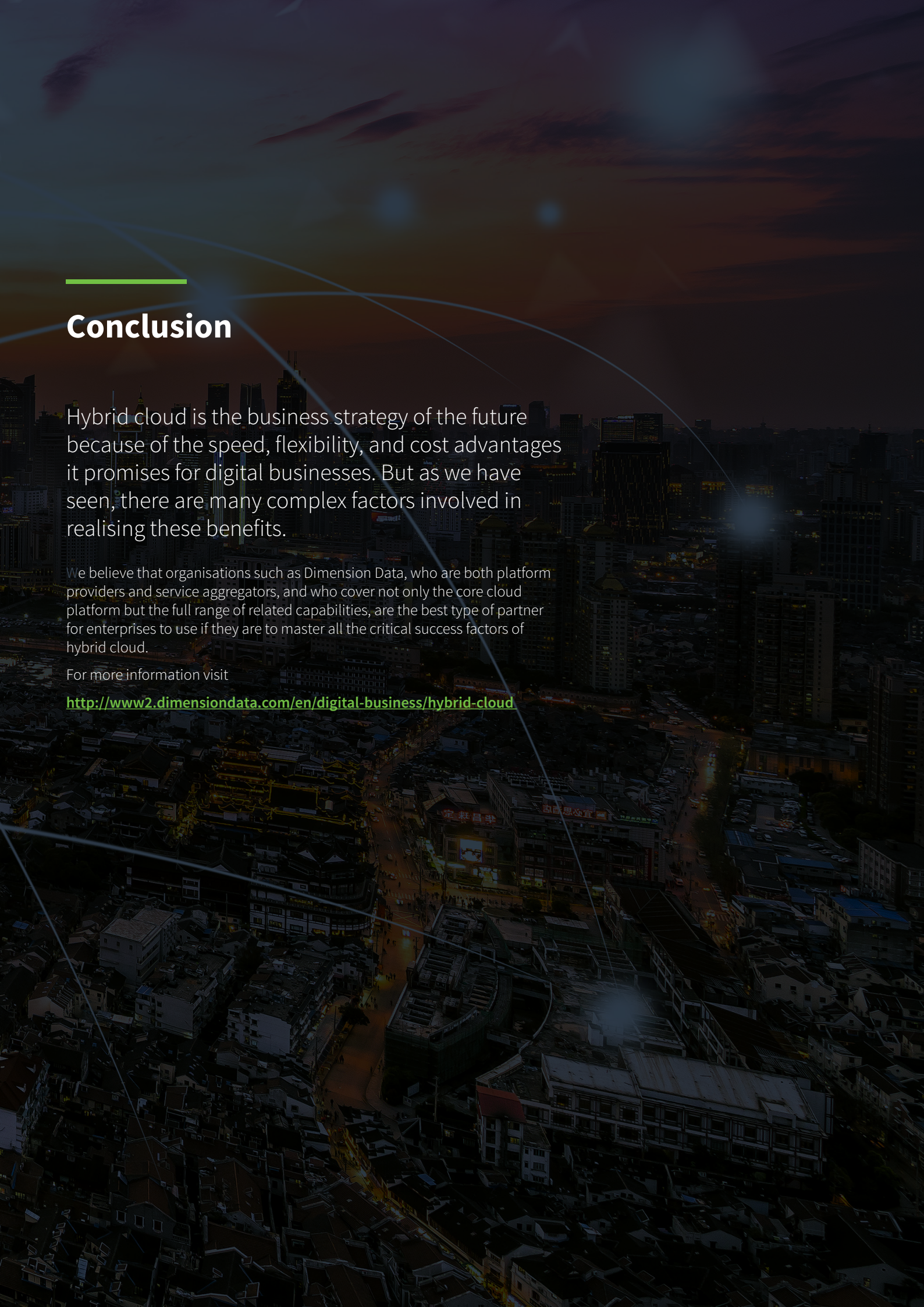
Managed disaster recovery

Hybrid cloud creates new opportunities for higher resilience, such as backing up desktops to the cloud. But it also requires a different approach to disaster recovery than traditional environments.

Not only are resources not on your premises, or under your direct control, but they may consist of multi-tier applications residing on different virtual machines spread between your premises and several cloud providers.

When it comes to restoring these systems following a compromise, you need to be able to preserve relational dependencies (such as between databases and logs) and restore systems in the right order. Consistency groups need to have shared journals so that you can reinstate to the situation just moments before the corruption occurred.

Not surprisingly, most enterprises opt for the confidence provided by a managed disaster recovery service. Enterprises should look for a service that includes developing the plan, testing and executing it, and keeping it up to date. A good service level agreement would offer recovery point objectives of less than 15 minutes and recovery time objectives of less than four hours. It's important to check that recovery would preserve the relational dependencies of applications supporting your mission-critical business processes.



Conclusion

Hybrid cloud is the business strategy of the future because of the speed, flexibility, and cost advantages it promises for digital businesses. But as we have seen, there are many complex factors involved in realising these benefits.

We believe that organisations such as Dimension Data, who are both platform providers and service aggregators, and who cover not only the core cloud platform but the full range of related capabilities, are the best type of partner for enterprises to use if they are to master all the critical success factors of hybrid cloud.

For more information visit

http://www2.dimensiondata.com/en/digital-business/hybrid-cloud